UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA DE TELEINFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE TELEINFORMÁTICA

YOSBEL RODRÍGUEZ ORTEGA

EFEITO CONJUNTO DE SINAIS INTERFERENTES E RUÍDO EM CANAIS *WIRETAP* COM MÚLTIPLAS ANTENAS E ATRASO DE *FEEDBACK*

FORTALEZA
2017

YOSBEL RODRÍGUEZ ORTEGA

EFEITO CONJUNTO DE SINAIS INTERFERENTES E RUÍDO EM CANAIS *WIRETAP* COM MÚLTIPLAS ANTENAS E ATRASO DE *FEEDBACK*

Dissertação apresentada ao Programa de Pós-graduação em Engenharia de Teleinformática da Universidade Federal do Ceará, como parte dos requisitos necessários para a 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)

O88e Ortega, Yosbel Rodríguez.
Efeito Conjunto de Sinais Interferentes e Ruído em Canais Wiretap com Múltiplas Antenas e Atraso de Feedback / Yosbel Rodríguez Ortega. – 2017.
90 f. : il. color.

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 outage.. 2. Canais wiretap.. 3. Sinais de interferência.. 4. CSI imperfeita.. I. Título.
CDD 621.38

YOSBEL RODRÍGUEZ ORTEGA

EFEITO CONJUNTO DE SINAIS INTERFERENTES E RUÍDO EM CANAIS *WIRETAP* COM MÚLTIPLAS ANTENAS E ATRASO DE *FEEDBACK*

Dissertação apresentada ao Programa de Pós-graduação em Engenharia de Teleinformática 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: 17/02/2017.

BANCA EXAMINADORA

Prof. Dr. DANIEL BENEVIDES DA COSTA (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Prof. Dr. FRANCISCO RODRIGO PORTO CAVALCANTI
Universidade Federal do Ceará (UFC)

Prof. Prof. Dr. FRANCISCO RAFAEL MARQUES LIMA
Universidade Federal do Ceará (UFC)

A minha família e amigos..

AGRADECIMENTOS

Esta nova realização profissional e pessoal não teria sido possível sem a ajuda e o apoio de muitas pessoas que fazem parte da minha vida.

Primeiro de tudo, gostaria de agradecer e dedicar esta conquista de maneira muito especial a minha família, pelo apoio espiritual em todo este tempo apesar da distância. Um monte de compreensão e amor é necessário para alcançar um objetivo longe da família. Especialmente a minha mãe Victoria Ortega e a minha filha Chenoa María Rodríguez.

A minha esposa Ivonne Montero por todo apoio incondicional, carinho, amor, compreensão, por estar ao meu lado durante todos os momentos difíceis.

Ao prof. Dr. Daniel Benevides da Costa por ter assumido o posto de orientador e pela sua ajuda ao longo deste período.

Aos meus amigos e companheiros do Grupo de Telecomunicações Sem Fio-GTEL, pela ajuda e por me fazer sentir como mais um brasileiro.

Aos professores e trabalhadores do GTEL pela compreensão e apoio durante este período.

Á Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) pelo apoio financeiro que tive durante esse período.

A todos minha sincera gratidão.

RESUMO

Nesta dissertação, a segurança da camada física de canais *wiretap* com múltiplas antenas e com informação de estado do canal (CSI, do inglês, *channel state information*) desatualizada, é investigada em termos da probabilidade de *outage* de sigilo. O efeito conjunto de múltiplos sinais de interferência e ruído no nó malicioso é estudado. Paralelamente, é analisado o caso especial para um canal em que apenas o transmissor é equipado com múltiplas antenas. Nestes modelos, o transmissor utiliza a técnica de seleção de antena (TAS, do inglês, *transmit antenna selection*); o receptor legítimo usa os esquemas de combinação por seleção (SC, do inglês, *selection combining*) e combinação por razão máxima (MRC, do inglês, *maximal-ratio combining*); e o nó malicioso adota somente a técnica MRC. Expressões analíticas exatas e em forma fechada para a probabilidade de *outage* de sigilo e a taxa de sigilo não-nula são derivadas, tanto assumindo CSI perfeita como CSI imperfeita, sendo aplicáveis para sinais de interferência com distribuição de potências arbitrárias. As expressões obtidas são simplificadas para dois casos especiais: sinais de interferência com distribuição de potências distintas e iguais. Uma análise assintótica da probabilidade de *outage* de sigilo é realizada, mostrando que o ganho de diversidade esperado não pode ser realizado para uma CSI imperfeita e a ordem de diversidade completa apenas pode ser alcançada em condições de CSI perfeita. Além disso, estes resultados mostram que o número de sinais de interferência, bem como o número de antenas no nó intruso, não afetam a ordem de diversidade do sistema. Exemplos numéricos representativos são apresentados para ilustrar os efeitos dos principais parâmetros do sistema no desempenho de *outage* de sigilo. Finalmente, a análise proposta é validada através de simulações de Monte Carlo.

Palavras-chave: Desempenho de *outage*, canais *wiretap*, sinais de interferência, CSI imperfeita.

ABSTRACT

In this dissertation, the physical layer security of wiretap channels with multiple antennas and outdated channel state information (CSI) at the transmitter is investigated in terms of the secrecy outage probability. The joint effect of multiple jamming signals and noise at the eavesdropper is studied. In parallel, it is analyzed the special case where only the transmitter is equipped with multiple antennas. On such models, the transmitter employs a transmit antenna selection (TAS) technique; the legitimate receiver uses either a selection combining (SC) or a maximal-ratio combining (MRC) scheme; and the eavesdropper adopts the MRC technique. Exact closed-form expressions for the non-zero secrecy rate and secrecy outage probability for arbitrary number of power distributed jamming signals are derived, by assuming both perfect and imperfect CSI. The attained expressions are simplified for two special cases: distinct and equal power distributed jamming signals. An asymptotic secrecy outage analysis is conducted, which shows that the expected diversity gain cannot be realized for imperfect CSI, and full diversity order can only be achieved under perfect CSI condition. In addition, those results reveal that the number of jamming signals as well as the number of antennas at the eavesdropper do not affect the system diversity order. Representative numerical examples are presented to illustrate the effects of the key system parameters on the secrecy outage performance. Finally, the proposed analysis is validated through Monte Carlo simulation results.

Keywords: Secrecy outage performance, wiretap channels, jamming signals, outdated CSI.

LISTA DE FIGURAS

Figura 1 – Esquema MIMO MxN. 26
Figura 2 – Ganho de diversidade na recepção. 28
Figura 3 – Ganho de diversidade e ganho de *array* na recepção. 29
Figura 4 – Esquema de Combinação por Seleção (SC). 30
Figura 5 – Esquema de Combinação por Razão Máxima (MRC). 31
Figura 6 – Diversidade na transmissão e recepção. 34
Figura 7 – TAS com modulação adaptativa e MRC 36
Figura 8 – Sistema *beamforming*. 38
Figura 9 – Alinhamento de ruído artificial. 41
Figura 10 – Modelo do Sistema. 43
Figura 11 – Probabilidade de *outage* de sigilo versus SNR média em Bob assumindo esquema SC em Bob. Premissas: $\bar{\gamma}_E = -3$dB; $R = 1$; sinais interferentes com distribuição de potências iguais. 65
Figura 12 – Probabilidade de *outage* de sigilo versus SNR média em Bob assumindo esquema MRC em Bob com CSI perfeita. Premissas: $\bar{\gamma}_E = -3$dB; $R = 1$; sinais interferentes com distribuição de potências distintas. 66
Figura 13 – Probabilidade de *outage* de sigilo versus SNR média em Bob assumindo esquema SC em Bob e um canal MISO. Premissas: $\bar{\gamma}_E = -3$dB; $R = 1$; sinais interferentes com distribuição de potências iguais. 66
Figura 14 – Probabilidade de *outage* de sigilo versus SNR média em Bob assumindo esquema MRC em Bob e um canal MISO. Premissas: $\bar{\gamma}_E = -3$dB; $R = 1$; sinais interferentes com distribuição de potências distintas. 67
Figura 15 – Probabilidade de *outage* de sigilo versus SNR média em Bob para diferentes esquemas de combinação de sinal e configurações de interferência. Premissas: $N_A = N_B = 2$, $N_E = 1$, $\bar{\gamma}_E = -3$dB; $R = 1$; sinais interferentes com distribuição de potências distintas. 68
Figura 16 – Probabilidade de *outage* de sigilo versus SNR média em Bob assumindo esquema MRC em Bob com CSI imperfeita para diferentes valores de ρ. Premissas: $\bar{\gamma}_E = 3$ dB; $R = 1$; $N_{\mathrm{A}} = N_{\mathrm{B}} = N_{\mathrm{E}} = 2$; sinais interferentes com distribuição de potências distintas com $\bar{\gamma}_i$=[1 2] dB. 69
Figura 17 – Probabilidade de *outage* de sigilo versus ρ assumindo esquema MRC em Bob. Premissas: $\bar{\gamma}_E = 3$ dB; $R = 1$; $\bar{\gamma}_B = 25$ dB; sinais interferentes com distribuição de potências distintas. 70

Figura 18 – Probabilidade de *outage* de sigilo versus SNR média em Bob assumindo esquema MRC em Bob com CSI imperfeita. Premissas: $\bar{\gamma}_E = 3$dB; $R_0 = 1$; $N_\mathrm{A} = N_\mathrm{B} = 2$; $\bar{\gamma}_E = 3$dB; sinais interferentes com distribuição de potências distintas com $\bar{\gamma}_i = \{(1,2),(2,3,4)\}$dB para $M = 2,3$. 70
Figura 19 – Probabilidade de *outage* de sigilo versus SNR média em Bob assumindo esquema MRC em Bob com diferentes configurações de antenas em Bob e diferentes valores de ρ. Premissas: $\bar{\gamma}_E = 3$dB; $R_0 = 1$; $N_\mathrm{A} = N_\mathrm{E} = 2$; sinais interferentes com distribuição de potências iguais com $\bar{\gamma}_i = 2$dB para $M = 2$. 71
Figura 20 – Probabilidade de *outage* de sigilo versus SNR média em Eve assumindo esquema SC em Bob. Premissas: $N_A = 2$; $N_B = 2$; $\bar{\gamma}_B = 10$dB; $R = 1$; sinais interferentes com distribuição de potências iguais. 72
Figura 21 – Probabilidade de *outage* de sigilo versus SNR média em Eve assumindo esquema MRC em Bob com CSI perfeita. Premissas: $N_A = 2$; $N_B = 2$; $\bar{\gamma}_B = 10$dB; $R = 1$; sinais interferentes com distribuição de potências distintas. 73
Figura 22 – Probabilidade de *outage* de sigilo versus SNR média em Eve assumindo esquema MRC em Bob com diferentes valores de ρ. Premissas: $\bar{\gamma}_E = 3$dB; $R = 1$; $N_\mathrm{A} = N_\mathrm{B} = 2$; $\bar{\gamma}_E = 3$dB; sinais interferentes com distribuição de potências distintas com $\bar{\gamma}_i = \{(1,2),(1,2,3,4)\}$dB para $M = 2,4$. 73
Figura 23 – Ganho de *array* versus número de antenas em Alice (N_A) assumindo esquema SC em Bob. Premissas: $N_B = 2$; $\bar{\gamma}_E = -5$dB; sinais interferentes com distribuição de potências distintas. 75
Figura 24 – Ganho de *array* versus número de antenas em Alice (N_A) assumindo esquema MRC em Bob. Premissas: $N_B = 2$; $\bar{\gamma}_E = -5$dB; sinais interferentes com distribuição de potências distintas. 75
Figura 25 – Ganho de *array* versus número de antenas em Alice (N_A) assumindo esquema SC em Bob e um canal MISO. Premissas: $N_B = 2$; $\bar{\gamma}_E = -5$dB; sinais interferentes com distribuição de potências distintas. 76
Figura 26 – Ganho de *array* versus número de antenas em Alice (N_A) assumindo esquema MRC em Bob e um canal MISO. Premissas: $\bar{\gamma}_E = -5$dB; sinais interferentes com distribuição de potências distintas. 77
Figura 27 – Taxa de sigilo não-nula versus SNR média em Bob, assumindo esquema SC em Bob. Premissas: $N_B = 3$; $\bar{\gamma}_E = 5$dB; sinais interferentes com distribuição de potências iguais com $\bar{\gamma}_i = 2$dB para $M = 2,3,4$. 77
Figura 28 – Taxa de sigilo não-nula versus SNR média em Bob, assumindo esquema MRC em Bob. Premissas: $N_B = 3$; $\bar{\gamma}_E = 5$dB; sinais interferentes com distribuição de potências distintas com $\bar{\gamma}_i = \{(2,3),(2,3,4),(2,3,4,5)\}$dB para $M = 2,3,4$ respectivamente. 78

Figura 29 – Taxa de sigilo não-nula versus SNR média em Bob, assumindo esquema SC em Bob e um canal MISO. Premissas: $\bar{\gamma}_E = 5$dB; sinais interferentes com distribuição de potências iguais com $\bar{\gamma}_i = 2$dB para $M = 2, 3, 4$. . . . 79
Figura 30 – Taxa de sigilo não-nula versus SNR média em Bob, assumindo esquema MRC em Bob e um canal MISO. Premissas: $\bar{\gamma}_E = 5$dB; sinais interferentes com distribuição de potências distintas com $\bar{\gamma}_i = \{(2, 3), (2, 3, 4), (2, 3, 4, 5)\}$dB para $M = 2, 3, 4$ respectivamente. 79
Figura 31 – Taxa de sigilo não-nula versus SNR média em Bob, assumindo esquema MRC para diferentes valores de ρ. Premissas: $\bar{\gamma}_E = 3$dB; $R = 1$; $N_{\mathrm{A}} = 2$; sinais interferentes com distribuição de potências distintas com $\bar{\gamma}_i = \{(2, 3), (2, 3, 4, 5)\}$dB para $M = 2, 4$. 80

LISTA DE TABELAS

Tabela 1 – Trabalhos que investigaram o desempenho de *outage* de sigilo com diferentes configurações. 21

LISTA DE ABREVIATURAS E SIGLAS

AWGN	Ruído Gaussiano Branco Aditivo
AF	Amplifica-e-Encaminha
AM	Modulação Adaptativa
CDF	Função de Distribuição Cumulativa
CEE	Erros de Estimação de Canal
CSI	Informação de Estado do Canal
DOA	Direção de Chegada
EGC	Combinação por Ganho Igual
FEC	Codificação para Correção de Erros
FJ	Nó Amigo
GSC	Combinação por Seleção Generalizada
IA	Alinhamento de Interferência
iid	independente e identicamente distribuído
MIMO	Múltiplas Entradas e Múltiplas Saídas
MISO	Múltiplas Entradas e Única Saída
ML	Máxima Verossimilhança
MRC	Combinação por Razão Máxima
MRT	Transmissão por Razão Máxima
PDF	Função de Densidade de Probabilidade
PHY	Camada Física
QoS	Qualidade de Serviço
PO	Probabilidade de Outage de Sigilo
RF	Rádio Frequência
RMS	Valor Quadrático Médio
SC	Combinação por Seleção
SSC	Combinação por Chaveamento e Fixação
SER	Taxa de Erro de Símbolo
SINR	Relação Sinal-Interferência Mais Ruído
SISO	Única Entrada e Única Saída
SIR	Relação Sinal-Interferência
SNR	Relação Sinal-Ruído
ST	Códigos Espaço-Temporais
STBC	Códigos Espaço-Temporais de Bloco
STTC	Códigos Espaço-Temporais de Treliça
TAS	Seleção de Antena de Transmissão
TB	Transmissão por Conformação de Feixe
TSC	Combinação de Seleção por Limiar

VA Variável Aleatória

LISTA DE SÍMBOLOS

$(.)^{\dagger}$	Conjugado transposto
$\|\|.\|\|$	Norma de Frobenius
$(.)^{T}$	Operador trasnposto
$\|.\|$	Valor absoluto
$f_{\gamma_{\mathrm{B,s}}}^{\mathrm{SC}}$	PDF da SNR em Bob usando esquema SC
$f_{\gamma_{\mathrm{B,s}}}^{\mathrm{MRC}}$	PDF da SNR em Bob usando esquema MRC
$f_{\breve{\gamma}_{\mathrm{B,s}}}^{\mathrm{MRC}}$	PDF da SNR em Bob usando esquema MRC e CSI desatualizada
$f_{\gamma_{\mathrm{I}}+1}$	PDF de interferência plus ruído
$f_{\Upsilon_{\mathrm{E,s}}}$	PDF da SINR em Eve
$F_{\gamma_{\mathrm{B,s}}}^{\mathrm{SC}}$	CDF da SNR em Bob usando esquema SC
$F_{\gamma_{\mathrm{B,s}}}^{\mathrm{MRC}}$	CDF da SNR em Bob usando esquema MRC
$F_{\breve{\gamma}_{\mathrm{B,s}}}^{\mathrm{MRC}}$	CDF da SNR em Bob usando esquema MRC e CSI desatualizada
$f_{\breve{\gamma}_{\mathrm{B,s}}^{\mathrm{MRC}}\|\gamma_{\mathrm{B,s}}^{\mathrm{MRC}}}$	PDF de $\breve{\gamma}_{\mathrm{B,s}}^{\mathrm{MRC}}$ condicionada por $\gamma_{\mathrm{B,s}}^{\mathrm{MRC}}$
$f_{\breve{\gamma}_{\mathrm{B},\lambda}^{\mathrm{MRC}},\gamma_{\mathrm{B},\lambda}^{\mathrm{MRC}}}$	PDF conjunta de $\breve{\gamma}_{\mathrm{B},\lambda}^{\mathrm{MRC}}$ e $\gamma_{\mathrm{B},\lambda}^{\mathrm{MRC}}$
G_{D}	Ganho de diversidade
G_{A}	Ganho de *array*
$\gamma_{\mathrm{B,s}}^{\mathrm{SC}}$	SNR instantânea em Bob usando esquema SC
$\gamma_{\mathrm{B,s}}^{\mathrm{MRC}}$	SNR instantânea em Bob usando esquema MRC
$\breve{\gamma}_{\mathrm{B,s}}^{\mathrm{MRC}}$	SNR instantânea em Bob usando esquema MRC e CSI desatualizada
$\bar{\gamma}_{\mathrm{B}}$	SNR média em Bob
$\bar{\gamma}_{i}$	Potência do $i^{ésimo}$ 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
f_d	Frequência Doppler Máxima
$\Gamma(.)$	Funcão Gamma
$\Psi(.,.,.)$	Funcão de Tricomi
$h_{\mathrm{AB},\lambda}^{\delta}$	Coeficiente de canal entre a $\lambda^{ésima}$ antena de Alice e a $\delta^{ésima}$ antena de Bob
$h_{\mathrm{AB,s}}$	Coeficiente de desvanecimento no enlace Alice-Bob
$\mathbf{h}_{\mathrm{AB},\lambda}$	Vetor de canal com dimensões $N_B \times 1$ entre Bob e a $\lambda^{ésima}$ antena em Alice
$\breve{\mathbf{h}}_{\mathrm{AB},\lambda}$	Versão de $\mathbf{h}_{\mathrm{AB},\lambda}$ com atraso no tempo
$\mathbf{h}_{\mathrm{AB,s}}$	Vetor de canal com dimensões $N_B \times 1$ entre a antena selecionada por Alice e Bob
$\breve{\mathbf{h}}_{\mathrm{AB},s}$	Versão de $\mathbf{h}_{\mathrm{AB},s}$ com atraso no tempo
$\mathbf{h}_{\mathrm{AE,s}}$	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 $i^{ésimo}$ sinal de interferência
$\breve{h}_{\mathrm{i}}$	Coeficiente do canal de interferência à saída do MRC

ϑ	Variável aleatória Gaussiana com variância igual à de $\mathbf{h}_{\mathrm{AB},\lambda}$
$I_k(.)$	$k^{ésima}$ funcão de Bessel modificada do primeiro tipo [62, Eq. (8.406.1)]
J_0	Funcão de Bessel de ordem zero de primeiro tipo [62, Eq. (8.402)]
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
$P_{\mathrm{s}}^{\mathrm{SC}}$	Probabilidade de *outage* para o esquema SC
$P_{\mathrm{s}}^{\mathrm{MRC}}$	Probabilidade de *outage* para o esquema MRC
$\breve{P}_{\mathrm{s}}^{\mathrm{MRC}}$	Probabilidade de *outage* para o esquema MRC e CSI desatualizada
$P_{\mathrm{r}}^{\mathrm{SC}}$	Taxa de sigilo distinta de zero para o esquema SC
$P_{\mathrm{r}}^{\mathrm{MRC}}$	Taxa de sigilo distinta de zero para o esquema MRC
$\breve{P}_{\mathrm{r}}^{\mathrm{MRC}}$	Taxa de sigilo distinta de zero para o esquema MRC e CSI desatualizada
$P_{\mathrm{s}}^{\infty(\mathrm{SC})}$	Probabilidade de *outage* assintótica para o esquema SC
$P_{\mathrm{s}}^{\infty(\mathrm{MRC})}$	Probabilidade de *outage* assintótica para o esquema MRC
$\breve{P}_{\mathrm{s}}^{\infty(\mathrm{MRC})}$	Probabilidade de *outage* assintótica para o esquema MRC e CSI desatualizada
R	Limiar estabelecido
$R_{\mathrm{B,s}}$	Capacidade do canal Alice-Bob
$R_{\mathrm{E,s}}$	Capacidade do canal Alice-Eve
ρ	Coeficiente de Correlacão
R_{S}	Capacidade de sigilo
s	Índice da antena de transmissão selecionado por Alice
τ	Atraso no tempo
σ_b^2	Variância
$\mathbf{w}_{\mathrm{B}}$	Vetor de pesos MRC
x	Sinal transmitida
y_{B}	Sinal combinado em Bob
y_{E}	Sinal combinado em Eve

SUMÁRIO

1 INTRODUÇÃO 18
1.1 Contexto do Problema 18
1.2 Revisão da Literatura 18
1.3 Motivação e Objetivos 21
1.4 Estrutura do Trabalho 23
1.5 Produção Científica 24
2 FUNDAMENTAÇÃO TEÓRICA 24
2.1 Introdução 24
2.2 Modelo do Sistema MIMO 25
2.2.1 *Ganhos nos Sistemas MIMO* 26
2.2.2 *Ganho de Diversidade* 27
2.2.3 *Ganho de Array* 28
2.3 Diversidade Espacial na Recepção 29
2.3.1 *Combinação por Seleção (SC, Selection Combining)* 30
2.3.2 *Combinação por Razão Máxima (MRC, maximal-ratio combining)* 31
2.3.3 *Outros Esquemas de Combinação na Recepção* 32
2.4 Diversidade Espacial na Transmissão 33
2.4.1 *Seleção de Antena de Transmissão (TAS, do inglês, transmit antenna selection)* 34
2.4.2 *Códigos Espaço-Temporais (ST, do inglês, space-time codes)* 35
2.4.3 *Codificação Espaço-Temporal de Bloco (STBC)* 36
2.4.4 *Codificação Espaço-Temporal de Treliça (STTC)* 37
2.4.5 *Beamforming* 37
2.5 Segurança na Camada Física 38
2.5.1 *Capacidade de Sigilo* 39
2.5.2 *Interferência Cooperativa* 40
2.6 Conclusões 42
3 SEGURANÇA DA CAMADA FÍSICA PARA SISTEMAS MIMO 42
3.1 Introdução 42
3.2 Modelo do Sistema 43
3.2.1 *Esquema MRC em Bob* 44
3.2.2 *Esquema SC em Bob* 45
3.2.3 *Esquema MRC em Eve Sujeito a Ruído e Sinais de Interferência* 46
3.3 Desempenho de *Outage* de Sigilo 47

3.3.1 ***Estatísticas Úteis*** 47
3.3.2 ***Esquema MRC em Bob*** 48
3.3.3 ***Esquema SC em Bob*** 50
3.3.4 ***Esquema MRC em Eve*** 50
3.4 **Probabilidade de *Outage* de Sigilo** 51
3.4.1 ***MRC em Bob*** 52
3.4.2 ***SC em Bob*** 55
3.5 **Taxa de Sigilo Não-Nula** 56
3.6 **Probabilidade de *Outage* de Sigilo Assintótica** 58
3.6.1 ***MRC em Bob com CSI perfeita*** 58
3.6.2 ***MRC em Bob com CSI imperfeita*** 59
3.6.3 ***SC em Bob*** 61
3.7 **Conclusões** 62
4 **RESULTADOS NUMÉRICOS E DISCUSSÕES** 63
4.1 **Introdução** 63
4.2 **Simulações de Monte Carlo** 63
4.3 **Apresentação dos Resultados Numéricos** 64
4.4 **Conclusões** 80
5 **CONCLUSÕES E TRABALHOS FUTUROS** 81
REFERÊNCIAS 83

1 INTRODUÇÃO

1.1 Contexto do Problema

As redes sem fio têm experimentado um crescimento significativo nas últimas décadas. As características de estar disponível para qualquer pessoa e a de facilitar a comunicação e a informação com rapidez em qualquer local público ou privado fizeram deste tipo de rede uma das tecnologias mais populares e exploradas na atualidade. Paradigmas tradicionais e essenciais em telecomunicações, tais como a qualidade de serviço e a segurança, têm sido estudados e adaptados para redes sem fio.

Com relação à segurança, ao longo dos anos, inúmeros esforços têm sido dedicados para alcançar e preservar o sigilo da informação. Estas preocupações tornam-se mais críticas em redes sem fio devido à natureza *broadcast* do meio, que as torna mais vulneráveis à intromissão de possíveis nós maliciosos (chamados intrusos, do inglês *eavesdroppers*), com a capacidade de interceptar a troca de informações entre os nós legítimos. Tradicionalmente, as estratégias para assegurar a privacidade eram efetuadas nas camadas superiores da pilha de protocolos, usando técnicas de criptografia [1] ou pela codificação de canal [2]. No entanto, em anos recentes, tem sido dada uma atenção significativa para a execução do sigilo da informação na camada física (PHY, do inglês *physical layer*). Com efeito, a segurança da camada física foi inicialmente introduzida por Wyner [3], através da apresentação do conceito de canais *wiretap*, que tem demonstrado ser uma estratégia eficaz para garantir um nível aceitável de sigilo em redes sem fio. Em [3], foi demonstrado que, quando o canal de comunicação entre o transmissor (Tx) e o nó malicioso é uma versão degradada do canal entre o Tx e o receptor legítimo (Rx), é possível garantir o sigilo na transmissão da informação. O trabalho de Wyner foi mais tarde estendido para canais *wiretap* Gaussianos em [4] e, desde então, inúmeros trabalhos foram propostos na literatura usando diferentes perspectivas. A variedade de possíveis modelos sistêmicos que utilizam diferentes configurações e técnicas de transmissão/recepção torna esta área sensível a uma gama de pesquisas ainda não abordadas na literatura.

1.2 Revisão da Literatura

Como mencionado na seção 1.1, desde a introdução do conceito de segurança na camada física apresentado por Wyner em [3], esta estratégia revolucionária ganhou muitos adeptos no campo da segurança em redes sem fio. Isso levou a diversas investigações assumindo padrões variados e diferentes pontos de vista. Alguns desses trabalhos são brevemente comentados a seguir.

Em [5, 6, 7, 8, 9], foi examinada a segurança da camada física usando uma abordagem sobre teoria da informação. Os autores em [5] investigaram um canal *broadcast* com desvanecimento assumindo mensagens confidenciais (BCC, do inglês, broadcast

confidential channels) e uma informação de estado do canal (CSI, do inglês, channel state information) perfeita entre o transmissor e os receptores. Em [5] foi mostrado que ter entradas independentes para cada subcanal é ótimo. Em [6], estabeleceu-se a região de capacidade de sigilo para os BCC paralelos, e foram obtidas as alocações ótimas de potência que alcançam o limite da região de capacidade de sigilo. O problema da comunicação secreta de um canal Gaussiano com múltiplas entradas e múltiplas saídas (MIMO, do inglês, *multiple-input and multiple-output*), foi investigado em [7], em que um transmissor possuía duas mensagens independentes que eram destinadas a um receptor. Em [7], foi provado que as duas mensagens podem ser transmitidas simultaneamente com suas respectivas taxas de sigilo máxima. Além disso, uma caracterização teórica da capacidade de sigilo de um canal MIMO *wiretap* foi apresentada em [8], enquanto em [9], foi assumido um cenário similar a [8], em presença de um nó malicioso. Ainda em [9], foi calculada a capacidade de sigilo perfeito com um número arbitrário de antenas no transmissor e receptor.

Por outra perspectiva, a probabilidade de *outage* de sigilo foi investigada em [10], em que foi apresentado um método que utiliza a diversidade do canal para aumentar a capacidade de sigilo em canais *wiretap*. Concluiu-se que, com a presença de diversidade espacial, um receptor pode conseguir uma capacidade de sigilo [1] relativamente elevada, mesmo em baixa razão sinal-ruído (SNR, do inglês, *signal-to-noise ratio*). Além disso, em [11], o desempenho de *outage* de sigilo foi examinado para um canal com múltiplas antenas no transmissor e uma única antena no receptor, em que o transmissor utiliza um esquema de seleção de antena (TAS, do inglês, *Transmit Antenna Selection*), enquanto que o nó intruso é equipado com múltiplas antenas. Verificou-se, que um aumento no número de antenas no Tx afeta positivamente a segurança do sistema, de modo que, altos níveis de segurança podem ser obtidos independentemente do número de antenas no nó intruso. Posteriormente, uma análise semelhante foi efetuada em [12], assumindo que todos os nós eram equipados com múltiplas antenas e se observando conclusões semelhantes. Os autores em [13] investigaram a capacidade de canais *wiretap* considerando um esquema de seleção de antena de transmissão TAS e diferentes esquemas de combinação de sinal no receptor, enquanto em [14], foi estudado o desempenho de *outage* assumindo TAS no Tx e uma combinação por seleção generalizada (GSC, do inglês, *generalized selection combining*) no Rx. Finalmente, em [15], um esquema TAS-Alamouti foi proposto para melhorar a segurança na camada física.

Em consonância com este ponto de vista, e a fim de aumentar a taxa de sigilo, vários trabalhos propuseram métodos que enviam sinais de interferência para o nó intruso, o que é conhecido como interferência cooperativa. Assim, o desempenho de sigilo inserindo ruído artificial em um canal *wiretap* MISO foi analisado em [16] considerando

[1] Define-se capacidade de sigilo como a diferença entre a capacidade do canal principal (i.e., transmissor e receptor) e a capacidade do canal secundário (i.e., transmissor e nó malicioso).

dois esquemas de transmissão: 1) um esquema de transmissão *on-off* com uma taxa de sigilo constante para todos os períodos de transmissão, e 2) um esquema de transmissão adaptativa com uma taxa de sigilo variável durante cada período de transmissão. Igualmente, em [17], assumindo um cenário em que o nó malicioso é limitado por interferências (isto é, desprezou-se o ruído), o desempenho de *outage* em canais *wiretap* com múltiplas antenas foi investigado e os resultados mostraram que o ganho de diversidade é igual ao valor mínimo entre o número de sinais de interferência e o produto do número de antenas no Tx e Rx. Do mesmo modo, em [18], uma estratégia de interferência cooperativa foi adotada usando os nós passivos da rede como nós de interferência. Trabalhos semelhantes a [18] podem ser encontrados em [19, 20], em que tanto o Rx quanto um nó interferente amigo, atacam o nó intruso com sinais de interferência. Além disso, a estratégia de envio de ruído artificial no espaço nulo do receptor foi tratada em [21, 22] (apenas o Tx envia ruído artificial) e em [23] (tanto o Tx quanto o Rx enviam ruído artificial). Utilizando esta estratégia, o desempenho de outage em canais MISO *wiretap* foi investigado em [24], supondo que o nó malicioso é afetado por ambos os sinais de interferência e ruído. No mesmo contexto da segurança na camada física, em [25] são investigadas técnicas robustas de otimização da taxa de sigilo para um canal *wiretap* MIMO com múltiplas antenas no nó intruso, assumindo que o transmissor tem uma CSI perfeita com o legítimo receptor e imperfeita com o nó intruso. Além disso, uma abordagem inovadora foi apresentada em [26], com a introdução do conceito de restrição espacial. Os autores em [26] analizaram a taxa de sigilo sem ter conhecimento do número exato de antenas no nó malicioso, sendo assumido que o nó intruso possui uma região espacial limitada para colocar um possível número infinito de antenas. De um ponto de vista prático, conhecer a restrição espacial é muito mais fácil do que saber o número de antenas no nó malicioso.

Comum aos trabalhos acima mencionados é a suposição de um *feedback* perfeito entre o Rx legítimo e o Tx. O conhecimento da CSI no Tx garante uma melhora importante na confiabilidade do canal, o que ajuda a alcançar um desempenho desejado através da aplicação de técnicas adaptativas para aumentar a taxa de transmissão e reduzir a potência de transmissão necessária. No entanto, de um ponto de vista prático, obter uma CSI perfeita é um processo inviável devido a erros de estimativa do canal e atrasos no *feedback*. Em [27], investigou-se o efeito do atraso no *feedback* sobre o desempenho de *outage* em canais MISO *wiretap* com desvanecimento Nakagami-m e utilizando um esquema TAS. Os resultados em [27] revelaram que, quando a CSI está desatualizada durante o processo de seleção de antena, o ganho de diversidade esperado não pode ser realizado. Uma conclusão similar foi alcançada em [28], em que utilizou-se uma técnica de transmissão por razão máxima (MRT, do inglês, *maximal-ratio transmission*) no Tx. Os efeitos prejudiciais de uma CSI desatualizada sobre o desempenho de *outage* em sistemas MIMO de dois saltos com *relay* amplifica-e-encaminha (AF, do inglês, *amplify-and-forward*) foi estudado em [29]. Os resultados revelaram que os atrasos de *feedback* nos canais *relay*-Tx

e/ou Rx-*relay* têm um impacto negativo significativo no desempenho do sistema. Um modelo sistêmico similar a [29] foi investigado em [30]. Em [30], assumindo transmissão por conformação de feixe (TB, do inglês, *transmit beamforming*) e seleção de *relay*, foi analisado o efeito conjunto de uma CSI desatualizada e os erros de estimação de canal (CEE, do inglês, *channel estimation errors*) no desempenho do sistema. Pesquisas mais recentes estudaram o desempenho de *outage* com *feedback* atrasado e/ou errôneo em canais MIMO *wiretap* utilizando a técnica TAS/MRC, e assumindo desvanecimento Rayleigh [31] e desvanecimento Nakagami-m [32], respectivamente. Em [31], foi adotada a melhor estratégia TAS e um único nó malicioso, enquanto em [32], foi assumido um esquema TAS de ordem geral e vários nós intrusos. Ambos os artigos concluíram que a ordem de diversidade é reduzida quando a CSI está desatualizada e não é limitada pelo número de antenas no nó malicioso, mesmo na presença de vários nós intrusos.

1.3 Motivação e Objetivos

Como discutido na seção 1.1, devido ao uso generalizado das redes sem fio, torna-se cada vez mais importante alcançar e manter um nível de segurança aceitável para garantir a integridade da informação. Na revisão da literatura realizada na seção 1.2, verificou-se a atenção especial de inúmeras investigações em torno da segurança na camada física. Destacam-se os estudos relacionados com a melhoria do desempenho de *outage* de sigilo através do método de envio de sinais de interferência para o nó intruso.

Assim, inúmeros trabalhos estudaram o desempenho de *outage* de sigilo assumindo diferentes configurações sistêmicas, além de múltiplos esquemas de seleção de antena no transmissor e técnicas de combinação de sinais no receptor e no nó intruso. Além disso, nestas análises foram assumidas diferentes condições de canal, às vezes ideais, a fim de facilitar cálculos matemáticos (CSI perfeita ou imperfeita). Alguns destes trabalhos são resumidos na Tabela 1.

Referência	**Canal**	**Técnica de Diversidade**	**CSI**	**Interferência Cooperativa**
[17]	MIMO	TAS/MRC-SC	Perfeita	sim
[24]	MISO	TAS/MRC	Perfeita	sim
[25]	MIMO	MRC	Perfeita	não
[27]	MISO	TAS/MRC	Imperfeita	não
[28]	MISO	MRT	Imperfeita	não
[31]	MIMO	TAS/MRC	Imperfeita	não
[32]	MIMO	TAS/MRC	Imperfeita	não

Tabela 1: Trabalhos que investigaram o desempenho de *outage* de sigilo com diferentes configurações.

Como observado na Tabela 1, até o momento, o desempenho de *outage* de sigilo em canais *wiretap*, assumindo que o nó malicioso seja afetado simultaneamente por sinais de interferência e ruído, não foi investigado na literatura ainda.

Em resposta à ausência de pesquisas anteriores considerando ambos parâmetros que influenciam o nó intruso, e pela necessidade de ter resultados mais próximo às condições naturais de um meio sem fio, esta dissertação tem como objetivo fornecer uma análise compreensiva do desempenho de *outage* de sigilo em canais MIMO *wiretap*, considerando uma CSI imperfeita e que o nó malicioso está sujeito a múltiplos sinais de interferência e ruído. Paralelamente, o cenário MISO é analisado como caso especial.
Como objetivos específicos deste trabalho de dissertação podem ser listados:

- Descrever o cenário a ser investigado, em que será considerado um sistema de canais *wiretap* com o Tx usando um esquema TAS, enquanto o Rx legítimo emprega as técnicas de combinação por seleção (SC, do inglês, *selection combining*) ou combinação por máxima razão (MRC, do inglês, *maximal-ratio combining*), enquanto o nó malicioso, adota apenas um esquema de MRC.
- Derivar as expressões analíticas exatas para a probabilidade de *outage* de sigilo em cada caso analisado.
- Realizar uma análise assintótica para determinar a ordem de diversidade do sistema, através da qual serão obtidos separadamente o ganho de diversidade (do inglês, *diversity gain*) e o ganho de *array* (do inglês, *array gain*).
- Estudar os efeitos dos principais parâmetros do sistema no desempenho de *outage*.

Em geral, e para responder aos objetivos planejados, as expressões analíticas exatas da probabilidade de *outage* de sigilo serão derivadas considerando CSI imperfeita (CSI perfeita será um caso particular do analisado), bem como sinais interferentes com uma distribuição de potências arbitrárias. Estas expressões serão simplificadas para dois casos especiais, assumindo padrões de distribuição de potências iguais ou distintas, respectivamente, nos sinais interferentes. Além disso, será realizada uma análise assintótica, com base na qual, serão determinados o ganho de diversidade e o ganho de *array*. Os resultados obtidos sugerem discussões interessantes sobre os efeitos dos parâmetros fundamentais do sistema no desempenho de *outage* de sigilo. Por exemplo, mostrar-se-á que, para todos os esquemas de combinação de sinais, o ganho de diversidade será dado pelo produto do número de antenas no Tx e no Rx legítimo quando é assumida uma CSI perfeita, enquanto o ganho de diversidade será reduzido apenas ao número de antenas no Rx legítimo quando é considerado um atraso no *feedback*. Em ambos os casos, a ordem de diversidade não será afetada pelo número de sinais de interferência, bem como pelo número de antenas no nó intruso. Estas observações contradizem as conclusões apresentadas em [17], em que foi mostrado que o ganho de diversidade não é afetado somente pelo número de antenas, mas também pelo número de sinais de interferência. Em outras palavras, nos casos práticos, é importante considerar a relação sinal-interferência mais ruído (SINR,

do inglês, *Signal-to-Interference-plus Noise Ratio*) em vez da relação sinal-interferência (SIR, do inglês, *Signal-to-Interference Ratio*) no nó intruso, a fim de obter resultados mais precisos. Além disso, mostrar-se-á que o número de antenas no nó malicioso (N_{E}), bem como o número de sinais interferentes M, afetam o ganho de *array* do sistema, ao aumentar o número de antenas no Tx. Mas, as alterações serão mais significativas para os valores mais elevados de N_{E} e/ou os valores menores de M. Finalmente, os resultados obtidos nesta dissertação também mostrarão que, quando N_{A} é igual a um, o número de sinais de interferência afeta mais o ganho de *array* do que o número de antenas no nó intruso (mantendo o mesmo número de antenas no Rx). Em outras palavras, para um cenário com $N_{\mathrm{A}} = 1$, o número de sinais de interferência tem um papel crucial em termos de ganho de *array*. No entanto, de forma interessante, aumentando o número de antenas no Tx para dois, o número de antenas no nó malicioso se torna mais influente no ganho de *array* do que o número de sinais de interferência. Até o momento, essas observações não foram relatadas na literatura ainda.

1.4 Estrutura do Trabalho

O restante desta dissertação está organizado da seguinte maneira:

- **Capítulo 2:** Neste capítulo, será apresentada a fundamentação teórica necessária para o entendimento da dissertação. Será fornecida uma caracterização de algumas das vantagens da utilização de sistemas MIMO, revisando alguns conceitos relevantes como os ganhos por diversidade espacial. Serão apresentados distintos esquemas de diversidade em recepção e transmissão. Além disso, será introduzida a estratégia de segurança da camada física.
- **Capítulo 3:** O modelo do sistema para um canal MIMO *wiretap* será apresentado neste capítulo. Além disso, será desenvolvido um equacionamento matemático que modela a probabilidade de *outage* de sigilo deste sistema para cada caso analisado. Uma análise assintótica com o intuito de determinar a ordem de diversidade do cenário proposto será desenvolvida. Em paralelo, serão obtidas as formulações e expressões fechadas para um canal MISO *wiretap*, como um caso especial do modelo descrito anteriormente, em que o transmissor possui múltiplas antenas, enquanto tanto o receptor legítimo quanto o nó intruso têm apenas uma antena.
- **Capítulo 4:** A apresentação dos resultados numéricos a fim de validar as expressões analíticas exatas e aproximadas que serão desenvolvidas no Capítulo 3 será realizada neste capítulo. De acordo com estes resultados, uma análise compreensiva do desempenho de *outage* de sigilo no sistema proposto será desenvolvida.
- **Capítulo 5:** Por último, as conclusões desta dissertação serão apresentadas neste capítulo. Além disso, serão apresentadas algumas perspectivas para trabalhos futuros.

1.5 Produção Científica

Os conteúdos e contribuições apresentados nesta dissertação de mestrado foram publicados e submetidos com as seguintes informações:

Artigos publicados:

ORTEGA, Y. R.; FERDINAND, N. S.; DA COSTA, D. B.; DE SOUSA, R. T.; DIAS, U. S., "**MISO TAS Wiretap Channels with Jamming and Noise at the Eavesdropper.**", 23rd International Conference on Telecommunications, Tessalônica, Grécia, Maio, 2016.

VASCONCELOS, L. M.; **ORTEGA, Y. R.**; DA COSTA, D. B.; DE SOUSA, R. T.; GIOZZA, W. F., "**PHY Security of MIMO Wiretap Channels with Generalized Selection Combining.**", XXXIV Simpósio Brasileiro de Telecomunicações e Processamento de Sinais (SBrT), Santarém, Pará, Setembro, 2016.

Artigos em Revisão:

ORTEGA, Y. R.; UPADHYAY, P. K.; DA COSTA, D. B.; BITHAS, P. S.; KANATAS, A. G.; DIAS, U. S.; DE SOUSA, R. T., "**Joint Effect of Jamming and Noise in Wiretap Channels with Multiple Antennas.**", Submetido em 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Espanha, Janeiro, 2017.

ORTEGA, Y. R.; UPADHYAY, P. K.; DA COSTA, D. B.; BITHAS, P. S.; KANATAS, A. G.; DIAS, U. S.; DE SOUSA, R. T., "**Joint Effect of Jamming and Noise in Wiretap Channels with Feedback Delay and Multiple Antennas.**", Submetido em Transactions on Emerging Telecommunications Technologies), Janeiro, 2017.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Introdução

Com o uso crescente de redes sem fio, paradigmas tradicionais no setor das comunicações como a qualidade de serviço (QoS, do inglês, *Quality of Service*) e a segurança tornaram-se fundamentais para a adoção desta tecnologia. Alcançar uma adequada QoS tornou-se um desafio pela crescente demanda de usuários e serviços que requerem taxas de transmissão cada vez maiores. Com relação à questão da segurança, os sistemas sem fio são especialmente vulneráveis em termos do sigilo da informação, por compartilhar o canal de comunicação com potenciais nós intrusos tentando decifrar a troca de dados entre os usuários legítimos da rede. Devido às suas características, o canal de rádio torna-se hostil para a transmissão devido ao desvanecimento gerado pela propagação por múltiplos percursos, o que degrada a qualidade e confiabilidade do canal e, portanto, a velocidade da comunicação. Além disso, o espectro de radiofrequências é um recurso li-

mitado, e inúmeros esforços são realizados para evitar a sua saturação. Neste contexto, assume particular importância a adoção de sistemas MIMO pelas possibilidades de atingir altas taxas de transmissão sem a necessidade de aumentar a potência de transmissão ou a largura de banda disponível. Ao contrário do que ocorre em sistemas de única entrada e única saída (SISO, do inglês, *single-input and single-output*) tradicionais, nos sistemas MIMO, mecanismos físicos de propagação tais como o espalhamento [33] ou a dispersão [34] podem proporcionar um aumento nas taxas de transmissão ou uma redução na taxa de erro. Outra vantagem dos sistemas MIMO é a sua capacidade de aumentar a eficiência espectral [35, 36], aproveitando as propriedades espaciais do canal por múltiplos percursos para obter uma alta eficiência.

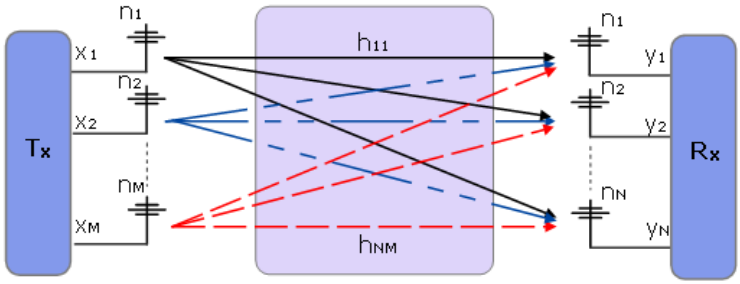
Neste capítulo será apresentada a fundamentação teórica que sustenta a pesquisa desenvolvida nesta dissertação. Na seção 2.2, será introduzida uma breve interpretação física dos sistemas MIMO. A origem dos ganhos e as vantagens introduzidas ao utilizar múltiplas antenas no transmissor e no receptor serão descritas na subseção 2.2.1; será dada especial atenção ao ganho de diversidade espacial (subseção 2.2.2) e o ganho de *array* (subseção 2.2.3), pela importância desses parâmetros no presente trabalho. Posteriormente, na seção 2.3, será realizada uma descrição da diversidade espacial na recepção, explicando o princípio de funcionamento de alguns dos principais esquemas para a exploração desta técnica. Uma análise similar é realizada na seção 2.4 detalhando a diversidade em transmissão e apresentando alguns dos esquemas mais utilizados para alcançar ganho por diversidade em transmissão. Finalmente, a possibilidade de alcançar e garantir um nível aceitável de segurança nas comunicações sem fio através de técnicas aplicadas na camada física da pilha de protocolos é introduzida na seção 2.5. Mais especificamente serão explicados conceitos importantes relacionados com a segurança da camada física, como o canal *wiretap*, a capacidade de sigilo e a interferência cooperativa.

2.2 Modelo do Sistema MIMO

A representação de um canal MIMO com M antenas de transmissão e N antenas de recepção (sistema MxN), em que se geram MN subcanais entre o *array* transmissor e o *array* receptor, é ilustrada na Figura 1.

Na Figura 1, cada um dos elementos $h_{ij}(\mathrm{t})$ representa o canal gerado entre a antena transmissora j, com $j \in \{1, \ldots, M\}$, e a antena receptora i, com $i \in \{1, \ldots, N\}$. Para simplificar o desenvolvimento, a dependência do tempo dos subcanais é removida, assumindo canais invariantes no tempo. A resposta ao impulso do canal MIMO representado pode ser expressa matricialmente como

Figura 1: Esquema MIMO MxN.



Fonte: Próprio autor.

$$\mathbf{H} = \begin{pmatrix} h_{11} & h_{12} & ... & h_{1M} \\ h_{21} & h_{22} & ... & h_{2M} \\ . & . & . & . \\ . & . & . & . \\ h_{N1} & h_{N2} & ... & h_{NM} \end{pmatrix} \tag{1}$$

É interessante ressaltar o caso em que o transmissor e o receptor encontram-se em um meio favorável para o espalhamento, assim os elementos da matriz **H** apresentam baixa correlação, fazendo com que o canal MIMO proporcione uma alta eficiência espectral.

Igualmente, os sinais recebidos podem ser descritos matematicamente como

$$\mathrm{y}_j = \sum_{i=1}^{M} h_{ji} x_i, \forall j \in \{1, \ldots, N\}. \tag{2}$$

2.2.1 *Ganhos nos Sistemas MIMO*

O desempenho de um canal MIMO é medido através da capacidade do canal, ou seja, a eficiência espectral máxima que o canal pode oferecer. A capacidade do canal depende apenas da SNR no receptor e da matriz do canal, independentemente do esquema de transmissão ou de codificação usado. No entanto, eficiências espectrais e taxas de transferência próximas à capacidade do canal somente são possíveis utilizando os esquemas de codificação e modulação apropriados. As altas taxas de transmissão dependem de diferentes fatores que podem melhorar os esquemas de transmissão, bem como a confiabilidade do enlace.

Entre as técnicas utilizadas para melhorar os esquemas de transmissão encontra-se a multiplexação espacial, na qual, com múltiplas antenas são gerados subcanais para-

lelos que podem ser utilizados para a transmissão de fluxos de informação independentes. A melhoria obtida com esta técnica é conhecida como ganho de multiplexação espacial. Por outra parte, existem fatores que melhoram as características do canal MIMO, minimizando a probabilidade de erro e melhorando a SNR no receptor. Isto permite alcançar altas taxas de transmissão através de esquemas de codificação mais eficientes, reduzir a potência de transmissão ou aumentar o alcance. Entre estas técnicas destaca-se a codificação espaço-temporal, que introduz o ganho de diversidade espacial, bem como o ganho de *array*, através da combinação do sinal em transmissão e/ou recepção.

Devido à importância destes conceitos nesta dissertação, a seguir serão descritos o ganho de diversidade, o ganho de *array*, assim como a contribuição destes parâmetros para a melhoria dos sistemas MIMO.

2.2.2 *Ganho de Diversidade*

O desempenho de um canal MIMO pode ser melhorado atenuando os desvanecimentos e/ou diminuindo a probabilidade de erro do sistema, o que acontece ao transmitir ou receber por várias antenas ao mesmo tempo. Assumindo que os MN enlaces do canal MIMO sofrem desvanecimento independente entre eles e o sinal transmitido é construído de um modo adequado, o receptor pode combinar os sinais recebidos e compensar os desvanecimentos de um canal SISO tradicional, melhorando a SNR do sinal recebido resultante. A melhora da SNR média no tempo, com respeito à SNR do melhor canal SISO possível é conhecida como ganho de diversidade (G_{D}).

Em um ambiente de desvanecimento geral, não pode ser garantido nenhum nível mínimo de SNR no receptor em um intervalo longo de tempo independentemente da potência de transmissão utilizada [37]. No entanto, é possível ajustar a potência de transmissão de tal modo que a SNR no receptor seja inferior a um especificado limiar somente com uma determinada probabilidade. Esta probabilidade é conhecida como probabilidade de *outage* de sigilo (P_{out}), e indica a probabilidade que o sistema não esteja disponível. A SNR do nível de *outage* está associada com a capacidade do canal através da fórmula de Shannon [37]

$$C_{\mathrm{out}} = B\log_{10}(1+\gamma_{\mathrm{out}}) \tag{3}$$

em que B denota a largura de banda, γ_{out} representa a SNR do nível de *outage* e C_{out} indica a capacidade de *outage* de sigilo, que pode ser garantida com uma probabilidade $(1-P_{\mathrm{out}})$.

O ganho de diversidade está estreitamente relacionado com o conceito de desempenho de *outage* de sigilo, o qual é descrito através da probabilidade de *outage* de sigilo do canal. Matematicamente, o ganho de diversidade pode pode ser obtido do ponto

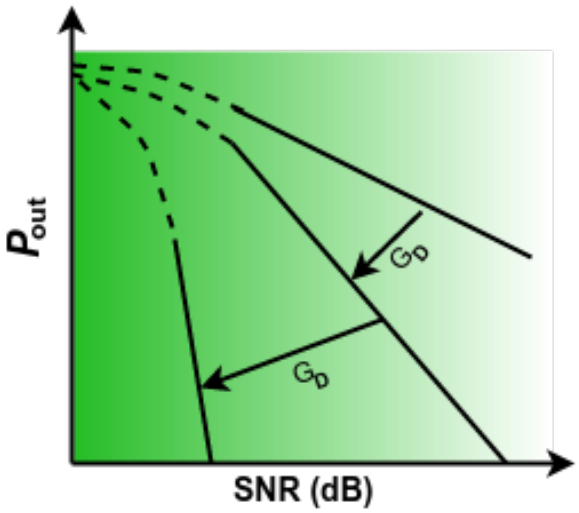
de vista da probabilidade de erro. Por exemplo, em [38] o ganho de diversidade é obtido a partir de

$$\lim_{\mathrm{SNR}\to\infty} \frac{logP_e(\mathrm{SNR})}{log(\mathrm{SNR})} = -d \tag{4}$$

em que P_e denota a probabilidade de erro e d representa o ganho de diversidade. Perceba que a probabilidade de erro decai com SNR^{-d}, enquanto em um sistema SISO decai 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. Por conseguinte, 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, em (4), $d_{max} = MN$.

Além disso, o ganho de diversidade pode ser determinado através de um gráfico em uma escala logarítmica de P_{out} versus SNR, em que a ordem de diversidade é obtida calculando a inclinação da curva, como ilustrado na Figura 2.

Figura 2: Ganho de diversidade na recepção.



Fonte: Próprio autor.

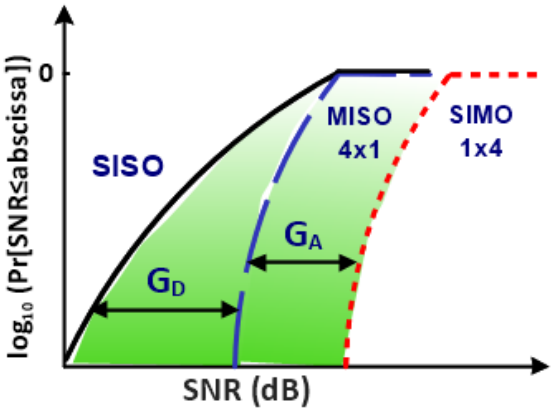
No caso de um sistema assumindo um nó malicioso na rede, a probabilidade de *outage* de sigilo pode indicar igualmente a probabilidade do nó intruso interceptar a troca de informações entre o transmissor e o receptor legítimo. Por conseguinte, o ganho de diversidade é determinado pelo valor mínimo da SNR tomada como referência.

2.2.3 *Ganho de Array*

O ganho de *array* acontece através do processamento do sinal, ao combinar coerentemente o sinal no transmissor e/ou receptor, obtendo-se um aumento na SNR

média no receptor. Em [39], o ganho de *array* é definido como o valor médio da potência recebida em um sistema MIMO em relação à potência recebida em um sistema SISO. O ganho de *array* é também conhecido como ganho de conformação de feixe ou *beamforming* [40], em que, com o auxílio de um arranjo de antenas, são considerados os pesos do sinal transmitido/recebido por cada antena. Assim, para realizar a combinação dos sinais é necessário conhecer a CSI no transmissor e/ou receptor para obter os pesos.

Figura 3: Ganho de diversidade e ganho de *array* na recepção.



Fonte: Próprio autor.

Conhecer a CSI no receptor através de sequências de treinamento é possível, mas é um processo difícil devido a um canal *feedback* ser necessário. Assim, para um canal MIMO $M \times N$ são comuns dois tipos de sistemas: de laço aberto (sem *feedback*), e de laço fechado (com *feedback*). Por exemplo, ao utilizar uma técnica de combinação de sinal MRC [2] no receptor, os sistemas de laço fechado proporcionam um ganho de *array* de $10\log_{10}MN$, enquanto que, assumindo um sistema de laço aberto, o ganho de *array* é $10\log_{10}N$. Por outro lado, em recepção, o ganho de diversidade e o ganho de *array* de um sistema estão inter-relacionados. Como representado na Figura. 3, enquanto o ganho de diversidade de um sistema $M \times 1$ é similar a um sistema $1 \times M$, este último fornece um ganho de *array* de $10\log_{10}M$.

2.3 Diversidade Espacial na Recepção

A diversidade espacial na recepção é uma técnica desenvolvida com o objetivo de combater os desvanecimentos gerados pelos múltiplos percursos e melhorar a SNR no receptor. A diversidade espacial é uma estratégia amplamente estudada e tem provado a sua eficácia, tornando esta técnica uma das mais utilizadas nas comunicações sem fio. Ela requer múltiplas antenas espaçadas a uma distância predefinida. Cada antena recebe uma réplica gradual do sinal transmitido. Assim, quando a separação entre as antenas receptoras é suficiente, o desvanecimento experimentado por cada canal será independente,

[2] O esquema MRC será analisado detalhadamente na Secção 2.3.2

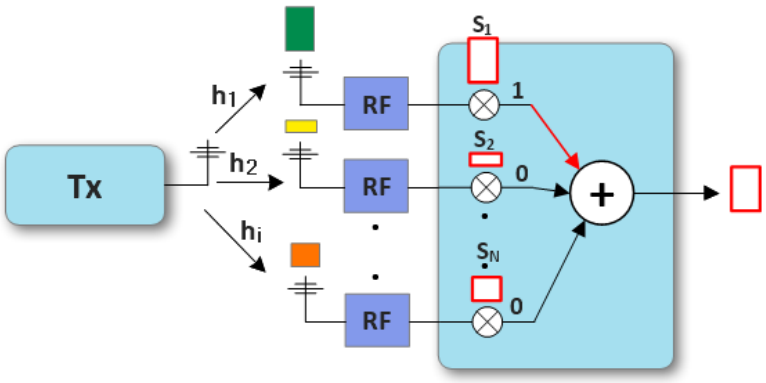
o que aumenta a probabilidade de que os sinais recebidos não experimentem um desvanecimento simultâneo. Em [41], foi mostrado que quando os coeficientes de correlação em potência entre os canais são de até 0,7, um sistema de diversidade vai proporcionar uma melhora significativa em relação a um sistema sem diversidade. Assim, o sucesso de um sistema com diversidade vai depender do grau de correlação entre os diferentes ramos.

Várias técnicas tem sido desenvolvidas para combinar os sinais recebidos nas antenas receptoras, e obter um sinal resultante de qualidade. A seguir, serão descritas as técnicas que serão utilizadas posteriormente na presente pesquisa.

2.3.1 *Combinação por Seleção (SC, Selection Combining)*

A combinação por seleção (SC) é um esquema que utiliza algoritmos simples, com poucos requerimentos de processamento do sinal, em que só o sinal com melhor SNR é selecionado, ou seja, a SNR de saída é igual à SNR máxima de todos os ramos, como representado na Figura 4.

Figura 4: Esquema de Combinação por Seleção (SC).



Fonte: Próprio autor.

Portanto, o sinal y_{SC} na saída do combinador, vai ser o conjunto de dados transmitido pelo melhor enlace, e é dada por

$$y_{SC} = S_i^* | h_i^* > h_i, \forall i \in \{1, \ldots, N\}. \tag{5}$$

em que S_i representa a i-ésima entrada no combinador e h_i representa o canal gerado entre a antena transmissora e a antena receptora i, com $i \in \{1, \ldots, N\}$. Assim, o canal equivalente vai ser

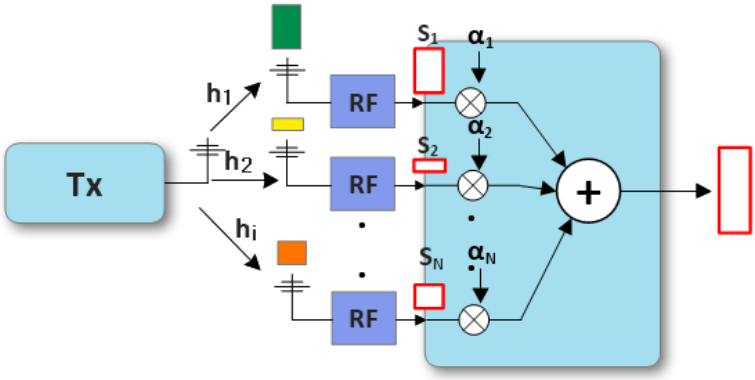
$$h_{SC} = max\,(h_i) \tag{6}$$

Na prática, é usado o sinal no qual a soma das potências do sinal e o ruído seja máxima [42]. Assim, será necessária a utilização de um receptor em cada antena para o monitoramento da SNR em cada um dos ramos continuamente, e em que somente um receptor será comutado para ativo. Além disso, a combinação por seleção, não precisa de uma sincronização de fase entre os sinais de cada ramo, e embora a máxima potência não seja alcançada constantemente, é observada uma melhoria em relação ao uso de uma antena [43].

2.3.2 *Combinação por Razão Máxima (MRC, maximal-ratio combining)*

O método de combinação por razão máxima (MRC) escolhe pesos para cada um dos sinais recebidos em cada antena e os combina coerentemente de forma a maximizar a SNR do sinal resultante na saída. Basicamente, os ramos com SNR maiores serão ponderados com valores maiores, e valores menores serão atribuídos aos ramos com SNR menores, resultando em um sinal na saída com uma soma ponderada de todos os ramos, como mostrado na Figura 5.

Figura 5: Esquema de Combinação por Razão Máxima (MRC).



Fonte: Próprio autor.

Na Figura 5, S_i representa a i-ésima entradas no combinador, e α_i são os pesos atribuídos a cada entrada. Assim, cada entrada S_i com $i \in \{1, \ldots N\}$, pode ser expressa como

$$\mathrm{S}_i = x\mathrm{h}_i e^{j\theta_i}, \tag{7}$$

em que x representa o sinal transmitido, e $\mathrm{h}_i e^{j\theta_i}$ é a resposta ao impulso do canal entre a antena de transmissão e a i-ésima antena receptora. Os sinais de cada ramo S_i são adicionados em conjunto, em que o ganho de cada ramo é feito proporcional ao nível de sinal quadrático médio (RMS, do inglês, *root mean square*) e inversamente proporcional

ao nível de ruído quadrático médio nesse canal [45]. Assim, são utilizadas diferentes constantes ou pesos de proporcionalidade (α_i) para cada canal, que serão do tipo

$$\alpha_i = \frac{\mathrm{h_i^*}}{n^2}, \tag{8}$$

em que n^2 denota a potência de ruído e $(\cdot)^*$ representa o conjugado complexo. A operação conjugado complexo é necessária para a sincronização de fase de todas as entradas, a ser incluída nos pesos α_i. Finalmente, o sinal resultante na saída do combinador é uma soma de todas as entradas ponderadas, e pode ser representado matematicamente como

$$\mathrm{y_{MRC}} = \sum_{i=1}^{N} \alpha_\mathrm{i} \mathrm{S_i}, \tag{9}$$

Em relação à SNR obtida na saída do combinador, a SNR média é equivalente à SNR média em um ramo multiplicada pelo número de ramos. Isto é

$$\mathrm{SNR} = \sum_{k=1}^{N} \mathrm{SNR}_k = N\tau$$

em que τ representa a SNR média em um ramo.

2.3.3 *Outros Esquemas de Combinação na Recepção*

Existem outras técnicas para combinar os sinais no receptor e obter um sinal melhorado. A seguir, serão brevemente mencionadas algumas destas técnicas, pela oportunidade de ser usadas em trabalhos futuros com o mesmo raciocínio utilizado nesta dissertação.

Uma variante do método de combinação por seleção é introduzida em [44], em que o sinal com maior SNR é selecionado e mantido sem realizar mais explorações, até a SNR cair abaixo de um determinado limiar, momento no qual, é selecionada de novo a antena com melhor SNR recebida. Esta variante é conhecida como combinação por chaveamento e fixação (SSC, do inglês, *Switch-and-Stay Combining*).

Outra técnica é a combinação de seleção por limiar (TSC, do inglês, *threshold selection combining*). Ela foi implementada para resolver o problema da necessidade de múltiplos receptores dedicados. Baseia-se em varrer sequencialmente cada ramo, e selecionar o primeiro ramo com SNR acima de um determinado limiar. A seleção se mantém enquanto a SNR se mantiver acima do limiar, e só vai escolher um outro ramo quando a SNR do primeiro ramo selecionado atingir o limiar estabelecido. A sincronização de fase entre os ramos é desnecessária nesta técnica.

A combinação por ganho igual (EGC, do inglês *equal gain combining*) é um

método com um princípio de funcionamento similar ao MRC, mas com menor complexidade na sua implementação. Com a utilização de EGC não são necessários controladores adaptativos (amplificadores/atenuadores). Além disso, nenhuma estimativa de amplitude do canal é necessária, ao contrário do esquema MRC. No entanto, a sincronização de fase de todas as entradas é necessária para evitar o cancelamento do sinal. Diferente ao método MRC, EGC utiliza pesos fixos com amplitude unitária, independentemente da amplitude do sinal, não sendo utilizada a SNR como parâmetro [45]. Uma vez que todos os pesos são iguais, a combinação dos sinais degrada a SNR em relação com o caso MRC, sendo mais visível esta redução no desempenho quando um dos sinais tem uma SNR baixa. A melhoria média da SNR do método EGC é tipicamente cerca de 1 dB pior do que com MRC, mas ainda muito melhor do que sem diversidade.

Combinação por seleção generalizada (GSC, do inglês, *generalized selection combining*) é um método em que são combinados os sinais de um subconjunto dos ramos disponíveis. Uma alteração no tamanho do subconjunto pode alterar o desempenho e a complexidade do receptor. Em [46], foi provado que reduzindo o número de ramos de combinação de diversidade é possível uma redução no consumo de potência e na complexidade dos RF no receptor. Igualmente, quando os ramos com menor SNR são excluídos do processo de combinação, GSC pode ser uma técnica robusta em minimizar os erros de estimativa [47].

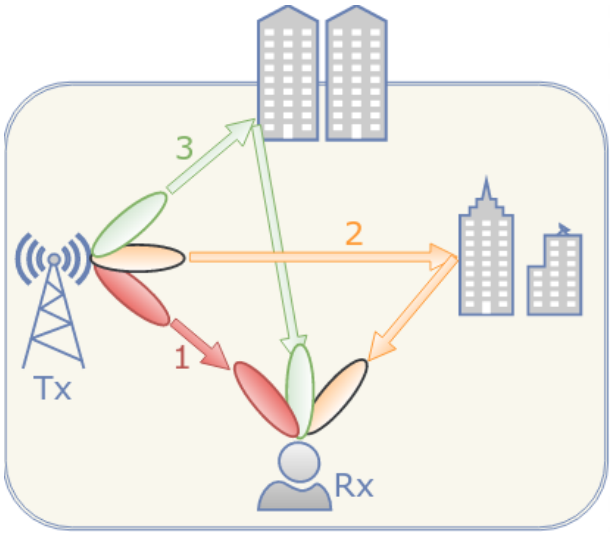
Pode-se concluir que dos esquemas de combinação de diversidade em recepção descritos, em geral, a máxima SNR é obtida através do método MRC, produzindo um sinal resultante com uma SNR média igual à soma das SNR individuais de cada ramo. Os esquemas de mais fácil implementação são SC e TSC. Além disso, o método EGC alcança altos desempenhos tendo todos os sinais uma fase comum de referência, o que permite uma soma construtiva dos sinais, embora a soma do ruído torne-se destrutiva. Finalmente, com a técnica GSC pode-se minimizar a complexidade dos módulos RF no receptor, mantendo um desempenho aceitável.

2.4 Diversidade Espacial na Transmissão

Similar à diversidade na recepção, o objetivo fundamental da diversidade na transmissão é reduzir os desvanecimentos. As técnicas de diversidade espacial na transmissão e recepção podem coexistir em um mesmo cenário como representado na Figura 6, aumentando o ganho de diversidade do sistema.

No entanto, alcançar um ganho por diversidade na transmissão na prática torna-se uma estratégia muito mais complexa que no caso do receptor, devido à necessidade de um processamento em transmissão e recepção para separar os sinais recebidos, que são combinados espacialmente antes de chegar ao receptor. Além disso, a diversidade na transmissão precisa em muitas ocasiões de um canal de *feedback*, através do qual

Figura 6: Diversidade na transmissão e recepção.



Fonte: Próprio autor.

o transmissor conheça a CSI do canal com o receptor, e assim possa adotar a melhor estratégia possível e maximize o ganho por diversidade para essa CSI.

Desde o esquema proposto por Wittneben [48], múltiplos métodos para alcançar ganho de diversidade na transmissão tem sido estudados. Em [48], uma das primeiras técnicas consistia em um sistema com duas antenas transmissoras, em que um símbolo era transmitido por uma das antenas, e uma réplica do mesmo, retardada em um tempo de símbolo, era transmitida pela outra antena aumentando artificialmente os múltiplos percursos. Esta estratégia tinha como desvantagem utilizar dois tempos de símbolos para transmitir um único símbolo, sendo a taxa de código de $\frac{1}{2}$. No entanto, a perda de eficiência espectral era mitigada com o uso de esquemas de modulação mais eficientes, ao melhorar a confiabilidade do enlace. A seguir, serão detalhadas algumas das técnicas mais utilizadas para alcançar ganho por diversidade em transmissão.

2.4.1 *Seleção de Antena de Transmissão (TAS, do inglês, transmit antenna selection)*

Um dos maiores inconvenientes da diversidade em transmissão nos sistemas de múltiplas antenas é precisar de uma alta complexidade no equipamento com altos custos. O método TAS tem a vantagem de ser o mais fácil de implementar por causa da sua simplicidade, reduzindo o consumo de energia do sistema e o número de cadeias de rádio frequência (RF) utilizadas, o que melhora a relação custo-benefício [49, 50]. Basicamente, a estratégia TAS consiste no receptor informar ao transmissor um conjunto de possíveis antenas a serem utilizadas para transmitir o próximo conjunto de dados, baseado na SNR instantânea do sinal recebido.

Embora MIMO possa aumentar a capacidade e confiabilidade do sistema, al-

cançar um ganho significa aumentar as cadeias de RF no transmissor e receptor, respectivamente. Por exemplo, um sistema com M antenas no transmissor e N antenas receptoras, requer M cadeias completas de RF no transmissor e N cadeias completas de RF no receptor. Além de precisar de amplificadores, conversores abaixadores e conversores analógico-digital no transmissor e receptor, ao aumentar o número de cadeias de RF o custo do sistema aumenta consideravelmente. Além disso, ao introduzir um maior número de elementos aumenta-se a complexidade para calcular o *feedback* e conhecer a CSI do canal. Como o preço das antenas que se conectam às cadeias de RF é bem menor, o objetivo do método TAS é implementar um número maior de antenas do que de cadeias RF, e utilizar somente um subconjunto delas. Isto é, em um sistema TAS tem-se M antenas transmissoras e L_t cadeias de RF, $L_t \leq M$.

Por outro lado, TAS requer apenas uma pequena fração da CSI para funcionar corretamente. São necessários apenas $L_t log(M)$ bits de informação de *feedback* para utilizar TAS [51]. Infelizmente, na prática, o processo de obter a informação de *feedback* pode se atrasar e o sistema agir com informação de canal desatualizada, fazendo com que o transmissor não escolha a antena corretamente, alterando o desempenho do sistema. Por exemplo, quando o canal entre o transmissor e o receptor tem baixa correlação, isto é, muda rapidamente, a CSI que chega ao transmissor pode ser totalmente desatualizada, aumentando a existência de erros no canal de *feedback*. Para minimizar o problema da taxa de erro de símbolo (SER, do inglês, *symbol error rate*) e maximizar a capacidade do canal, têm sido estudados e concebidos vários algoritmos de TAS, sendo um dos mais eficazes o apresentado em [52].

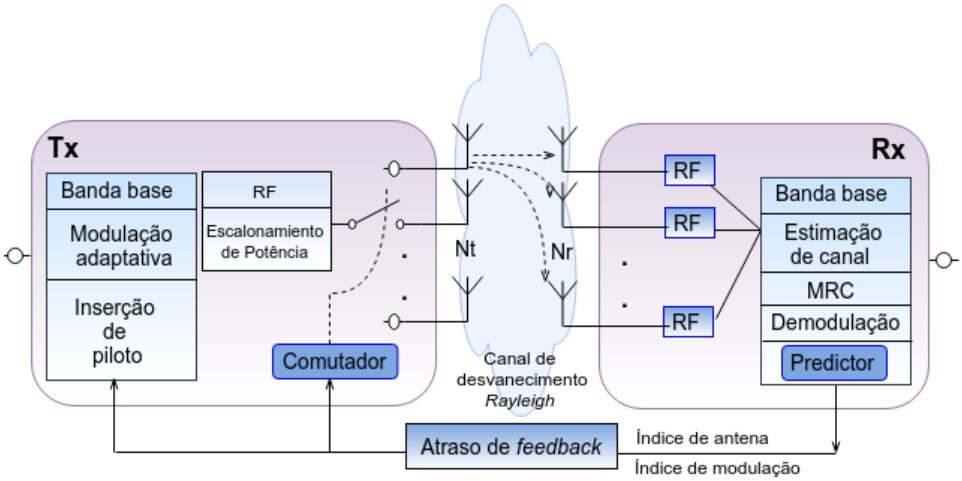
Em [52], um sistema com seleção de subconjunto de antenas foi proposto, em que N_t e N_r, representaram o número de antenas disponíveis em transmissão e recepção, respectivamente. Por sua vez, o número de antenas selecionadas em transmissão e recepção, foram denotadas como L_t e L_r, respectivamente. Foi provado que para selecionar as antenas de transmissão, $\binom{N_t}{L_t}$ combinações têm de ser verificadas. No caso das antenas selecionadas em recepção, a capacidade do canal tem de ser calculada para as $\binom{N_r}{L_r}$ possíveis combinações.

Uma variante mais recente foi apresentada em [53], como mostrado na Figura 7. Em [53], foi acrescentada modulação adaptativa (AM, do inglês, *Adaptive Modulation*) em um sistema TAS com esquema MRC no receptor, em que de acordo com as variações do canal, foram adaptadas as taxas de transmissão de dados e a profundidade de modulação do sistema.

2.4.2 *Códigos Espaço-Temporais (ST, do inglês, space-time codes)*

O método da codificação espaço-temporal tem como principal objetivo aproveitar os desvanecimentos do canal MIMO e minimizar os error introduzidos pelo canal.

Figura 7: TAS com modulação adaptativa e MRC .



Fonte: [53].

É possível diminuir a taxa média de erro do canal MIMO através da geração de códigos espaço-temporais adequados, o que resulta em uma maximização do ganho por diversidade espacial [54]. A finalidade desta técnica é introduzir correlação entre os sinais transmitidos desde várias antenas em diferentes períodos de tempo, de modo que a codificação é realizada tanto no espaço quanto no tempo [42].

Assim, a codificação espaço-temporal consegue diversidade espacial em transmissão sem a necessidade de aumentar a largura de banda. Outras vantagens do método são a possibilidade de se combinar com a técnica de codificação de canal, obtendo assim ganho por codificação e não precisar conhecer a CSI do canal no transmissor. Uma característica importante desta estratégia é não precisar de múltiplas antenas no receptor, tornando este método útil em sistemas com receptores leves de baixa complexidade. Além disso, os códigos espaço-temporais provaram ser muito eficazes em condições de funcionamento desfavoráveis, como efeito *Doppler* ou com erros na estimativa do canal. Vários esquemas de codificação espaço-temporal têm sido propostos, baseados fundamentalmente nos conceitos de códigos de bloco (BC, do inglês, *ST-Block Codes*) [55, 56] e códigos de treliça (TC, do inglês, *ST-Trellis Codes*) [57], os quais serão descritos a seguir.

2.4.3 *Codificação Espaço-Temporal de Bloco (STBC)*

A codificação espaço-temporal de bloco é realizada através do mapeamento de um bloco de símbolos de entrada no domínio do espaço e do tempo, criando sequências ortogonais transmitidas a partir de diferentes antenas. Nesta estratégia, o receptor é constituído por uma etapa em que o canal é estimado, outra fase em que são combinados os sinais, e a etapa final de verossimilhança. Foi proposta inicialmente por Alamouti para sistemas 2x1 e 2x2 em [55], e generalizada por Tarokh [56] para sistemas MxN.

O código de Alamouti é amplamente utilizado pela simplicidade e eficácia.

Neste esquema, dois símbolos diferentes δ_1 e δ_2 são transmitidos ao mesmo tempo, no primeiro período de símbolo, pelas antenas transmissoras 1 e 2, respectivamente. Em seguida, são transmitidos pelas as mesmas antenas, no segundo período de símbolos, os símbolos δ_1^* e δ_2^*, sendo δ^* o complexo conjugado de δ. Durante este processo, é assumido um canal plano em frequência, em que cada subcanal é uma variável aleatória Gaussiana com média igual a zero e variância unitária, independente e identicamente distribuída. Algumas das vantagens do método são: a não necessidade de um canal de *feedback* para fornecer diversidade e possuir uma taxa de código unitário, embora, quando a ordem de diversidade do sistema aumenta, a taxa de código diminua. Além disso, esta técnica não introduz ganho por codificação, ao contrário da técnica de codificação espaço-temporal de treliça a ser descrita a seguir.

2.4.4 *Codificação Espaço-Temporal de Treliça (STTC)*

No método de codificação espaço-temporal de treliça os símbolos são codificados na antena transmissora e a decodificação é realizada utilizando um decodificador de máxima verossimilhança (ML, do inglês, *maximum likelihood*). É um esquema eficaz, ao combinar o ganho por codificação obtido da codificação para correção de erros (FEC, do inglês, *forward error correction*), com o ganho de diversidade, fornecendo ganhos significativos no desempenho do sistema. Como desvantagem, a técnica necessita de um processamento adicional, que aumenta exponencialmente conforme a eficiência espectral e a ordem de diversidade [56].

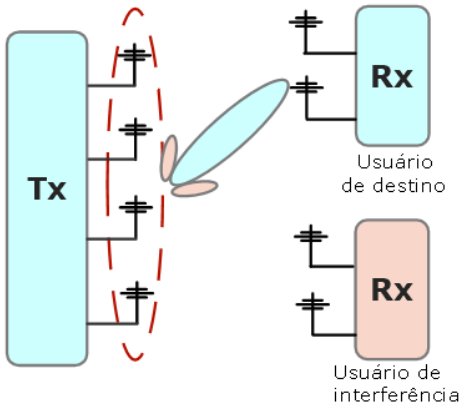
2.4.5 *Beamforming*

A conformação de feixe ou *beamforming*, embora seja uma técnica aplicada na transmissão, é geralmente associada ao ganho de *array*, e não direitamente à diversidade espacial na transmissão. O método de *beamforming* tradicional, baseia-se na estimativa da direção de chegada (DOA, do inglês, *direction of arrival*) de fase de *array* de feixes e no cálculo dos pesos do *beamforming*. Usualmente, os feixes são formados com base na matriz de coeficientes de canal e são usados para obter os pesos de *beamforming*.

Com o uso da tecnologia de *beamforming* pode ser alcançado ganho de *array* e ganho de redução da interferência co-canal. Ao ponderar os fluxos do sinal, o *beamforming* forma feixes de ondas estreitas que apontam para a direção de um usuário de destino específico, suprimindo o sinal de interferência de outros usuários do sistema, como mostrado na Figura 8. Esta característica causa ganho de *array* e ganho de redução da interferência co-canal, mas não causa ganho de diversidade e/ou multiplexação, ao transmitir apenas um fluxo de dados de cada vez.

Em geral, existem duas maneiras de implementar um sistema *beamforming*, uma baseada em um único conjunto de antenas, como na Figura 8, e outra com base em

Figura 8: Sistema *beamforming*.



Fonte: Próprio autor.

subconjuntos de *array* de antenas.

O método de *beamforming* e as técnicas de diversidade na transmissão em um mesmo sistema podem representar um equilíbrio entre o ganho de *array* e o ganho de diversidade. Em [58], demonstrou-se que, para um determinado número de antenas transmissoras, pode-se optar por colocar as antenas juntas para formar um *beam*, ou colocá-las longe e usar diversidade na transmissão. Por exemplo, em um sistema com condições ideais, com desvanecimento não-correlacionado ou sem *handoff*, o método de diversidade na transmissão tem vantagem em relação ao *beamforming*. Em contraste, em condições de *handoff*, a técnica de *beamforming* tanto tem ganho de *array* quanto ganho de diversidade, melhorando o desempenho do sistema em relação à diversidade em transmissão. Em geral, o desempenho relativo da diversidade na transmissão e do *beamforming* vai depender da combinação particular de condições presentes no sistema analisado.

2.5 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 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 [1]. Com o desenvolvimento tecnológico, a capacidade de processamento dos nós intrusos tem crescido exponencialmente, aumentando a probabilidade de obter a chave de encriptação através da exploração das múltiplas combinações possíveis. Portanto, preservar o sigilo da informação baseado unicamente na estratégia da criptografia tem se baseado em sistemas cada vez mais complexos para neutralizar a capacidade

dos nós maliciosos e não se tornarem obsoletos.

Em anos recentes, surgiu como solução ou complemento, a possibilidade da execução do sigilo da informação na camada física. Baseadas na premissa introduzida por Wyner em [3], em que foi apresentado o conceito de canais *wiretap*, 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 encriptação é realizada em camadas superiores independentes da camada física, ambas as estratégias podem funcionar simultaneamente, surgindo sistemas com uma abordagem multi-camadas 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.

2.5.1 *Capacidade de Sigilo*

No canal *wiretap* proposto por Wyner [3], foi estabelecida uma comunicação entre dois usuários legítimos através de um canal principal (canal Tx-Rx), enquanto um nó malicioso tinha acesso às versões degradadas das saídas do canal que chegam ao receptor legítimo. O conceito de canal *wiretap* foi mais tarde generalizado em [4], em que foram assumidos canais AWGN. Em [59], adotou-se um modelo sistêmico similar à [4], com potências de ruído N_p e N_w para o canal Tx-Rx e o canal *wiretap*, respectivamente. Em [59], $N_w > N_p$, isto é, a SNR do canal Tx-Rx Gaussiano é maior do que a SNR do canal *wiretap* Gaussiano, sendo a condição para alcançar a confidencialidade da informação. Neste cenário, a potência é limitada de acordo com

$$\frac{1}{n}\sum_{i=1}^{n} E[|X(i)|^2] \leq P, \tag{10}$$

em que n denota o número de canais, $E[\cdot]$ denota o valor esperado, $X(i)$ representa o sinal transmitido e P corresponde à potência média do sinal transmitido. Logo, a capacidade de sigilo é definida como a taxa de transmissão máxima na qual o nó intruso é incapaz de decodificar qualquer informação transmitida [8], e é igual à diferença entre as capacidades do canal Tx-Rx e o canal *wiretap*, respectivamente, como

$$C_s = C_p - C_w, \tag{11}$$

em que

$$C_p = B \log_{10} \left(1 + \frac{P}{N_p}\right) \tag{12}$$

e

$$C_w = B \log_{10} \left(1 + \frac{P}{N_w}\right). \tag{13}$$

Um método interessante foi apresentado em [10], utilizando a diversidade espacial do canal para aumentar a capacidade de sigilo do sistema. Em [10], foi demonstrado que, em presença de diversidade de canal, é possível atingir capacidades de sigilo relativamente elevadas no receptor, mesmo para baixas SNRs, introduzindo uma análise teórica do efeito da probabilidade de *outage* sobre a capacidade de sigilo do sistema. Neste cenário, adotando um canal MIMO e empregando uma técnica de combinação de diversidade MRC no receptor legítimo, a capacidade do canal Tx-Rx (C_p) pode ser melhorada, o que pode levar a um aumento da capacidade de sigilo (C_s) e da segurança do sistema. Além disso, pode-se diminuir ligeiramente a potência de transmissão para reduzir a capacidade do canal *wiretap* (C_w), e ainda manter um nível aceitável de C_p através do aproveitamento da diversidade espacial. Igualmente, outro possível mecanismo para aumentar a capacidade de sigilo foi proposto em [10], em que, com a utilização de múltiplos nós *relay* na rede, são obtidos múltiplos percursos entre o Tx e o Rx a fim de maximizar o efeito da diversidade espacial em recepção. Com este método, e utilizando um protocolo de controle de acesso adequado, foi constatado que o Rx legítimo tem maior capacidade de adquirir os enlaces cooperativos que o nó malicioso.

2.5.2 *Interferência Cooperativa*

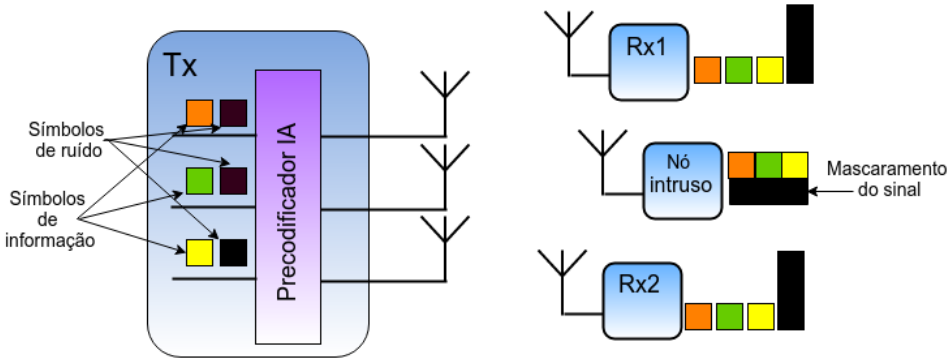
As estratégias para alcançar e preservar o sigilo da informação na camada física são variadas. Um dos métodos mais estudados é a interferência cooperativa, que consiste no envio de sinais de interferência para o nó malicioso. Para o envio dos sinais interferentes

podem ser utilizados unicamente nós passivos presentes na rede [18], conhecidos como nós amigos, ou o caso em que tanto o Rx legítimo quanto um nó interferente amigo enviam sinais de interferência para o nó intruso [19, 20]. 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 [60]. No entanto, é difícil conhecer perfeitamente a CSI do canal Tx-Rx, devido à presença do erro de estimativa da CSI. Na prática, a adoção de uma CSI obsoleta pelos nós legítimos da rede, resulta em que o ruído artificial transmitido não esteja perfeitamente no espaço nulo do canal Tx-Rx, e desta forma certa interferência será recebida no Rx legítimo.

Além disso, a estratégia de envio de ruído artificial no espaço nulo do receptor tem sido apresentada em cenários sem a presença de nós passivos na rede, chamada transmissão de ruído artificial. Como variantes desta técnica, apenas o Tx envia ruído artificial [21, 22], ou tanto o Tx quanto o Rx enviam ruído artificial [23]. Na prática, quando o número de receptores legítimos excede o número de antenas de Tx, não é possível usar a transmissão de ruído artificial devido à impossibilidade de encontrar o espaço nulo para todos os vetores de canal simultaneamente. Surge então a técnica conhecida como alinhamento de interferência (IA, do inglês, *interference alignment*), o que resulta em alinhar o ruído nos receptores legítimos. Na Figura 9 mostra-se um sistema com múltiplas antenas no Tx (N_t) que utiliza a técnica de transmissão por IA.

Figura 9: Alinhamento de ruído artificial.



Fonte: Próprio autor.

Conforme mostrado na Figura 9, o Tx transmite uma superposição de símbolos de informação e ruído. Nos receptores legítimos, os símbolos de informação ocupam $(1 - 1/N_t)$ graus de liberdade, podendo ser descodificados, enquanto que os símbolos de ruído são alinhados e requerem apenas $1/N_t$ graus de liberdade. Por outro lado, no nó malicioso, os símbolos de ruído ocupam totalmente um grau de liberdade, e os símbolos de informação são completamente mascarados pelos símbolos de ruído.

2.6 Conclusões

Neste capítulo foi realizada uma passagem teórica através dos principais conceitos e tecnologias que serão usados nos capítulos a seguir, no modelo sistêmico a ser proposto e a análise do desempenho de *outage* de sigilo do sistema. Foram mostradas as vantagens da utilização de sistemas MIMO nas comunicações sem fio, especialmente na obtenção de ganhos por diversidade, e foram descritos alguns dos esquemas de diversidade espacial na recepção e transmissão mais utilizados. Além disso, foi apresentada a segurança na camada física como uma estratégia efetiva em garantir o sigilo na informação. Em conjunto, a parceria entre as duas técnicas fornece sistemas mais robustos, com níveis aceitáveis de segurança, além de altas taxas de transferências.

3 SEGURANÇA DA CAMADA FÍSICA PARA SISTEMAS MIMO

3.1 Introdução

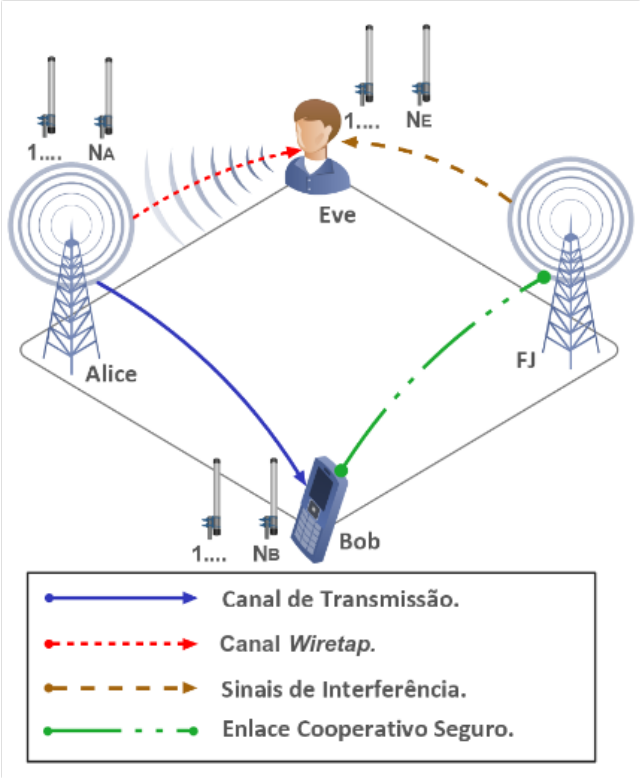
Como mencionado anteriormente, desde a introdução do conceito de canais *wiretap* realizada por Wyner [3], a segurança da camada física tem demostrado ser uma abordagem efetiva para garantir um nível de sigilo razoável em redes sem fio. Na literatura é possível encontrar várias técnicas a fim de aumentar a taxa de sigilo para diferentes modelos sistêmicos. Uma das técnicas mais amplamente aceitas é a interferência cooperativa, que consiste no envio de sinais de interferência para o nó intruso a partir do receptor legítimo ou usando um nó amigo presente na rede. Embora muitos estudos tenham abordado esta técnica, devido à variedade de modelos sistêmicos existentes, ainda existem lacunas na literatura que seriam úteis investigar a fim de ter uma melhor informação do desempenho de *outage* de sigilo. Este capítulo pretende preencher uma dessas lacunas existentes na literatura ainda, analisando o desempenho de *outage* de um canal MIMO *wiretap* assumindo que o nó intruso é afetado por sinais de interferência e ruído.

O presente capítulo fará um estudo do desempenho de *outage* de sigilo em sistemas *wiretap* MIMO para dois esquemas de combinação de sinal no receptor, apresentados no Capítulo 2. São eles: o SC e o MRC. Para isso, primeiramente será apresentado, na Seção 3.2, o modelo sistêmico adotado nesta dissertação. As formulações matemáticas e as expressões analíticas fechadas que descrevem o desempenho de *outage* de sigilo são apresentadas na Seção 3.3. Finalmente, o ganho de *array* e a ordem de diversidade do sistema são determinadas através de uma análise assintótica na Subseção 3.6. Nas análises, é assumido atraso no *feedback* entre o canal Tx-Rx.

3.2 Modelo do Sistema

O sistema a ser investigado é um canal MIMO *wiretap*, composto de um transmissor (Tx) chamado Alice, um receptor (Rx) legítimo chamado Bob, e um nó malicioso (ou seja, o intruso, ou *eavesdropper*), chamado Eve, que tenta interceptar a troca de informações entre Alice e Bob, como ilustrado na Figura 10. Todos os nós estão equipados com múltiplas antenas. Especificamente, Alice possui N_{A} antenas e emprega um esquema TAS para selecionar a antena de transmissão. Similarmente, Bob é equipado com N_{B} antenas e adota os esquemas SC ou MRC para combinar os sinais recebidos de Alice. Além disso, Eve é equipado com N_{E} antenas e usa um esquema MRC.

Figura 10: Modelo do Sistema.



Fonte: Própio autor.

A fim de realizar TAS, Alice depende da CSI do Bob para selecionar a antena que maximiza a SNR instantânea em Bob. Nesta análise considera-se um nó amigo (FJ, do inglês, *Friendly Jammer*) que tem uma cooperação completa e segura com Bob e provoca interferências no nó malicioso. Assim, assume-se que o Eve é afetado tanto por ruído quanto por sinais de interferência com distribuição de potências arbitrária. Além disso, Eve é um nó intruso passivo, isto é, não existe qualquer *feedback*) entre Eve e Alice. Supõe-se também, que o canal principal (canal Alice-Bob) e o canal do nó intruso (canal Alice-Eve) são independentes um do outro, e experimentam um desvanecimento lento com o mesmo comprimento de desvanecimento em bloco, sendo suficientemente longo para permitir códigos de realização-capacidade (do inglês, *capacity-achieving codes*)

dentro de cada bloco. A seguir, os esquemas de combinação de sinal em Bob e Eve serão detalhados.

3.2.1 *Esquema MRC em Bob*

Considerando um esquema MRC em Bob, Alice seleciona a antena de transmissão com índice s de acordo com a regra

$$s = \arg \max_{\lambda \in \{1,\ldots,N_{\mathrm{A}}\}} \mathbf{h}_{\mathrm{AB},\lambda}, \tag{14}$$

em que $||.||$ indica norma de Frobenius e $\mathbf{h}_{\mathrm{AB},\lambda}$ denota o vetor de canal com dimensões $N_B \times 1$ entre Bob e a $\lambda^{ésima}$ antena em Alice, sendo definido como $\mathbf{h}_{\mathrm{AB},\lambda} = [h^1_{\mathrm{AB},\lambda}, h^2_{\mathrm{AB},\lambda}..h^{N_B}_{\mathrm{AB},\lambda}]^T$, com $(.)^T$ representando operador trasposto. Em sistemas práticos, devido à natureza variável no tempo do meio sem fio, o canal Alice-Bob pode ter mudado no momento em que Alice recebe o *feedback* de Bob com o índice ótimo de antena. Como resultado, a antena ótima é selecionada com base em uma CSI desatualizada com uma versão do coeficiente de canal $\mathbf{h}_{\mathrm{AB},\lambda}$ com um atraso de tempo, denotada $\breve{\mathbf{h}}_{\mathrm{AB},\lambda}$. Assim, a relação de correlação entre $\mathbf{h}_{\mathrm{AB},\lambda}$ e $\breve{\mathbf{h}}_{\mathrm{AB},\lambda}$ pode ser expressa como

$$\breve{\mathbf{h}}_{\mathrm{AB},\lambda} = \sqrt{\rho}\mathbf{h}_{\mathrm{AB},\lambda} + \sqrt{1-\rho}\boldsymbol{\vartheta}, \tag{15}$$

em que $\boldsymbol{\vartheta}$ denota uma variável aleatória Gaussiana com variância igual à de $\mathbf{h}_{\mathrm{AB},\lambda}$ e ρ representa o coeficiente de correlação entre $\mathbf{h}_{\mathrm{AB},\lambda}$ e $\breve{\mathbf{h}}_{\mathrm{AB},\lambda}$ e é dado pelo modelo de autocorrelação de Jake [32] como

$$\rho = {J_0}^2(2\pi f_d \tau), \tag{16}$$

em que f_d representa a frequência máxima Doppler, τ denota o atraso no tempo, e J_0 indica a função de Bessel de ordem zero de primeiro tipo [62, Eq. (8.402)]. Considerando que Alice tenha selecionado a antena s para transmitir o sinal x tendo como base a CSI desatualizada de Bob, o sinal recebido em Bob no instante de tempo t pode ser modelado como

$$\mathbf{y}_{\mathrm{B}}(t) = \sqrt{P}\breve{\mathbf{h}}_{\mathrm{AB,s}}x(t) + \mathbf{n}_{\mathrm{B}}, \tag{17}$$

em que $\breve{\mathbf{h}}_{\mathrm{AB,s}}$ denota a versão com atraso no tempo de $\mathbf{h}_{\mathrm{AB,s}}$, com $\mathbf{h}_{\mathrm{AB,s}}$ indicando o vetor de canal com dimensões $N_B \times 1$ entre a antena selecionada por Alice e Bob, e $\mathbf{n}_{\mathrm{B}}$ representa o vetor de canal do ruído Gaussiano Branco Aditivo (AWGN, do inglês, *Additive White Gaussian Noise*) com dimensões $N_B \times 1$, cujas entradas têm variância σ_b^2 e média zero. Logo, por [17], o vetor de pesos MRC é dado por $\mathbf{w}_{\mathrm{B}} = \frac{\breve{\mathbf{h}}_{\mathrm{AB,s}}^{\dagger}}{||\breve{\mathbf{h}}_{\mathrm{AB,s}}||}$, com $(.)^{\dagger}$ denotando conjugado trasposto. Assim, o sinal na saída do MRC pode ser expressa como

$$\mathbf{y}_{\mathrm{B}}(t) = \mathbf{w}_{\mathrm{B}}\sqrt{P}\breve{\mathbf{h}}_{\mathrm{AB,s}}x(t) + \mathbf{w}_{\mathrm{B}}\mathbf{n}_{\mathrm{B}}. \tag{18}$$

É assumido que Bob mantém uma cooperação completa com o nó amigo, assim é capaz de cancelar completamente qualquer sinal de interferência proveniente deste nó. Logo, a SNR recebida em Bob pode ser escrita como

$$\breve{\gamma}_{\mathrm{B,s}}^{\mathrm{MRC}} = \bar{\gamma}_{\mathrm{B}}||\breve{\mathbf{h}}_{\mathrm{AB,s}}||^2. \tag{19}$$

em que $\bar{\gamma}_{\mathrm{B}} = \frac{P}{\sigma_b^2}$.

3.2.2 *Esquema SC em Bob*

Considerando um esquema SC em Bob, Alice seleciona a antena de transmissão com índice s de acordo com a regra

$$s = \arg \max_{\lambda \in \{1,\ldots,N_{\mathrm{A}}\} \forall \delta \in \{1,\ldots,N_{\mathrm{B}}\}} |h_{\mathrm{AB},\lambda}^{\delta}|, \tag{20}$$

em que $|.|$ significa valor absoluto, e $h_{\mathrm{AB},\lambda}^{\delta}$ denota o coeficiente de canal entre a $\lambda^{ésima}$ antena de Alice e a $\delta^{ésima}$ antena de Bob. Seguindo um raciocínio semelhante ao caso MRC, Alice transmite o sinal x com a antena selecionada s baseada em uma CSI desatualizada, enquanto Bob usa o esquema SC para selecionar o ramo com maior SNR. Assim, é assumida uma versão do coeficiente de canal $h_{\mathrm{AB},\lambda}^{\delta}$ com um atraso no tempo, denotada $\breve{h}_{\mathrm{AB},\lambda}^{\delta}$, e cujo relacionamento vai seguir o mesmo princípio que na expressão (15), através da substituição dos coeficientes de canal correspondentes ao caso SC. Isto resulta no sinal combinado y_{B}, que pode ser expresso como

$$y_{\mathrm{B}} = \sqrt{P}\breve{h}_{\mathrm{AB,s}}x + n_{\mathrm{B}}, \tag{21}$$

em que P denota a potência de transmissão em Alice, n_{B} é a componente de AWGN com variância σ_b^2 e média zero, e $h_{\mathrm{AB,s}}$ é dado por

$$\breve{h}_{\mathrm{AB,s}} = \max_{\delta \in \{1,\ldots N_{\mathrm{B}}\}} |\breve{h}^{\delta}_{\mathrm{AB},\lambda}|. \tag{22}$$

Finalmente, Alice transmite o sinal x utilizando a antena s selecionada e a SNR em Bob pode ser escrita como

$$\breve{\gamma}^{\mathrm{SC}}_{\mathrm{B,s}} = \bar{\gamma}_B |\breve{h}_{\mathrm{AB,s}}|^2. \tag{23}$$

3.2.3 *Esquema MRC em Eve Sujeito a Ruído e Sinais de Interferência*

No caso do nó intruso, Eve consegue estimar o canal de Alice por meio de sequências de treinamento. Foi assumido um esquema MRC no nó malicioso por ter uma maior capacidade de processamento que outros esquemas (por exemplo, SC), o que representa o pior caso possível. Assim, com a adoção de um esquema MRC, além de estar sujeito a ruído e múltiplos sinais de interferência (M), o sinal recebido em Eve pode ser expresso como

$$\mathbf{y}_{\mathrm{E}} = \sqrt{P}\mathbf{h}_{\mathrm{AE,s}}x + \sum_{i=1}^{M} \sqrt{\bar{\gamma}_i}\mathbf{h}_{\mathrm{i}} + \mathbf{n}_{\mathrm{E}}, \tag{24}$$

em que $\mathbf{h}_{\mathrm{AE,s}}$ representa o vetor de canal com dimensões $N_E \times 1$ entre Eve e a antena s selecionada por Alice, $\mathbf{h}_{\mathrm{i}}$ representa o vetor do canal entre Eve e o $i^{ésimo}$ sinal de interferência, $\bar{\gamma}_i$ denota a potência do $i^{ésimo}$ sinal de interferência, e $\mathbf{n}_{\mathrm{E}}$ denota o vetor de canal do AWGN com dimensões $N_E \times 1$, cujas entradas têm variância unitária. Logo, o sinal recebido na saída do MRC pode ser escrito como

$$y_{\mathrm{E}} = \sqrt{P}\frac{\mathbf{h}^{\dagger}_{\mathrm{AE,s}}}{||\mathbf{h}_{\mathrm{AE,s}}||}\mathbf{h}_{\mathrm{AE,s}}x + \sum_{i=1}^{M}\sqrt{\bar{\gamma}_i}\frac{\mathbf{h}^{\dagger}_{\mathrm{AE,s}}}{||\mathbf{h}_{\mathrm{AE,s}}||}\mathbf{h}_{\mathrm{i}} + \mathbf{n}_{\mathrm{E}} = \sqrt{P}||\mathbf{h}_{\mathrm{AE,s}}||x + \sum_{i=1}^{M}\sqrt{\bar{\gamma}_i}\ddot{h}_{\mathrm{i}} + \mathbf{n}_{\mathrm{E}}. \tag{25}$$

Sabendo que $\mathbf{h}_{\mathrm{AE,s}}$ e $\mathbf{h}_{\mathrm{i}}$ são independentes, foi demonstrado em [17] que $\ddot{h}_{\mathrm{i}} = \frac{\mathbf{h}^{\dagger}_{\mathrm{AE,s}}}{||\mathbf{h}_{\mathrm{AE,s}}||}\mathbf{h}_i$ segue a mesma distribuição de $\mathbf{h}_i$. Devido a este fato, a relação sinal-interferência-mais ruído (SINR, do inglês, *Signal-to-Interference-plus Noise Ratio*) em Eve pode ser expressa como

$$\Upsilon_{\mathrm{E,s}} = \frac{\gamma_{\mathrm{E,s}}}{\gamma_{\mathrm{I}} + 1}, \tag{26}$$

em que $\gamma_{\mathrm{E,s}} = \bar{\gamma}_{\mathrm{E}}||\mathbf{h}_{\mathrm{AE,s}}||^2$, $\gamma_{\mathrm{I}} = \sum_{i=1}^{M} \bar{\gamma}_i|\breve{h}_{\mathrm{i}}|^2$, e $\bar{\gamma}_{\mathrm{E}}$ denota a variância do canal.

3.3 Desempenho de *Outage* de Sigilo

Neste contexto, um evento de *outage* ocorre quando o canal entre Alice-Bob está deteriorado (o que se conhece como canal em *outage*), ou quando Eve é capaz de interceptar a troca de informações entre Alice e Bob. Em canais de desvanecimento, o sinal recebido não tem uma SNR constante pois depende da qualidade do canal, que pode ser descrito por modelos de probabilidades. Assim, a SNR torna-se uma variável aleatória (VA), o que torna a capacidade máxima do canal uma VA. Então, a probabilidade de *outage* de sigilo (PO), dependendo da variabilidade da SNR no receptor, vai descrever a probabilidade de uma determinada taxa não ser suportada devido à variabilidade na SNR, e é definida como a probabilidade de que o sinal recebido em Bob seja inferior a um limiar estabelecido, ou como a probabilidade que Eve intercepte a troca de informações entre Alice e Bob. Logo, é comum o uso da PO como a métrica primária para a análise de esquemas de diversidade em sistemas de comunicações sem fio [61]. Nesta seção, o desempenho de *outage* de sigilo no cenário proposto é analisado através da apresentação de expressões analíticas que descrevem o mesmo.

3.3.1 *Estatísticas Úteis*

Para descrever o canal como um modelo de probabilidade, são necessárias algumas estatísticas preliminares que serão úteis para a posterior derivação analítica e assintótica da PO. Nesta subseção são apresentadas as expressões probabilísticas que descrevem o canal de desvanecimento proposto.

Seja $R_{\mathrm{B,s}} = \log_2(1 + \gamma_{\mathrm{B,s}})$ a capacidade do canal Alice-Bob e $R_{\mathrm{E,s}} = \log_2(1 + \Upsilon_{\mathrm{E,s}})$ a capacidade do canal Alice-Eve. Então, a capacidade de sigilo pode ser definida como [24]

$$R_{\mathrm{S}} = \begin{cases} R_{\mathrm{B,s}} - R_{\mathrm{E,s}}, & \gamma^{j}_{\mathrm{B,s}} > \Upsilon_{E,s}, \\ 0, & \gamma^{j}_{\mathrm{B,s}} \leq \Upsilon_{\mathrm{E,s}}. \end{cases} \tag{27}$$

em que $j \in$ (MRC, SC).

3.3.2 *Esquema MRC em Bob*

Em primeiro lugar, assumimos que todos os canais sofrem desvanecimento *Rayleigh*. Assim, respeitando as condições de desvanecimento independente e identicamente distribuído (iid, do inglês, *independent and identically distributed*), a função de densidade de probabilidade (PDF, do inglês, *probability density function*) e a (CDF, do inglês, *cumulative distribution function*) da VA $\gamma_{\mathrm{B},\lambda}^{\mathrm{MRC}} = \bar{\gamma}_{\mathrm{B}}||\mathbf{h}_{\mathrm{AB},\lambda}||^2$ podem ser obtidas, respectivamente, como

$$f_{\gamma_{\mathrm{B},\lambda}}^{\mathrm{MRC}}(z) = \frac{z^{N_B-1}e^{-\frac{z}{\bar{\gamma}_{\mathrm{B}}}}}{\bar{\gamma}_{\mathrm{B}}^{N_B}\Gamma(N_B)}, \tag{28}$$

e

$$F_{\gamma_{\mathrm{B},\lambda}}^{\mathrm{MRC}}(z) = 1 - e^{-\frac{z}{\bar{\gamma}_{\mathrm{B}}}}\sum_{u=0}^{N_B-1}\frac{1}{u!}\left(\frac{z}{\gamma_{\mathrm{B}}}\right)^u. \tag{29}$$

em que $\Gamma(.)$ denota a função Gamma [62, Eq. (8.310.1)]. Quando Alice seleciona a antena de transmissão baseada em uma CSI desatualizada, com um tempo de atraso τ e $\rho \neq 1$, $\gamma_{\mathrm{B,s}}^{\mathrm{MRC}}$ vai ser uma versão atrasada no tempo da atual SNR $\breve{\gamma}_{\mathrm{B,s}}^{\mathrm{MRC}}$. Assim, considerando a relação entre $\gamma_{\mathrm{B,s}}^{\mathrm{MRC}}$ e $\breve{\gamma}_{\mathrm{B,s}}^{\mathrm{MRC}}$, a PDF de $\breve{\gamma}_{\mathrm{B,s}}^{\mathrm{MRC}}$ pode ser derivada como

$$f_{\breve{\gamma}_{\mathrm{B,s}}^{\mathrm{MRC}}}(x) = \int_0^\infty f_{\breve{\gamma}_{\mathrm{B,s}}^{\mathrm{MRC}}|\gamma_{\mathrm{B,s}}^{\mathrm{MRC}}}(x|y)f_{\gamma_{\mathrm{B,s}}^{\mathrm{MRC}}}(y)dy. \tag{30}$$

em que $f_{\breve{\gamma}_{\mathrm{B,s}}^{\mathrm{MRC}}|\gamma_{\mathrm{B,s}}^{\mathrm{MRC}}}(\cdot|\cdot)$ indica a PDF de $\breve{\gamma}_{\mathrm{B,s}}^{\mathrm{MRC}}$ condicionada por $\gamma_{\mathrm{B,s}}^{\mathrm{MRC}}$, e pode ser expressa como

$$f_{\breve{\gamma}_{\mathrm{B,s}}^{\mathrm{MRC}}|\gamma_{\mathrm{B,s}}^{\mathrm{MRC}}}(x|y) = \frac{f_{\breve{\gamma}_{\mathrm{B},\lambda}^{\mathrm{MRC}},\gamma_{\mathrm{B},\lambda}^{\mathrm{MRC}}}(x,y)}{f_{\gamma_{\mathrm{B},\lambda}^{\mathrm{MRC}}}}, \tag{31}$$

em que $f_{\breve{\gamma}_{\mathrm{B},\lambda}^{\mathrm{MRC}},\gamma_{\mathrm{B},\lambda}^{\mathrm{MRC}}}(\cdot,\cdot)$ denota a PDF conjunta de $\breve{\gamma}_{\mathrm{B},\lambda}^{\mathrm{MRC}}$ e $\gamma_{\mathrm{B},\lambda}^{\mathrm{MRC}}$. Assim, com a ajuda de [63], $f_{\breve{\gamma}_{\mathrm{B},\lambda}^{\mathrm{MRC}},\gamma_{\mathrm{B},\lambda}^{\mathrm{MRC}}}(\cdot,\cdot)$ é dada por

$$f_{\breve{\gamma}_{\mathrm{B},\lambda}^{\mathrm{MRC}},\gamma_{\mathrm{B},\lambda}^{\mathrm{MRC}}}(x,y) = \frac{1}{(1-\rho)}\left(\frac{1}{\bar{\gamma_{\mathrm{B}}}}\right)\left(\frac{x}{\rho y}\right)^{\frac{N_B-1}{2}}e^{-\frac{\rho y+x}{(1-\rho)\bar{\gamma}_{\mathrm{B}}}}I_{N_B-1}\left(\frac{2\sqrt{\rho xy}}{(1-\rho)\bar{\gamma}_{\mathrm{B}}}\right), \tag{32}$$

em que $I_k(.)$ é a $k^{ésima}$ função de Bessel modificada do primeiro tipo [62, Eq. (8.406.1)]. Por outro lado, utilizando conceitos da teoria da probabilidade e o teorema multinomial, a PDF de $\gamma_{\mathrm{B,s}}^{\mathrm{MRC}}$, pode ser expressa como

$$f_{\gamma_{\mathrm{B,s}}}^{\mathrm{MRC}}(z) = \frac{N_A}{\Gamma(N_B)} \sum_{n_1=0}^{N_\mathrm{A}-1} (-1)^n \binom{N_\mathrm{A}-1}{n_1} \sum_{N_B,n_1} \frac{z^{N_B+\beta-1}}{\bar{\gamma}_\mathrm{B}^{N_B+\beta}} e^{-\frac{(n_1+1)z}{\bar{\gamma}_\mathrm{B}}}. \tag{33}$$

em que a notação $\sum_{N_B,n_1}$ é dada por

$$\sum_{N_B,n_1} = \sum_{n_2=0}^{n_1} \sum_{n_3=0}^{n_2} \cdots \sum_{n_{N_B}=0}^{n_{N_B-1}} \prod_{i=0}^{N_B-1} \left(\frac{1}{i!}\right)^{n_{i+1}-n_{i+2}} \binom{n_{i+1}}{n_{i+2}}, \tag{34}$$

sendo $n_{N_B+1} = 0$ e $\beta = \sum_{j=0}^{N_B-1} j\,(n_{j+1} - n_{j+2})$.

Então, substituindo (32) e (33) em (30), e utilizando o teorema multinomial, $f_{\breve{\gamma}_{\mathrm{B,s}}^{\mathrm{MRC}}}$ é expandida como

$$f_{\breve{\gamma}_{\mathrm{B,s}}^{\mathrm{MRC}}}(x) = \frac{N_A}{(N_B-1)!} \sum_{n1=0}^{N_\mathrm{A}-1} \binom{N_\mathrm{A}-1}{n1} (-1)^{n1} \frac{1}{(1-\rho)} \left(\frac{x}{\rho}\right)^{\frac{N_B-1}{2}} \sum_{N_B,n_1} \left(\frac{1}{\bar{\gamma}_\mathrm{B}}\right)^{N_B+\beta+1} e^{-\frac{x}{(1-\rho)\bar{\gamma}_\mathrm{B}}} \Lambda, \tag{35}$$

em que Λ é a integral expressa por

$$\Lambda = \int_0^\infty y^{\frac{N_B-1}{2}+\beta} e^{-y\frac{1+n1(1-\rho)}{(1-\rho)\bar{\gamma}_\mathrm{B}}} I_{N_B-1}\left(\frac{2\sqrt{\rho x y}}{(1-\rho)\bar{\gamma}_\mathrm{B}}\right) dy. \tag{36}$$

Assim, com o suporte das combinações da função de Bessel [62, Eq. (6.643.2)], os termos polinomiais da função de Whittaker-M [62, Eq. (9.220.2)], e algumas manipulações matemáticas, Λ é derivada e $f_{\breve{\gamma}_{\mathrm{B,s}}^{\mathrm{MRC}}}(x)$ pode ser obtida como

$$\begin{aligned} f_{\breve{\gamma}_{\mathrm{B,s}}^{\mathrm{MRC}}}(x) =& \frac{N_A}{(N_B-1)!} \sum_{n_1=0}^{N_\mathrm{A}-1} \binom{N_\mathrm{A}-1}{n_1} (-1)^{n_1} \sum_{N_B,n_1} \sum_{\alpha=0}^{\beta} \binom{\beta}{\alpha} \left(\frac{1}{\bar{\gamma}_\mathrm{B}}\right)^{N_B+\alpha} \frac{(N_B+\beta-1)!}{(N_B+\alpha-1)!} \\ & \times \frac{\rho^\alpha (1-\rho)^{\beta-\alpha}}{(n_1(1-\rho)+1)^{N_B+\beta+\alpha}} x^{N_B+\alpha-1} e^{-\frac{(n_1+1)x}{(n_1(1-\rho)+1)\bar{\gamma}_\mathrm{B}}}. \end{aligned} \tag{37}$$

A CDF de $\breve{\gamma}_{\mathrm{B,s}}^{\mathrm{MRC}}$ pode ser obtida através da integração de $f_{\breve{\gamma}_{\mathrm{B,s}}^{\mathrm{MRC}}}$ como

$$\begin{aligned} F_{\breve{\gamma}_{\mathrm{B,s}}^{\mathrm{MRC}}}(x) =& \frac{N_A}{(N_B-1)!} \sum_{n_1=0}^{N_\mathrm{A}-1} \binom{N_\mathrm{A}-1}{n_1} (-1)^{n_1} \sum_{N_B,n_1} \sum_{\alpha=0}^{\beta} \binom{\beta}{\alpha} (N_B+\beta-1)! \sum_{m=0}^{N_B+\alpha-1} \left(\frac{1}{\bar{\gamma}_\mathrm{B}}\right)^m \\ & \times \frac{\rho^\alpha (1-\rho)^{\beta-\alpha}}{(n_1(1-\rho)+1)^{\beta+m}} \frac{x^m}{m!(n_1+1)^{N_B+\alpha-m}} e^{-\frac{(n_1+1)x}{(n_1(1-\rho)+1)\bar{\gamma}_\mathrm{B}}}. \end{aligned} \tag{38}$$

Finalmente, podemos reduzir o CDF para o caso com *feedback* perfeito, estabelecendo $\rho = 1$ em (38) como

$$F_{\gamma_{\mathrm{B,s}}}^{\mathrm{MRC}}(z) = \left[F_{\gamma_{\mathrm{B},\lambda}}(z)\right]^{N_{\mathrm{A}}} = \sum_{n_1=0}^{N_{\mathrm{A}}} (-1)^n \binom{N_{\mathrm{A}}}{n_1} \sum_{N_B,n_1} \left(\frac{z}{\bar{\gamma}_{\mathrm{B}}}\right)^{\beta} e^{-\frac{n_1 z}{\bar{\gamma}_{\mathrm{B}}}}. \tag{39}$$

Perceba que, as expressões (41), (40), (33), (37), (38) e (39) podem ser reduzidas para o caso de um canal MISO *wiretap*, com a suposição que Bob possui apenas uma antena, isto é, fixando N_B=1.

3.3.3 *Esquema SC em Bob*

Assumindo que todos os canais sofrem desvanecimento *Rayleigh* respeitando as condições iid, e uma CSI perfeita, a PDF e a CDF da VA $\gamma_{\mathrm{B,s}}^{\mathrm{SC}} = \bar{\gamma}_{\mathrm{B}}|h_{\mathrm{AB,s}}|^2$ podem ser derivadas, após à aplicação da expansão binomial, como

$$f_{\gamma_{\mathrm{B,s}}}^{\mathrm{SC}}(z) = \frac{N_{\mathrm{A}} N_{\mathrm{B}}}{\bar{\gamma}_{\mathrm{B}}} \sum_{n=0}^{N_{\mathrm{A}}N_{\mathrm{B}}-1} (-1)^n \binom{N_{\mathrm{A}}N_{\mathrm{B}}-1}{n} e^{-\frac{(n+1)z}{\bar{\gamma}_{\mathrm{B}}}}. \tag{40}$$

e

$$F_{\gamma_{\mathrm{B,s}}}^{\mathrm{SC}}(z) = \left(1 - e^{-\frac{z}{\bar{\gamma}_{\mathrm{B}}}}\right)^{N_A N_B} = 1 - \sum_{n=1}^{N_{\mathrm{A}}N_{\mathrm{B}}} (-1)^{n+1} \binom{N_{\mathrm{A}}N_{\mathrm{B}}}{n} e^{-\frac{nz}{\bar{\gamma}_{\mathrm{B}}}}. \tag{41}$$

3.3.4 *Esquema MRC em Eve*

A PDF e a CDF da VA $\Upsilon_{\mathrm{E,s}}$ podem ser obtidas através da substituição de N_{B} e $\bar{\gamma}_{\mathrm{B}}$ por N_{E} e $\bar{\gamma}_{\mathrm{E}}$ em (28) e (29) respectivamente.

Sejam $\bar{\gamma}_1, \bar{\gamma}_2, \ldots, \bar{\gamma}_t$ valores diferentes com multiplicidades $\eta_1, \eta_2, \ldots, \eta_t$ tal que $\sum_{i=1}^{t} \eta_i = M$. Então, por [64], a PDF de γ_{I} pode ser escrita como

$$f_{\gamma_{\mathrm{I}}}(z) = \sum_{i=1}^{t} \sum_{j=1}^{\eta_i} \frac{\Omega_{i,j}}{(j-1)!\bar{\gamma}_i^j} z^{j-1} e^{-\frac{z}{\bar{\gamma}_i}}, \tag{42}$$

em que

$$\Omega_{i,j} = \frac{1}{(\eta_i - j)!\bar{\gamma}_i^{\eta_i - j}} \frac{\partial^{\eta_i - j}}{\partial s^{\eta_i - j}} \left[\prod_{k=1,k\neq i}^{t} \left(\frac{1}{1 + s\bar{\gamma}_k}\right)^{\eta_k}\right]_{s=-\frac{1}{\bar{\gamma}_i}}. \tag{43}$$

Realizando o procedimento padrão de mudança de variável, a PDF de $\gamma_{\mathrm{I+1}}$ pode ser obtida a partir de (42) como

$$f_{\gamma_{\mathrm{I}+1}}(z) = \sum_{i=1}^{t}\sum_{j=1}^{\eta_i} \frac{\Omega_{i,j}}{(j-1)!\bar{\gamma}_i^j} \sum_{k=1}^{j}\sum_{p=1}^{k} \binom{j-1}{k-1}\binom{k-1}{p-1} z^{p-1} e^{-\frac{z}{\bar{\gamma}_i}}. \tag{44}$$

Voltando a atenção para as estatísticas da VA $\Upsilon_{\mathrm{E,s}}$, a PDF pode ser definida como

$$f_{\frac{\gamma_{\mathrm{E}}}{\gamma_{\mathrm{I}+1}}}(x) = \frac{\partial}{\partial x}\left[\int_0^{\infty} F_{\gamma_{\mathrm{E,s}}}(xz) f_{\gamma_{\mathrm{I}+1}}(z) dz\right]. \tag{45}$$

Realizando as substituições apropriadas e após algumas manipulações algébricas, uma expressão analítica fechada para a PDF de $\Upsilon_{\mathrm{E,s}}$ é obtida

$$\begin{aligned} f_{\frac{\gamma_{\mathrm{E}}}{\gamma_{\mathrm{I}+1}}}(x) = f_{\Upsilon_{\mathrm{E,s}}}(x) = \sum_{i=1}^{t}\sum_{j=1}^{\eta_i} \Omega_{i,j} \sum_{k=1}^{j}\sum_{p=1}^{k} (-1)^{j-k} \sum_{u=0}^{N_E-1}\sum_{q=0}^{u} \frac{\Gamma(p+q)\bar{\gamma}_i^{p+q-j}}{(j-k)!(k-p)!(p-1)!(u-q)!q!} \\ \times \left(\frac{x}{\bar{\gamma}_E}\right)^u e^{-\frac{x}{\bar{\gamma}_E}} \left[(p+q)\frac{\bar{\gamma}_i}{\bar{\gamma}_E}\left(1+\frac{x\bar{\gamma}_i}{\bar{\gamma}_E}\right)^{-p-q-1} + \frac{1}{\bar{\gamma}_E}\left(1+\frac{x\bar{\gamma}_i}{\bar{\gamma}_E}\right)^{-p-q} - ux^{-1} \right. \\ \left. \times \left(1+\frac{x\bar{\gamma}_i}{\bar{\gamma}_E}\right)^{-p-q}\right]. \end{aligned} \tag{46}$$

Para o caso especial de um canal MISO *wiretap* entre Alice e o nó intruso, em que Eve possui apenas uma antena, isto é, com N_E=1, (46) pode ser reduzida como

$$\begin{aligned} f_{\frac{\gamma_{\mathrm{E}}}{\gamma_{\mathrm{I}+1}}}(x) = \sum_{i=1}^{t}\sum_{j=1}^{\eta_i} \Omega_{i,j} \sum_{k=1}^{j}\sum_{p=1}^{k} (-1)^{j-k} \frac{\bar{\gamma}_i^{p-j-1}}{(j-k)!(k-p)!\bar{\gamma}_E} e^{-\frac{x}{\bar{\gamma}_E}} \\ \times \left[\left(1+\frac{x\bar{\gamma}_i}{\bar{\gamma}_E}\right)^{-p} + p\bar{\gamma}_i\left(1+\frac{x\bar{\gamma}_i}{\bar{\gamma}_E}\right)^{-p-1}\right]. \end{aligned} \tag{47}$$

3.4 Probabilidade de *Outage* de Sigilo

Como mencionado, a probabilidade de *outage* de sigilo é amplamente usada como métrica para avaliar os regimes de diversidade em sistemas de comunicações sem fio, sendo geralmente usada como indicador bruto de desempenho. Define-se então, como a probabilidade de que R_{S} caia abaixo de um determinado limiar de taxa de R, e a representação matemática para tal métrica pode ser escrita como

$$
\begin{aligned}
P_{\mathrm{s}}(R) &= \Pr(R_{\mathrm{S}} < R) \\
&= \Pr\left(\frac{1+\gamma_{\mathrm{B,s}}^{j}}{1+\Upsilon_{\mathrm{E,s}}} < 2^{R}\right) \Pr\left(\gamma_{\mathrm{B,s}}^{j} > \Upsilon_{\mathrm{E,s}}\right) \\
&+ \Pr\left(\gamma_{\mathrm{B,s}}^{j} < \Upsilon_{\mathrm{E,s}}\right) = \Pr\left(\frac{1+\gamma_{\mathrm{B,s}}^{j}}{1+\frac{\gamma_{\mathrm{E,s}}}{\gamma_{\mathrm{I}}+1}} < 2^{R}\right) \Pr\left(\gamma_{\mathrm{B,s}}^{j} > \frac{\gamma_{\mathrm{E,s}}}{\gamma_{\mathrm{I}}+1}\right) \\
&+ \Pr\left(\gamma_{\mathrm{B,s}}^{j} < \frac{\gamma_{\mathrm{E,s}}}{\gamma_{\mathrm{I}}+1}\right). \qquad (48)
\end{aligned}
$$

com Pr(.) denotando probabilidade. Perceba que, com um nó intruso passivo, a transmissão de Alice é realizada com uma taxa de código constante R. Neste caso, quando $R_{\mathrm{S}} > R$, as "palavras-código"com a taxa de código selecionada por Alice vão garantir um sigilo perfeito. Por outro lado, quando $R_{\mathrm{S}} < R$, Eve vai conseguir escutar os dados secretos, logo, o sigilo perfeito não é garantido. Isto indica que a taxa no nó malicioso não vai ser zero. Na sequência, a probabilidade de *outage* torna-se uma métrica de desempenho muito útil e prática para avaliar a segurança.

3.4.1 *MRC em Bob*

Baseando-se em conceitos da teoria da probabilidade, (48) pode ser reescrita como

$$
\begin{aligned}
P_{s}(R) &= F_{\frac{1+\check{\gamma}_{\mathrm{B,s}}^{\mathrm{MRC}}}{1+\frac{\gamma_{\mathrm{E,s}}}{\gamma_{\mathrm{I}+1}}}}(2^{R}) = \int_{1}^{\infty} F_{1+\check{\gamma}_{\mathrm{B,s}}^{\mathrm{MRC}}}(2^{R}x) f_{1+\frac{\gamma_{\mathrm{E,s}}}{\gamma_{\mathrm{I}+1}}}(x)dx \\
&= \int_{0}^{\infty} F_{\check{\gamma}_{\mathrm{B,s}}}^{\mathrm{MRC}}(2^{R}x + 2^{R} - 1) f_{\frac{\gamma_{\mathrm{E,s}}}{\gamma_{\mathrm{I}+1}}}(x)dx = \int_{0}^{\infty} F_{\check{\gamma}_{\mathrm{B,s}}}^{\mathrm{MRC}}(2^{R}x + 2^{R} - 1) f_{\Upsilon_{\mathrm{E,s}}}(x)dx.
\end{aligned} \qquad (49)
$$

em que $F_{\check{\gamma}_{\mathrm{B,s}}}^{\mathrm{MRC}}(.)$ é dada em (38) e $f_{\Upsilon_{\mathrm{E,s}}}(.)$ foi determinada em (46). Em seguida, efetuando as substituições apropriadas seguidas de algumas manipulações algébricas, e a partir de [62, Eq. (9.211.4)], uma expressão analítica fechada para a probabilidade de *outage* de sigilo assumindo sinais com potências de interferência arbitrárias pode ser alcançada como

$$\breve{P}_{\mathrm{s}}^{\mathrm{MRC}}(R) = 1 - \frac{N_{\mathrm{A}}}{(N_{\mathrm{B}}-1)!}\sum_{n_1=0}^{N_{\mathrm{A}}-1}(-1)^{n_1}\binom{N_{\mathrm{A}}-1}{n_1}\sum_{N_{\mathrm{B}},n_1}\sum_{\alpha=0}^{\beta}\binom{\beta}{\alpha}\sum_{m=0}^{N_{\mathrm{B}}+\alpha-1}\frac{(N_{\mathrm{B}}+\beta-1)!}{(n_1+1)^{N_{\mathrm{B}}+\alpha-m}m!}$$
$$\times\frac{\rho^{\alpha}(1-\rho)^{\beta-\alpha}}{\varphi^{\beta+m}}\sum_{i=1}^{t}\sum_{j=1}^{\eta_i}\Omega_{i,j}\sum_{k=1}^{j}\sum_{p=1}^{k}(-1)^{j-k}\sum_{u=0}^{N_{\mathrm{E}}-1}\sum_{q=0}^{u}\sum_{s=0}^{m}\binom{m}{s}2^{R_{\mathrm{s}}}(2^R-1)^{m-s}$$
$$\times\frac{\Gamma(p+q)}{(j-k)!(k-p)!(u-q)!(p-1)!q!}\frac{\bar{\gamma}_E^{s}\bar{\gamma}_i^{p+q-j-s-u}}{\bar{\gamma}_B^{m}}e^{-\frac{(n_1+1)(2^R-1)}{\varphi\bar{\gamma}_B}}\xi_1, \tag{50}$$

em que

$$\xi_1 = \Bigg[(p+q)\Gamma(s+u+1)\Psi\left(s+u+1, s+u-p-q+1, \frac{(n_1+1)\bar{\gamma}_E 2^R+\varphi\bar{\gamma}_B}{\varphi\bar{\gamma}_i\bar{\gamma}_B}\right)+\Gamma(s+u+1)$$
$$\times\frac{1}{\bar{\gamma}_i}\,\Psi\left(s+u+1, s+u-p-q+2, \frac{(n_1+1)\bar{\gamma}_E 2^R+\varphi\bar{\gamma}_B}{\varphi\bar{\gamma}_i\bar{\gamma}_B}\right)-\Theta_1^{\mathrm{MRC}}\Bigg], \tag{51}$$

e

$$\Theta_1^{\mathrm{MRC}} = \begin{cases} u\Gamma(s+u)\Psi\left(s+u, s+u-p-q+1, \frac{(n_1+1)\bar{\gamma}_E 2^R+\varphi\bar{\gamma}_B}{\varphi\bar{\gamma}_i\bar{\gamma}_B}\right), & u\neq 0 \\ 0, & u=0 \end{cases} \tag{52}$$

com $\Psi(.,.,.)$ denotando a função de Tricomi (confluência hipergeométrica) [62, Eq.(9.211.4)], e $\varphi = (n_1(1-\rho)+1)$. A expressão (50) pode ser reduzida para o caso com uma CSI perfeita fixando $\rho = 1$ em (50) como

$$P_{\mathrm{s}}^{\mathrm{MRC}}(R) = 1 - \sum_{n_1=1}^{N_{\mathrm{A}}}\binom{N_{\mathrm{A}}}{n_1}\sum_{N_{\mathrm{B}},n_1}(-1)^{n_1+1}\sum_{i=1}^{t}\sum_{j=1}^{\eta_i}\Omega_{i,j}\sum_{k=1}^{j}\sum_{p=1}^{k}(-1)^{j-k}\sum_{u=0}^{N_{\mathrm{E}}-1}\sum_{q=0}^{u}$$
$$\times\frac{\Gamma(p+q)}{(j-k)!(k-p)!(u-q)!(p-1)!q!}\sum_{s=0}^{\beta}\binom{\beta}{s}2^{R_{\mathrm{s}}}(2^R-1)^{\beta-s}$$
$$\times\frac{\bar{\gamma}_E^{s}\bar{\gamma}_i^{p+q-j-s-u}}{\bar{\gamma}_B^{\beta}}e^{-\frac{n_1(2^R-1)}{\bar{\gamma}_B}}\xi_2 \tag{53}$$

em que

$$\xi_2 = \Bigg[(p+q)\Gamma(s+u+1)\Psi\left(s+u+1, s+u-p-q+1, \frac{n_1\bar{\gamma}_E 2^R+\bar{\gamma}_B}{\bar{\gamma}_i\bar{\gamma}_B}\right)+\Gamma(s+u+1)$$
$$\times\frac{1}{\bar{\gamma}_i}\,\Psi\left(s+u+1, s+u-p-q+2, \frac{n_1\bar{\gamma}_E 2^R+\bar{\gamma}_B}{\bar{\gamma}_i\bar{\gamma}_B}\right)-\Theta_2^{\mathrm{MRC}}\Bigg], \tag{54}$$

e

$$\Theta_2^{\mathrm{MRC}} = \begin{cases} u\Gamma(s+u)\Psi\left(s+u, s+u-p-q+1, \frac{n_1\bar{\gamma}_E 2^R+\bar{\gamma}_B}{\bar{\gamma}_i\bar{\gamma}_B}\right), & u\neq 0 \\ 0, & u=0 \end{cases} \tag{55}$$

Igualmente, baseado em (50), podem ser alcançadas as expressões fechadas para dois casos especiais, isto é, distribuição de potências iguais e diferentes respectivamente. Especificamente, definindo $j = k = p = 1$, (50) reduz-se para o caso em que todos os sinais de interferência possuem distribuição de potências diferentes, de modo que

$$\begin{aligned}\breve{P}_{\mathrm{s}}^{\mathrm{MRC}}(R) =& 1 - \frac{N_{\mathrm{A}}}{(N_{\mathrm{B}}-1)!}\sum_{n_1=0}^{N_{\mathrm{A}}-1}(-1)^{n_1}\binom{N_{\mathrm{A}}-1}{n_1}\sum_{N_{\mathrm{B}},n1}\sum_{\alpha=0}^{\beta}\binom{\beta}{\alpha}\sum_{m=0}^{N_{\mathrm{B}}+\alpha-1}\frac{(N_{\mathrm{B}}+\beta-1)!}{(n_1+1)^{N_{\mathrm{B}}+\alpha-m}m!} \\ &\times \frac{\rho^{\alpha}(1-\rho)^{\beta-\alpha}}{\varphi^{\beta+m}}\sum_{i=1}^{M}\bar{\gamma}_i^{M-1}\left[\prod_{k=1,k\neq i}^{t}(\bar{\gamma}_i-\bar{\gamma}_k)^{-1}\right]\sum_{u=0}^{N_{\mathrm{E}}-1}\sum_{q=0}^{u}\sum_{s=0}^{m}\binom{m}{s}2^{R\mathrm{s}}(2^R-1)^{m-s} \\ &\times \frac{\Gamma(1+q)}{(u-q)!q!}\frac{\bar{\gamma}_E^{s}\bar{\gamma}_i^{q-s-u}}{\bar{\gamma}_B^{m}}e^{-\frac{(n_1+1)(2^R-1)}{\varphi\bar{\gamma}_B}}\xi_1, \end{aligned} \tag{56}$$

em que em ξ_1 e Θ_1^{MRC}, $p = 1$. Para o caso em que um *feedback* perfeito é assumido, com $\rho = 1$ em (56), (56) pode ser reduzida como

$$\begin{aligned}P_{\mathrm{s}}^{\mathrm{MRC}}(R) =& 1 - \sum_{n_1=1}^{N_{\mathrm{A}}}\binom{N_{\mathrm{A}}}{n_1}\sum_{N_{\mathrm{B}},n_1}(-1)^{n_1+1}\sum_{i=1}^{M}\bar{\gamma}_i^{M-1}\left[\prod_{k=1,k\neq i}^{t}(\bar{\gamma}_i-\bar{\gamma}_k)^{-1}\right] \\ &\times \sum_{u=0}^{N_{\mathrm{E}}-1}\sum_{q=0}^{u}\frac{\Gamma(1+q)}{(u-q)!q!}\sum_{s=0}^{\beta}\binom{\beta}{s}2^{R_{\mathrm{s}}}(2^R-1)^{\beta-s}\frac{\bar{\gamma}_E^{s}\bar{\gamma}_i^{q-s-u}}{\bar{\gamma}_B^{\beta}}e^{-\frac{n_1(2^R-1)}{\bar{\gamma}_B}}\xi_2 \end{aligned} \tag{57}$$

em que em ξ_2 e Θ_2^{MRC}, $p = 1$.

Além disso, assumindo $j = M$ e $\bar{\gamma}_1 = \bar{\gamma}_2 \ldots = \bar{\gamma}_M$ em (50), a probabilidade de *outage* de sigilo para o caso de distribuição de potências iguais nos sinais interferentes pode ser obtida como

$$\begin{aligned}\breve{P}_{\mathrm{s}}^{\mathrm{MRC}}(R) =& 1 - \frac{N_{\mathrm{A}}}{(N_{\mathrm{B}}-1)!}\sum_{n_1=0}^{N_{\mathrm{A}}-1}(-1)^{n_1}\binom{N_{\mathrm{A}}-1}{n_1}\sum_{N_{\mathrm{B}},n1}\sum_{\alpha=0}^{\beta}\binom{\beta}{\alpha}\sum_{m=0}^{N_{\mathrm{B}}+\alpha-1}\frac{(N_{\mathrm{B}}+\beta-1)!}{(n_1+1)^{N_{\mathrm{B}}+\alpha-m}m!} \\ &\times \frac{\rho^{\alpha}(1-\rho)^{\beta-\alpha}}{\varphi^{\beta+m}}\sum_{k=1}^{M}\sum_{p=1}^{k}(-1)^{M-k}\sum_{u=0}^{N_{\mathrm{E}}-1}\sum_{q=0}^{u}\sum_{s=0}^{m}\binom{m}{s}2^{R\mathrm{s}}(2^R-1)^{m-s} \\ &\times \frac{\Gamma(p+q)}{(M-k)!(k-p)!(u-q)!(p-1)!q!}\frac{\bar{\gamma}_E^{s}\bar{\gamma}_1^{p+q-M-s-u}}{\bar{\gamma}_B^{m}}e^{-\frac{(n_1+1)(2^R-1)}{\varphi\bar{\gamma}_B}}\xi_1. \end{aligned} \tag{58}$$

em que em ξ_1, $\bar{\gamma}_i = \bar{\gamma}_1$. Igualmente, assumindo $\rho = 1$ em (58), (58) pode ser reduzida para o caso com uma CSI perfeita como

$$P_{\mathrm{s}}^{\mathrm{MRC}}(R) = 1 - \sum_{n_1=1}^{N_{\mathrm{A}}} \binom{N_{\mathrm{A}}}{n_1} \sum_{N_{\mathrm{B}},n_1} (-1)^{n_1+1} \sum_{k=1}^{M} \sum_{p=1}^{k} (-1)^{M-k} \sum_{u=0}^{N_{\mathrm{E}}-1} \sum_{q=0}^{u} \sum_{s=0}^{\beta} \binom{\beta}{s} 2^{R_{\mathrm{s}}} (2^R - 1)^{\beta-s} \times \frac{\Gamma(p+q)}{(M-k)!(k-p)!(u-q)!(p-1)!q!} \frac{\bar{\gamma}_E^s \bar{\gamma}_1^{p+q-M-s-u}}{\bar{\gamma}_B^{\beta}} e^{-\frac{n_1(2^R-1)}{\bar{\gamma}_B}} \xi_2 \tag{59}$$

em que em ξ_2, $\bar{\gamma}_i = \bar{\gamma}_1$. Finalmente, perceba que, todas as expressões obtidas podem ser reduzidas para o caso especial MISO, pressupondo N_B=1, N_E=1, e $u = q = 0$.

3.4.2 *SC em Bob*

Para o caso SC, usando o mesmo raciocínio empregado para o caso MRC e assumindo uma CSI perfeita, após efetuar as substituições apropriadas ((41) e (46) em (49)), seguidas de algumas manipulações algébricas, e a partir de [62, Eq. (9.211.4)], uma expressão analítica fechada para a probabilidade de *outage* de sigilo assumindo sinais com potências de interferência arbitrárias pode ser alcançada como

$$P_{\mathrm{s}}^{\mathrm{SC}}(R) = 1 - \sum_{n=1}^{N_{\mathrm{A}}N_{\mathrm{B}}} \binom{N_{\mathrm{A}}N_{\mathrm{B}}}{n} (-1)^{n+1} \sum_{i=1}^{t} \sum_{j=1}^{\eta_i} \Omega_{i,j} \sum_{k=1}^{j} \sum_{p=1}^{k} (-1)^{j-k} \times \sum_{u=0}^{N_{\mathrm{E}}-1} \sum_{q=0}^{u} \frac{\Gamma(p+q)\bar{\gamma}_i^{p+q-j-u}}{(j-k)!(k-p)!(u-q)!(p-1)!q!} e^{-\frac{n(2^R-1)}{\bar{\gamma}_B}} \xi_3. \tag{60}$$

em que

$$\xi_3 = \left[(p+q)\Gamma(u+1)\Psi\left(u+1, u-p-q+1, \frac{n\bar{\gamma}_E 2^R + \bar{\gamma}_B}{\bar{\gamma}_i \bar{\gamma}_B}\right) + \Gamma(u+1)\frac{1}{\bar{\gamma}_i} \times \Psi\left(u+1, u-p-q+2, \frac{n\bar{\gamma}_E 2^R + \bar{\gamma}_B}{\bar{\gamma}_i \bar{\gamma}_B}\right) - \Theta_1^{\mathrm{SC}} \right]. \tag{61}$$

e

$$\Theta_1^{\mathrm{SC}} = \begin{cases} u\Gamma(u)\Psi\left(u, u-p-q+1, \frac{n\bar{\gamma}_E 2^R + \bar{\gamma}_B}{\bar{\gamma}_i \bar{\gamma}_B}\right), & u \neq 0 \\ 0, & u = 0 \end{cases} \tag{62}$$

Por outro lado, ao reduzir (60) para o caso de potências distintas, tem-se que, através da simplificação de $j = k = p = 1$ em (60), a probabilidade de *outage* de sigilo pode ser reduzida a

$$P_{\mathrm{s}}^{\mathrm{SC}}(R) = 1 - \sum_{n=1}^{N_{\mathrm{A}}N_{\mathrm{B}}} \binom{N_{\mathrm{A}}N_{\mathrm{B}}}{n} (-1)^{n+1} \sum_{i=1}^{M} \bar{\gamma}_i^{M-1} \left[\prod_{k=1,k\neq i}^{t} (\bar{\gamma}_i - \bar{\gamma}_k)^{-1} \right] \times \sum_{u=0}^{N_{\mathrm{E}}-1} \sum_{q=0}^{u} \frac{\Gamma(1+q)\bar{\gamma}_i^{q-u}}{(u-q)!q!} e^{-\frac{n(2^R-1)}{\bar{\gamma}_B}} \xi_3, \tag{63}$$

em que em ξ_3 e Θ_1^{SC}, $p = 1$. Além disso, pressupondo $j = M$ e $\bar{\gamma}_1 = \bar{\gamma}_2 \ldots = \bar{\gamma}_M$ em (60) tem-se o caso de distribuição de potências iguais nos sinais interferentes, ou seja

$$P_{\mathrm{s}}^{\mathrm{SC}}(R) = 1 - \sum_{n=1}^{N_{\mathrm{A}}N_{\mathrm{B}}} \binom{N_{\mathrm{A}}N_{\mathrm{B}}}{n} (-1)^{n+1} \sum_{k=1}^{M} \sum_{p=1}^{k} (-1)^{M-k} \times \sum_{u=0}^{N_{\mathrm{E}}-1} \sum_{q=0}^{u} \frac{\Gamma(p+q)\bar{\gamma}_1^{p+q-M-u}}{(M-k)!(k-p)!(u-q)!(p-1)!q!} e^{-\frac{n(2^R-1)}{\bar{\gamma}_B}} \xi_4, \tag{64}$$

em que em ξ_3, $\bar{\gamma}_i = \bar{\gamma}_1$. Finalmente, perceba que, todas as expressões obtidas para o caso SC podem ser reduzidas para o caso especial MISO, pressupondo N_B=1, N_E=1, e $u = q = 0$.

3.5 Taxa de Sigilo Não-Nula

Demostrado em [3], quando o canal *wiretap* entre Alice e Eve é uma versão degradada do canal de transmissão, Alice e Bob podem trocar mensagens perfeitamente seguras a uma taxa de sigilo não-nula. Esta seção fornece a definição e as expressões fechadas para a probabilidade da taxa de sigilo não-nula. Logo, desde uma perspectiva estatística, pode-se escrever a probabilidade da existência de uma taxa de sigilo não-nula como

$$\begin{aligned} P_{\mathrm{r}}(R_{\mathrm{s}} > 0) &= \Pr(R_{\mathrm{B}} > R_{\mathrm{E}}) = \Pr(\gamma_{\mathrm{B,s}} > \Upsilon_{\mathrm{E,s}}) \\ &= \int_0^{\infty} \int_0^{x} f_{\gamma_{\mathrm{B,s}}}(x) f_{\Upsilon_{\mathrm{E,s}}}(y) dy dx = \int_0^{\infty} \int_0^{x} f_{\gamma_{\mathrm{B,s}}}(x) f_{\frac{\gamma_{\mathrm{E,s}}}{\gamma_{\mathrm{I}}+1}}(y) dy dx. \end{aligned} \tag{65}$$

Assim, com base nas expressões da probabilidade de *outage* de sigilo derivadas anteriormente, a taxa de sigilo não-nula para os esquemas MRC e SC em Bob, podem ser alcançadas. Especificamente, substituindo (37) e (46) em (65), e efetuando as manipulações matemáticas necessárias, a expressão analítica fechada para a técnica MRC em Bob é

$$\breve{P}_{\mathrm{r}}^{\mathrm{MRC}}(R_{\mathrm{s}}>0) = 1 - \frac{N_{\mathrm{A}}}{(N_{\mathrm{B}}-1)!}\sum_{n_1=0}^{N_{\mathrm{A}}-1}(-1)^{n_1}\binom{N_{\mathrm{A}}-1}{n_1}\sum_{N_{\mathrm{B}},n_1}\sum_{\alpha=0}^{\beta}\binom{\beta}{\alpha}\frac{(N_{\mathrm{B}}+\beta-1)!}{(N_{\mathrm{B}}+\alpha-1)!} \times \frac{\rho^{\alpha}(1-\rho)^{\beta-\alpha}}{\varphi^{N_{\mathrm{B}}+\beta+\alpha}}\sum_{i=1}^{t}\sum_{j=1}^{\eta_i}\Omega_{i,j}\sum_{k=1}^{j}\sum_{p=1}^{k}(-1)^{j-k}\sum_{u=0}^{N_{\mathrm{E}}-1}\sum_{q=0}^{u} \times \frac{\Gamma(p+q)\bar{\gamma}_i^{-p+q-j-u}}{(j-k)!(k-p)!(u-q)!(p-1)!q!}\left(\frac{\bar{\gamma}_E}{\bar{\gamma}_i\bar{\gamma}_B}\right)^{N_{\mathrm{B}}+\alpha}\epsilon_1, \tag{66}$$

em que

$$\epsilon_1 = \left[\Gamma(N_{\mathrm{B}}+\alpha+u)\Psi\left(N_{\mathrm{B}}+\alpha+u, N_{\mathrm{B}}+\alpha+u-p-q+1, \frac{(n_1+1)\bar{\gamma}_E+\varphi\bar{\gamma}_B}{\varphi\bar{\gamma}_i\bar{\gamma}_B}\right)\right]. \tag{67}$$

Depois da substituição de (33) e (46) em (65), a taxa de probabilidade de sigilo não-nula assumindo a técnica MRC em Bob com uma CSI perfeita pode ser derivada como

$$P_{\mathrm{r}}^{\mathrm{MRC}}(R_{\mathrm{s}}>0) = 1 - \frac{N_{\mathrm{A}}}{\Gamma(N_{\mathrm{B}})}\sum_{n_1=0}^{N_{\mathrm{A}}-1}\binom{N_{\mathrm{A}}-1}{n_1}\sum_{N_{\mathrm{B}},n_1}(-1)^{n_1}\sum_{i=1}^{t}\sum_{j=1}^{\eta_i}\Omega_{i,j}\sum_{k=1}^{j}\sum_{p=1}^{k}(-1)^{j-k} \times \sum_{u=0}^{N_{\mathrm{E}}-1}\sum_{q=0}^{u}\frac{\Gamma(p+q)\bar{\gamma}_i^{-p+q-j-u}}{(j-k)!(k-p)!(u-q)!(p-1)!q!}\left(\frac{\bar{\gamma}_E}{\bar{\gamma}_i\bar{\gamma}_B}\right)^{N_{\mathrm{B}}+\beta} \times \epsilon_2, \tag{68}$$

em que

$$\epsilon_2 = \left[\Gamma(N_{\mathrm{B}}+\beta+u)\Psi\left(N_{\mathrm{B}}+\beta+u, N_{\mathrm{B}}+\beta+u-p-q+1, \frac{(n_1+1)\bar{\gamma}_E+\bar{\gamma}_B}{\bar{\gamma}_i\bar{\gamma}_B}\right)\right]. \tag{69}$$

Finalmente, assumindo um esquema SC em Bob e levando em conta uma CSI perfeita, após de substituir (40) e (46) em (65), a taxa de probabilidade de sigilo não-nula pode ser derivada como

$$P_{\mathrm{r}}^{\mathrm{SC}}(R_{\mathrm{s}}>0) = 1 - N_{\mathrm{A}}N_{\mathrm{B}}\sum_{n=0}^{N_{\mathrm{A}}N_{\mathrm{B}}-1}\binom{N_{\mathrm{A}}N_{\mathrm{B}}-1}{n}(-1)^{n}\sum_{i=1}^{t}\sum_{j=1}^{\eta_i}\Omega_{i,j}\sum_{k=1}^{j}\sum_{p=1}^{k}(-1)^{j-k} \times \sum_{u=0}^{N_{\mathrm{E}}-1}\sum_{q=0}^{u}\frac{\Gamma(p+q)}{(j-k)!(k-p)!(u-q)!(p-1)!q!}\frac{\bar{\gamma}_i^{-p+q-j-u-1}\bar{\gamma}_E}{\bar{\gamma}_B} \times \left[\Gamma(u+1)\Psi\left(u+1, u-p-q+2, \frac{(n+1)\bar{\gamma}_E+\bar{\gamma}_B}{\bar{\gamma}_i\bar{\gamma}_B}\right)\right]. \tag{70}$$

3.6 Probabilidade de *Outage* de Sigilo Assintótica

A fim de ganhar novas perspectivas para o desempenho de *outage* de sigilo, uma análise assintótica (isto é, regiões de alta SNR) é realizada nesta seção, com base na qual será determinada a ordem de diversidade e o ganho de *array* do cenário proposto. Assim, representando as regiões de alta SNR, assumimos que a SNR média em Bob é maior que a SINR média em Eve, isto é, $\bar{\gamma}_B > \frac{\bar{\gamma}_E}{\bar{\gamma}_{I+1}}$ [24].

3.6.1 *MRC em Bob com CSI perfeita*

Ao usar séries de Taylor e Maclaurin para expandir a função exponencial em (29), $F^{\mathrm{MRC}}_{\gamma_{\mathrm{B},\lambda}}(z)$ pode ser reescrita como

$$F^{\mathrm{MRC}}_{\gamma_{\mathrm{B},\lambda}}(z) = z^{N_B}\left(\frac{\left(\frac{1}{\bar{\gamma}_B}\right)^{N_B}}{\Gamma(N_B)N_B} - \frac{\left(\frac{1}{\bar{\gamma}_B}\right)^{N_B+1} z}{\Gamma(N_B)N_B+1} + \frac{\left(\frac{1}{\bar{\gamma}_B}\right)^{N_B+2} z^2}{2\Gamma(N_B)N_B+2}\ldots\right). \tag{71}$$

Em seguida, através da substituição de (71) em (39), e utilizando o teorema multinomial, seguido de algumas manipulações algébricas, tem-se que em alta SNR $F^{\mathrm{MRC}}_{\gamma_{\mathrm{B,s}}}(.)$ pode ser expressa como

$$F^{\mathrm{MRC}}_{\gamma_{\mathrm{B,s}}}(x) = \frac{x^{N_{\mathrm{A}}N_{\mathrm{B}}}}{\bar{\gamma}_B^{N_{\mathrm{A}}N_{\mathrm{B}}}}\frac{1}{[\Gamma(N_B)N_B]^{N_A}} + o(x^{N_{\mathrm{A}}N_{\mathrm{B}}+1}). \tag{72}$$

em que $\Gamma(N_B)N_B = N_B!$. Finalmente, após à substituição de (72) e (46) em (49), a expressão assintótica de *outage* para o caso MRC pode ser derivada como

$$\begin{aligned}
P_{\mathrm{s}}^{\infty(\mathrm{MRC})}(R) =& \sum_{i=1}^{t}\sum_{j=1}^{\eta_i}\Omega_{i,j}\sum_{k=1}^{j}\sum_{p=1}^{k}\sum_{n=0}^{N_{\mathrm{A}}N_{\mathrm{B}}}\sum_{m=0}^{n}\binom{N_{\mathrm{A}}N_{\mathrm{B}}}{n}\binom{n}{m}(-1)^{N_{\mathrm{A}}N_{\mathrm{B}}+j-k-n}\\
&\times\sum_{u=0}^{N_{\mathrm{E}}-1}\sum_{q=0}^{u}\frac{\Gamma(p+q)\bar{\gamma}_i^{p+q-j-m-u}\bar{\gamma}_E^{m}}{(j-k)!(k-p)!(u-q)!(p-1)!q!}\frac{1}{N_{\mathrm{B}}!^{N_{\mathrm{A}}}}\\
&\times\left[(p+q)\Gamma(m+u+1)\Psi\left(m+u+1,m+u-p-q+1,\frac{1}{\bar{\gamma}_i}\right)+\Gamma(m+u+1)\right.\\
&\left.\times\frac{1}{\bar{\gamma}_i}\,\Psi\left(m+u+1,m+u-p-q+2,\frac{1}{\bar{\gamma}_i}\right)-\Theta_1^{\infty\mathrm{MRC}}\right]\frac{1}{\bar{\gamma}_B^{N_{\mathrm{A}}N_{\mathrm{B}}}}.
\end{aligned} \tag{73}$$

em que

$$\Theta_1^{\infty\mathrm{MRC}} = \begin{cases} u\Gamma(m+u)\Psi\left(m+u, m+u-p-q+1, \frac{1}{\bar{\gamma}_i}\right), & u \neq 0 \\ 0, & u = 0 \end{cases} \tag{74}$$

Da literatura [17], é conhecido que uma expressão de *outage* assintótica pode ser escrita geralmente como

$$P_{\mathrm{s}}^{\infty}(R) = G_{\mathrm{A}}(\bar{\gamma}_B)^{-G_{\mathrm{D}}} + o(\bar{\gamma}_B^{-G_{\mathrm{D}}}). \tag{75}$$

em que $o(x)$ denota o termo de ordem superior em relação a x, que satisfaz $\lim_{x\to 0} o(x)/x = 0$, enquanto G_{A} e G_{D} simbolizam, respectivamente, o ganho de *array* e o ganho de diversidade do sistema. Acima, a expressão assintótica de *outage* mostra que o ganho de diversidade é igual a $G_{\mathrm{D}} = N_{\mathrm{A}}N_{\mathrm{B}}$. Isto permite garantir que o ganho de diversidade é limitado apenas pelo número de antenas em Alice e Bob, independentemente da quantidade de sinais de interferência que chegam a Eve, bem como pelo número de antenas no nó intruso. Curiosamente, tal observação difere de [17], no qual foi assumido um cenário limitado somente por interferência em Eve, e o ganho de diversidade foi dado por $G_{\mathrm{D}} = min(N_{\mathrm{A}}N_{\mathrm{B}}, M)$. Em outras palavras, nos casos práticos, é importante considerar a SINR em vez da SIR no nó intruso, a fim de obter resultados mais precisos e realistas. Além disso, por meio da comparação de (73) com (75), o ganho de *array* pode ser escrito como

$$\begin{aligned} G_{\mathrm{A}}^{\mathrm{MRC}} =& \sum_{i=1}^{t}\sum_{j=1}^{\eta_i}\Omega_{i,j}\sum_{k=1}^{j}\sum_{p=1}^{k}\sum_{n=0}^{N_{\mathrm{A}}N_{\mathrm{B}}}\sum_{m=0}^{n}\binom{N_{\mathrm{A}}N_{\mathrm{B}}}{n}\binom{n}{m}(-1)^{N_{\mathrm{A}}N_{\mathrm{B}}+j-k-n} \\ &\times \sum_{u=0}^{N_{\mathrm{E}}-1}\sum_{q=0}^{u}\frac{\Gamma(p+q)\bar{\gamma}_i^{p+q-j-m-u}\bar{\gamma}_E^{m}}{(j-k)!(k-p)!(u-q)!(p-1)!q!}\frac{1}{N_{\mathrm{B}}!^{N_{\mathrm{A}}}} \\ &\times \left[(p+q)\Gamma(m+u+1)\Psi\left(m+u+1, m+u-p-q+1, \frac{1}{\bar{\gamma}_i}\right) + \Gamma(m+u+1)\right. \\ &\left.\times \frac{1}{\bar{\gamma}_i}\,\Psi\left(m+u+1, m+u-p-q+2, \frac{1}{\bar{\gamma}_i}\right) - \Theta_1^{\infty\mathrm{MRC}}\right]. \end{aligned} \tag{76}$$

com $\Theta_1^{\infty\mathrm{MRC}}$ anteriormente definido em (74). Finalmente, para o caso especial MISO, as expressões (73) e (76) são reduzidas assumindo $N_B = N_E = 1$.

3.6.2 *MRC em Bob com CSI imperfeita*

Usando uma lógica semelhante, ou seja, expandindo a função exponencial em (38) e utilizando a série de Taylor, mantemos os dois primeiros termos e obtemos a nova $F_{\bar{\gamma}_{\mathrm{B,s}}}^{\mathrm{MRC}}$ para uma CSI desatualizada como

$$F_{\breve{\gamma}_{\mathrm{B,s}}^{\mathrm{MRC}}}(\vartheta) = \frac{N_A}{(N_B-1)!}\sum_{n_1=0}^{N_{\mathrm{A}}-1}\binom{N_{\mathrm{A}}-1}{n_1}(-1)^{n_1}\sum_{N_B,n_1}\frac{(N_B+\beta-1)!}{N_B!}\frac{(1-\rho)^{\beta}}{\varphi^{\beta+N_B}} \times\left(\frac{\vartheta}{\bar{\gamma}_B}\right)^{N_{\mathrm{B}}}+o\left[\left(\frac{\vartheta}{\bar{\gamma}_B}\right)^{N_{\mathrm{B}}}\right]. \tag{77}$$

Assim, depois da substituição de (77) e (46) em (49), uma expressão assintótica para a probabilidade de *outage* de sigilo com *feedback* imperfeito pode ser derivada como

$$\begin{aligned}\breve{P}_{\mathrm{s}}^{\infty(\mathrm{MRC})}(R) =& \frac{N_{\mathrm{A}}}{(N_{\mathrm{B}}-1)!}\sum_{n_1=0}^{N_{\mathrm{A}}-1}(-1)^{n_1}\binom{N_{\mathrm{A}}-1}{n_1}\sum_{N_B,n_1}\frac{(N_B+\beta-1)!}{N_B!}\frac{(1-\rho)^{\beta}}{\varphi^{\beta+N_B}}\\ &\times\sum_{m=0}^{N_{\mathrm{B}}}(-1)^{N_{\mathrm{B}}-m}\binom{N_{\mathrm{B}}}{m}2^{Rm}\sum_{v=0}^{m}\binom{m}{v}\sum_{i=1}^{t}\sum_{j=1}^{\eta_i}\Omega_{i,j}\sum_{k=1}^{j}\sum_{p=1}^{k}(-1)^{j-k}\\ &\times\sum_{u=0}^{N_{\mathrm{E}}-1}\sum_{q=0}^{u}\frac{\Gamma(p+q)\bar{\gamma}_E^{v}\bar{\gamma}_i^{p+q-j-v-u}}{(j-k)!(k-p)!(u-q)!(p-1)!q!}\\ &\times\left[(p+q)\Gamma(v+u+1)\Psi\left(v+u+1,v+u-p-q+1,\frac{1}{\bar{\gamma}_i}\right)+\Gamma(v+u+1)\right.\\ &\left.\times\frac{1}{\bar{\gamma}_i}\,\Psi\left(v+u+1,v+u-p-q+2,\frac{1}{\bar{\gamma}_i}\right)-\Theta_2^{\infty\mathrm{MRC}}\right]\frac{1}{\bar{\gamma}_B^{N_{\mathrm{B}}}}.\end{aligned} \tag{78}$$

em que

$$\Theta_2^{\infty\mathrm{MRC}}=\begin{cases}u\Gamma(v+u)\Psi\left(v+u,v+u-p-q+1,\frac{1}{\bar{\gamma}_i}\right), & u\neq 0\\ 0, & u=0\end{cases} \tag{79}$$

Acima, nota-se que, com uma CSI desatualizada, a ordem de diversidade completa não pode ser realizada, e o ganho de diversidade é reduzido a $G_{\mathrm{D}}=N_{\mathrm{B}}$. No entanto, observa-se que tanto para o *feedback* perfeito quanto para o *feedback* imperfeito, o ganho de diversidade não é limitado pelos parâmetros do nó malicioso e/ou pelo número de sinais de interferência. Da mesma forma, o ganho de *array* pode ser escrito como

$$\breve{G}_{\mathrm{A}}^{\mathrm{MRC}} = \frac{N_{\mathrm{A}}}{(N_{\mathrm{B}}-1)!}\sum_{n_1=0}^{N_{\mathrm{A}}-1}(-1)^{n_1}\binom{N_{\mathrm{A}}-1}{n_1}\sum_{N_B,n_1}\frac{(N_B+\beta-1)!}{N_B!}\frac{(1-\rho)^{\beta}}{\varphi^{\beta+N_B}}\sum_{m=0}^{N_{\mathrm{B}}}(-1)^{N_{\mathrm{B}}-m}\binom{N_{\mathrm{B}}}{m}2^{Rm}$$
$$\times\sum_{v=0}^{m}\binom{m}{v}\sum_{i=1}^{t}\sum_{j=1}^{\eta_i}\Omega_{i,j}\sum_{k=1}^{j}\sum_{p=1}^{k}(-1)^{j-k}\sum_{u=0}^{N_{\mathrm{E}}-1}\sum_{q=0}^{u}\frac{\Gamma(p+q)\bar{\gamma}_E^{v}\bar{\gamma}_i^{p+q-j-v-u}}{(j-k)!(k-p)!(u-q)!(p-1)!q!}$$
$$\times\left[(p+q)\Gamma(v+u+1)\Psi\left(v+u+1,v+u-p-q+1,\frac{1}{\bar{\gamma}_i}\right)+\Gamma(v+u+1)\right.$$
$$\left.\times\frac{1}{\bar{\gamma}_i}\,\Psi\left(v+u+1,v+u-p-q+2,\frac{1}{\bar{\gamma}_i}\right)-\Theta_2^{\infty\mathrm{MRC}}\right]. \tag{80}$$

3.6.3 *SC em Bob*

Em primeiro lugar, o termo $e^{-\frac{nx}{\bar{\gamma}_B}}$ é expandido usando a série de Maclaurin de modo que (41) pode ser reescrita como

$$F_{\gamma_{\mathrm{B,s}}}^{\mathrm{SC}}(x) = 1 - \sum_{n=1}^{N_{\mathrm{A}}N_{\mathrm{B}}}(-1)^{n+1}\binom{N_{\mathrm{A}}N_{\mathrm{B}}}{n}\sum_{m=0}^{\infty}\frac{(-1)^m}{m!}\frac{n^m x^m}{\bar{\gamma}_B^m}. \tag{81}$$

Sabendo que os $n < N_{\mathrm{A}}N_{\mathrm{B}}$ termos em (81) somam zero, (81) pode ser simplificada depois de algumas operações matemáticas para

$$F_{\gamma_{\mathrm{B,s}}}^{\mathrm{SC}}(x) = \frac{x^{N_{\mathrm{A}}N_{\mathrm{B}}}}{\bar{\gamma}_B^{N_{\mathrm{A}}N_{\mathrm{B}}}} + o(x^{N_{\mathrm{A}}N_{\mathrm{B}}+1}), \tag{82}$$

Logo, substituindo (82) e (46) em (49), e utilizando o teorema binomial e algumas manipulações algébricas, a integral necessária é resolvida com a ajuda de [62, Eq. (9.211.4)], de modo que uma expressão assintótica para a probabilidade de *outage* de sigilo, assumindo um esquema SC em Bob pode ser obtida como

$$P_{\mathrm{s}}^{\infty(\mathrm{SC})}(R) = \sum_{i=1}^{t}\sum_{j=1}^{\eta_i}\Omega_{i,j}\sum_{k=1}^{j}\sum_{p=1}^{k}\sum_{n=0}^{N_{\mathrm{A}}N_{\mathrm{B}}}\sum_{m=0}^{n}\binom{N_{\mathrm{A}}N_{\mathrm{B}}}{n}\binom{n}{m}(-1)^{N_{\mathrm{A}}N_{\mathrm{B}}+j-k-n}$$
$$\times\sum_{u=0}^{N_{\mathrm{E}}-1}\sum_{q=0}^{u}\frac{\Gamma(p+q)\bar{\gamma}_i^{p+q-j-m-u}\bar{\gamma}_E^{m}}{(j-k)!(k-p)!(u-q)!(p-1)!q!}$$
$$\times\left[(p+q)\Gamma(m+u+1)\Psi\left(m+u+1,m+u-p-q+1,\frac{1}{\bar{\gamma}_i}\right)+\Gamma(m+u+1)\right.$$
$$\left.\times\frac{1}{\bar{\gamma}_i}\,\Psi\left(m+u+1,m+u-p-q+2,\frac{1}{\bar{\gamma}_i}\right)-\Theta_2^{SC}\right]\frac{1}{\bar{\gamma}_B^{N_{\mathrm{A}}N_{\mathrm{B}}}}. \tag{83}$$

em que

$$\Theta_2^{\mathrm{SC}} = \begin{cases} u\Gamma(m+u)\Psi\left(m+u, m+u-p-q+1, \frac{1}{\bar{\gamma}_i}\right), & u \neq 0 \\ 0, & u = 0 \end{cases} \tag{84}$$

Então, por uma comparação entre (83) e (75), segue-se que G_{A} pode ser escrito como

$$\begin{aligned} G_{\mathrm{A}}^{\mathrm{SC}} =& \sum_{i=1}^{t}\sum_{j=1}^{\eta_i}\Omega_{i,j}\sum_{k=1}^{j}\sum_{p=1}^{k}\sum_{n=0}^{N_{\mathrm{A}}N_{\mathrm{B}}}\sum_{m=0}^{n}\binom{N_{\mathrm{A}}N_{\mathrm{B}}}{n}\binom{n}{m}(-1)^{N_{\mathrm{A}}N_{\mathrm{B}}+j-k-n} \\ &\times \sum_{u=0}^{N_{\mathrm{E}}-1}\sum_{q=0}^{u}\frac{\Gamma(p+q)\bar{\gamma}_i^{p+q-j-m-u}\bar{\gamma}_E^{m}}{(j-k)!(k-p)!(u-q)!(p-1)!q!} \\ &\times \left[(p+q)\Gamma(m+u+1)\Psi\left(m+u+1, m+u-p-q+1, \frac{1}{\bar{\gamma}_i}\right) + \Gamma(m+u+1)\right. \\ &\left.\times \frac{1}{\bar{\gamma}_i}\,\Psi\left(m+u+1, m+u-p-q+2, \frac{1}{\bar{\gamma}_i}\right) - \Theta_2^{\mathrm{SC}}\right]. \end{aligned} \tag{85}$$

em que Θ_2^{SC} foi definida em (84). Logo, por meio de uma abordagem análoga à utilizada nas subseções anteriores, para sintetizar a análise assintótica para o caso MISO, é só levar $N_B = N_E = 1$ nas expressões (83) e (85) respectivamente.

Também, de (75) pode-se observar que o ganho de diversidade é igual a $G_{\mathrm{D}} = N_A N_B$, similar ao caso MRC com uma CSI perfeita, o que leva a concluir que assumindo as duas, interferência e ruído em Eve, o ganho de diversidade é limitado apenas pelo número de antenas em Alice e Bob, não dependendo do número de sinais de interferência, bem como pelo número de antenas no nó malicioso. Nota-se ainda, que para o caso MISO, como esperado, o ganho de diversidade é limitado somente pelo número de antenas no transmissor, ou seja $G_{\mathrm{D}} = N_A$.

3.7 Conclusões

Neste capítulo foi analisado o desempenho de *outage* de sigilo de um canal MIMO *wiretap*, assumindo que o nó malicioso é afetado por sinais de interferência e ruído. Paralelamente, foi analisado o caso MISO como caso especial. Na seção 3.2 foi apresentado o modelo sistêmico proposto nesta dissertação. Em seguida, na seção 3.3, foi realizada uma breve revisão estatística, especificamente na subseção 3.3.1, com base na qual foram obtidas as expressões analíticas fechadas que descrevem a probabilidade de *outage* de sigilo e a taxa de sigilo não-nula, nas subsecões 3.4 e 3.5, respectivamente. Finalmente, uma análise assintótica foi desenvolvida na seção 3.6, determinando a ordem de diversidade do sistema, e obtendo individualmente o ganho de diversidade e o ganho de *array*.

Em resumo, nota-se que, quando são assumidos tanto sinais interferentes quanto ruído em Eve, o ganho de diversidade do sistema é limitado pelo número de antenas em Alice e Bob quando uma CSI perfeita é assumida, e apenas pelo número de antenas em Bob quando é analisado o caso com atraso no *feedback*. Portanto, o ganho de diversidade é independente do número de antenas no nó intruso e do número de sinais de interferência que chegam a Eve. Porém, o ganho de *array* do sistema é afetado por ambos, o número de antenas em Eve e o número de sinais de interferência, afetando o desempenho de *outage* de canais *wiretap* MIMO. Além disso, até onde vai o conhecimento deste autor, todas as expressões derivadas são novas e levam a conclusões que nunca foram relatadas na literatura.

4 RESULTADOS NUMÉRICOS E DISCUSSÕES

4.1 Introdução

neste capítulo, alguns resultados numéricos representativos serão apresentados, a fim de avaliar os efeitos de alguns dos parâmetros sistêmicos (ou seja, o número de antenas, o número de sinais de interferência, o padrão de potências de interferência) sobre o desempenho de *outage* de sigilo. Além disso, todas as análises propostas serão validadas através de simulações de Monte Carlo. Como será observado, para todos os casos, evidencia-se uma excelente concordância entre as curvas analíticas e as simuladas. Para as figuras, a notação $\gamma_i = [abc]$ dB representa a adoção de três sinais de interferência com potências médias a, b e c dB, respectivamente.

4.2 Simulações de Monte Carlo

Ao longo deste capítulo, as curvas simuladas serão geradas utilizando o método de Monte Carlo. Uma aproximação de Monte Carlo é uma boa opção quando se deseja calcular os índices de confiabilidade de um sistema, simulando o processo e o comportamento aleatório do mesmo [66]. Este método aborda um problema como uma série de experiências reais, e tem como vantagem, a viabilidade de ter em conta, teoricamente, cada variável aleatória, cada contingência, e a possibilidade de adotar políticas semelhantes à operação real. A única desvantagem do método poderia ser o tempo de simulação necessária, dependendo da capacidade de computação disponível.

Conforme [65], estatisticamente o método de Monte Carlo baseia-se na interpretação de frequência relativa de probabilidade, sendo a probabilidade $\Pr[\psi]$ de um evento ψ, definida pelo limite

$$\Pr(\psi) = \lim_{n\to\infty} \frac{n_\psi}{n}, \tag{86}$$

em que n_ψ é o número de ocorrências de ψ, e n é o número de ensaios. Logo para o caso real em que $n < \infty$, $\frac{n_\psi}{n}$ é uma estimativa da $\Pr[\psi]$.

Então, utilizando esse raciocínio para prover uma estimativa da probabilidade de *outage* de sigilo do sistema, a seguir serão validados todos os resultados numéricos através de simulações de Monte Carlo, considerando 10^5 iterações em cada caso.

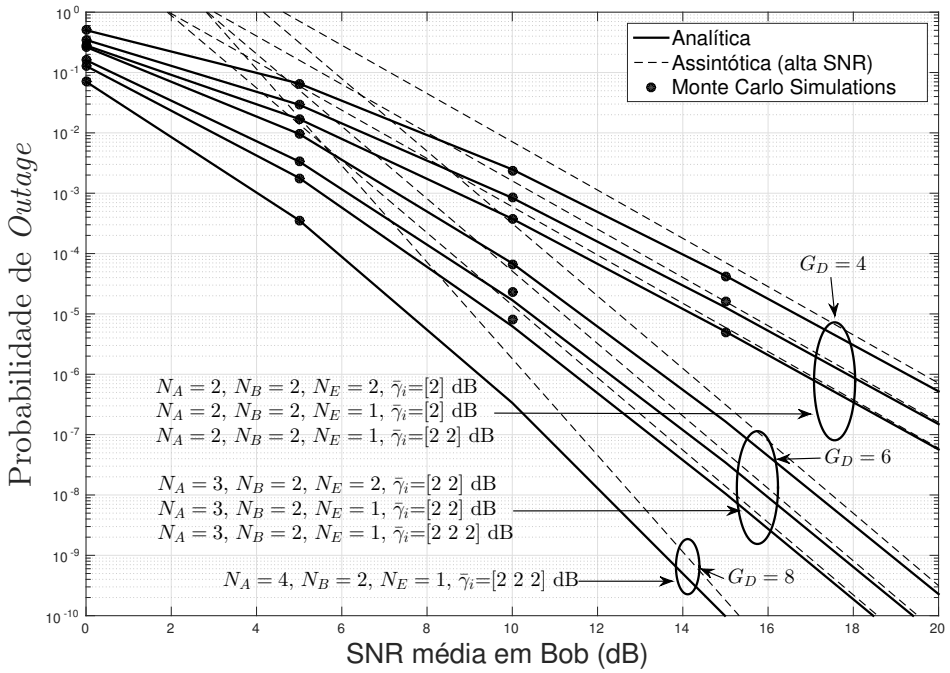
4.3 Apresentação dos Resultados Numéricos

Em capítulos anteriores, as expressões analíticas exatas, bem como as expressões aproximadas assintóticas que regem o desempenho de *outage* de sigilo no modelo sistêmico proposto, foram obtidas. Nesta seção, a avaliação destas expressões através de resultados numéricos será realizada, em que serão simuladas situações e configurações diferentes, a fim de um melhor esclarecimento da influência de cada um dos principais parâmetros do sistema no desempenho de *outage* de sigilo.

A Figura 11, descreve a probabilidade de *outage* de sigilo em relação à SNR média em Bob assumindo um esquema SC em Bob, e para o caso em que todos os sinais interferentes possuem uma distribuição de potências iguais. Na Figura 11, $\gamma_i = [a]; [a, a]; [a, a, a]$ representam $M = 1, 2$ e 3, com potência média a. Como observado, mantendo-se inalterado o número de antenas em Alice e Bob, o ganho de diversidade mantém um valor constante, mesmo variando a quantidade de sinais de interferência que chegam a Eve. Este resultado esperado, é perceptível nas três curvas de nível superior, em que com N_A e N_B igual a 2, o ganho de diversidade é 4 ($G_\mathrm{D} = 4$). Isto mostra que o ganho de diversidade é governado apenas pelo número de antenas no Tx e no Rx legítimo, e o valor quantitativo é o produto de N_A por N_B. Perceba também que, a partir das três curvas de nível superior, que a última curva proporciona um melhor desempenho de *outage* de sigilo devido ao aumento do ganho de *array*, uma vez que o número de sinais interferentes M aumenta de 1 para 2. Além disso, ao comparar as duas primeiras curvas, observa-se que uma variação do número de antenas em Eve (N_E varia de 2 a 1), não implica um reforço no ganho de diversidade, mas mostra uma melhoria da probabilidade de *outage* de sigilo com a diminuição de N_E, como esperado. Um comportamento semelhante foi observado para o grupo das três curvas intermediárias. Da Figura 11, pode-se também distinguir que, ao manter inalterado $N_B = 2$, e ao aumentar o número de antenas em Alice para $N_A = 3$, o ganho de diversidade aumenta para $G_\mathrm{D} = 6$, confirmando o resultado discutido acima. Além disso, o aumento do número de sinais de interferência de 2 para 3, o desempenho *outage* de sigilo melhora devido a um aumento do ganho de

array, mantendo ao mesmo tempo o ganho de diversidade igual a 6.

Figura 11: Probabilidade de *outage* de sigilo versus SNR média em Bob assumindo esquema SC em Bob. Premissas: $\bar{\gamma}_E = -3$dB; $R = 1$; sinais interferentes com distribuição de potências iguais.



Fonte: Próprio autor.

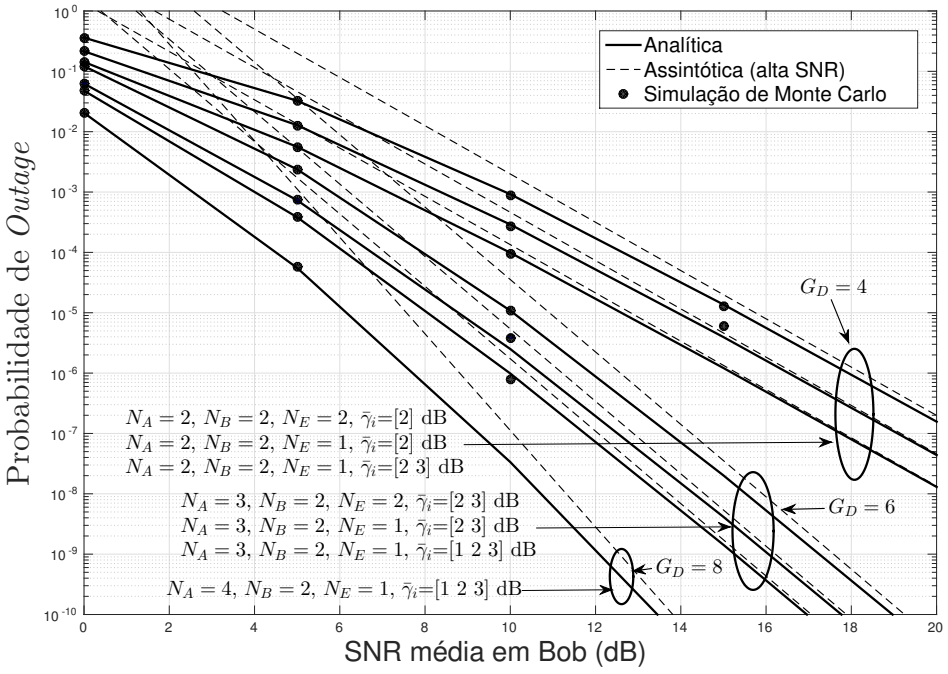
A Figura 12 representa a probabilidade de *outage* de sigilo versus SNR média em Bob assumindo um esquema MRC no receptor com CSI perfeita, bem como uma distribuição de potências distintas nos sinais de interferência.

As mesmas conclusões observadas na Figura 11 podem ser aplicadas à Figura 12. Também, comparando as Figuras 11 e 12, pode-se perceber que o desempenho de *outage* do esquema MRC supera o desempenho do esquema SC, conforme esperado.

As Figuras 13 e 14 representam análises semelhantes às Figuras 11 e 12, mas ilustrando o desempenho de *outage* de sigilo de um canal MISO *wiretap*, como caso especial do canal MIMO, assumindo apenas uma antena no Rx legítimo e no nó malicioso, isto é, $N_B = 1$ e $N_E = 1$. Nas Figuras 13 e 14, são assumidas as mesmas premissas e notações utilizadas nas Figuras 11 e 12, analisando o caso do esquema SC com distribuição de potências iguais na Figura. 13, e o caso do esquema MRC com distribuição de potências distintas na Figura 14, podendo-se observar que as conclusões listadas acima, são satisfeitas para o caso especial do canal MISO, como esperado.

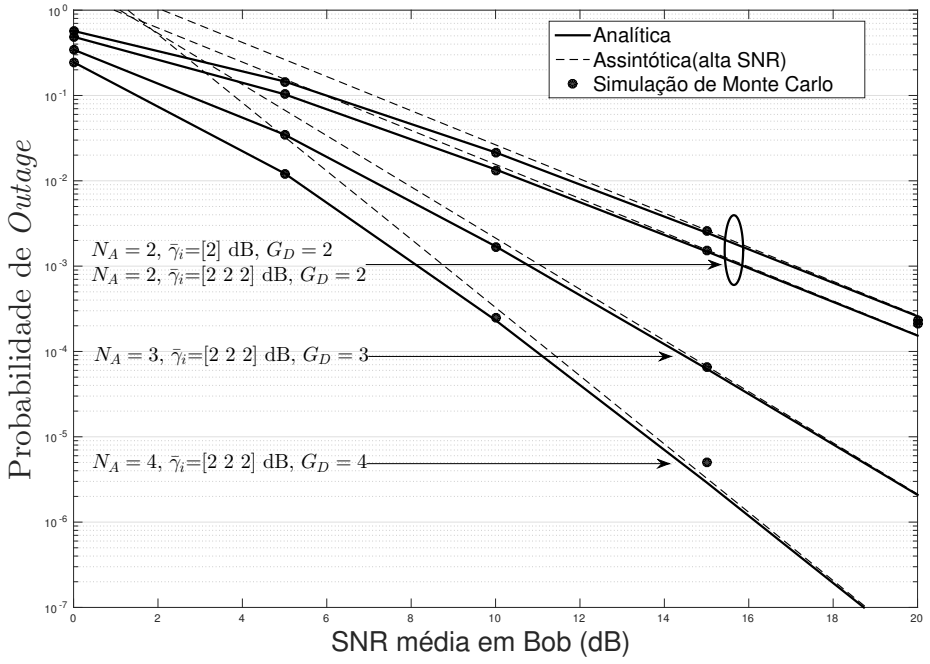
Das curvas nas Figuras 13 e 14, pode-se concluir que o ganho de diversidade é apenas governado pelo número de antenas em Alice, ($G_\mathrm{D} = N_A$). Perceba também que,

Figura 12: Probabilidade de *outage* de sigilo versus SNR média em Bob assumindo esquema MRC em Bob com CSI perfeita. Premissas: $\bar{\gamma}_E = -3$dB; $R = 1$; sinais interferentes com distribuição de potências distintas.



Fonte: Próprio autor.

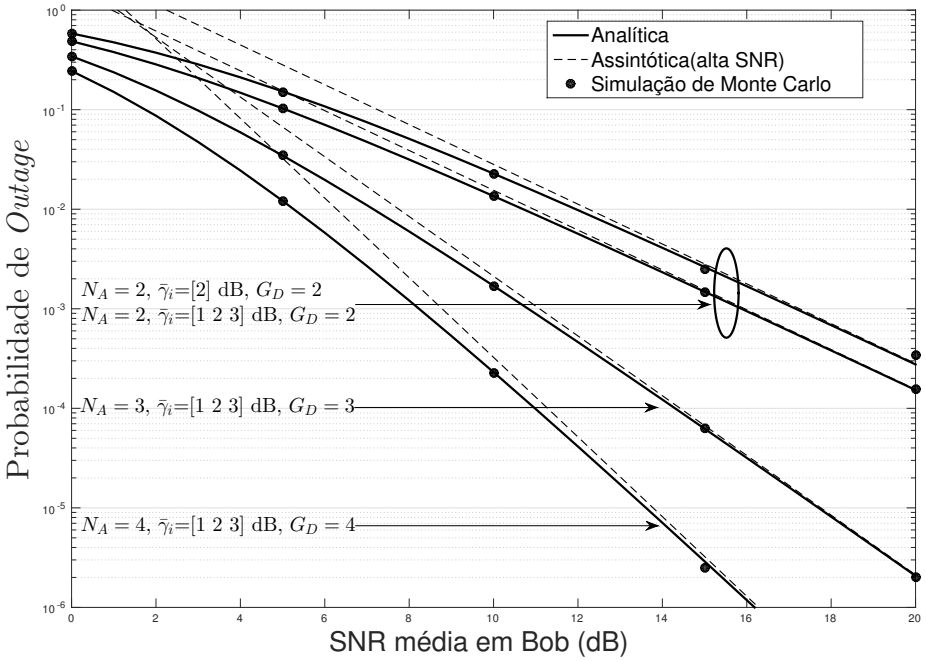
Figura 13: Probabilidade de *outage* de sigilo versus SNR média em Bob assumindo esquema SC em Bob e um canal MISO. Premissas: $\bar{\gamma}_E = -3$dB; $R = 1$; sinais interferentes com distribuição de potências iguais.



Fonte: Próprio autor.

nas duas curvas de nível superior, mantendo constante $N_A = 2$, o ganho de diversidade é 2 ($G_\mathrm{D} = 2$), embora o número de sinais de interferências M aumente de 1 para 3. Além disso, a segunda curva proporciona um desempenho de *outage* de sigilo melhorado em comparação com o desempenho da primeira curva, como consequência do aumento do ganho do *array* ao aumentar M de 1 para 3. Por outra parte, as duas curvas de nível inferior nas duas figuras, representam $N_A = 3$ e $N_A = 4$, com $G_\mathrm{D} = 3$ e $G_\mathrm{D} = 4$, respectivamente, reforçando os resultados alcançados. Finalmente, ao comparar as Figuras 13 e 14, pode-se notar que o desempenho de *outage* de sigilo do esquema MRC é superior ao desempenho do esquema SC, similar à comparação entre as Figuras 11 e 12 para o caso MIMO.

Figura 14: Probabilidade de *outage* de sigilo versus SNR média em Bob assumindo esquema MRC em Bob e um canal MISO. Premissas: $\bar{\gamma}_E = -3$dB; $R = 1$; sinais interferentes com distribuição de potências distintas.

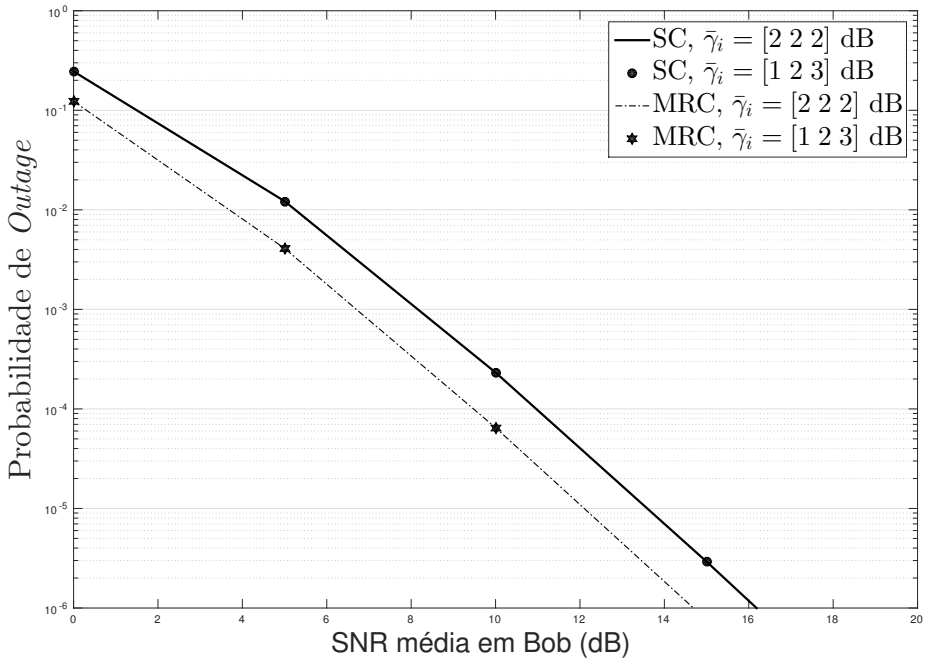


Fonte: Próprio autor.

A Figura 15 mostra a probabilidade de *outage* de sigilo versus SNR média em Bob com $M = 3$ para os esquemas SC e MRC com CSI perfeita. São assumidas iguais configurações de antenas em todos os nós do sistema para o traçado das curvas, neste caso $N_A = N_B = 2$ e $N_E = 1$, mas os sinais interferentes são considerados com distribuição de potências diferentes e iguais simultaneamente para cada esquema, procurando destacar o efeito de diferentes sinais de interferência atingindo Eve. A primeira conclusão da Figura 15, como esperado, é que o regime MRC supera em probabilidade de *outage* de sigilo ao esquema SC. Observa-se também que, para as duas distribuições de potências nos sinais

interferentes, as curvas têm o mesmo desempenho quando têm o mesmo número de sinais de interferência e quando a soma das potências médias de interferência são iguais. Esta observação é de suma importância, mostrando que é possível usar o sistema simplificado de sinais interferentes com distribuição igual de potências na avaliação do desempenho de *outage* de sigilo. Mais uma vez, as simulações de Monte Carlo são coincidentes com as curvas analíticas, corroborando nossos resultados.

Figura 15: Probabilidade de *outage* de sigilo versus SNR média em Bob para diferentes esquemas de combinação de sinal e configurações de interferência. Premissas: $N_A = N_B = 2$, $N_E = 1$, $\bar{\gamma}_E = -3$dB; $R = 1$; sinais interferentes com distribuição de potências distintas.



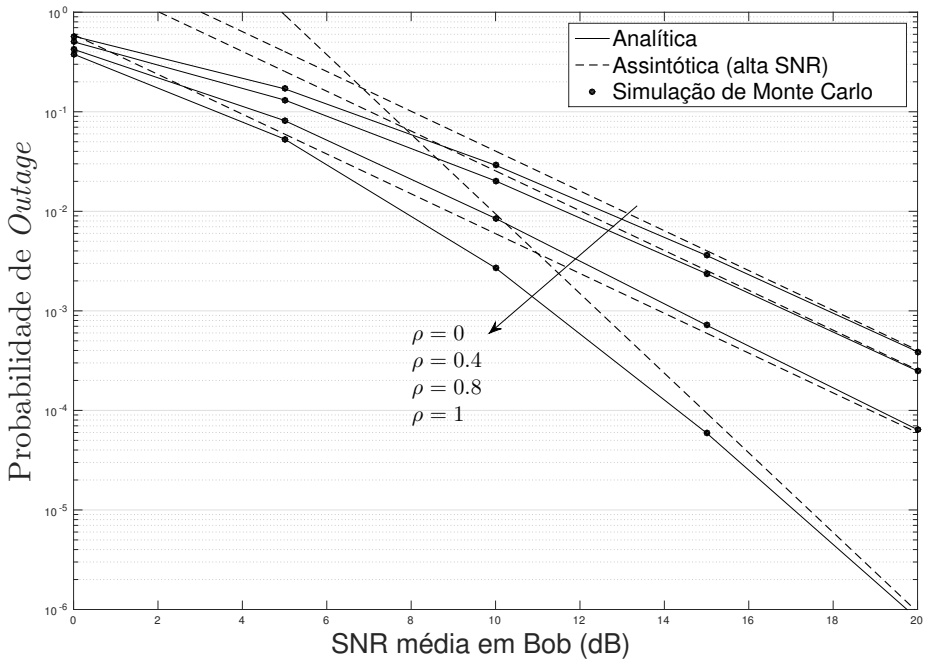
Fonte: Próprio autor.

A fim de demonstrar o efeito de uma CSI desatualizada sobre o desempenho de *outage* de sigilo, a Figura 16 ilustra a probabilidade de *outage* em relação à SNR média em Bob assumindo um esquema MRC em Bob para diferentes valores do coeficiente de correlação ρ. Como notado, um *feedback* desatualizado tem um impacto importante sobre o desempenho de *outage*. Os resultados mostram uma perda na probabilidade de *outage* de sigilo à medida que os atrasos de *feedback* aumentam, isto é, os valores de ρ diminuem. Para o caso de $\rho = 0$, o feedback é severamente desatualizado, e a estratégia TAS não pode obter qualquer ganho de desempenho. Nestas condições, um aumento de N_A não tem qualquer impacto sobre a capacidade de *outage*, o que seria o caso para $N_A = 1$. Além disso, o máximo de desempenho de *outage* de sigilo alcançado através da estratégia de diversidade espacial TAS/MRC é obtido quando não há atraso de *feedback*, $\rho = 1$. Neste caso, o ganho de diversidade para as curvas com algum atraso no *feedback* é igual

a 2, devido ao fato de $N_B = 2$, enquanto que $G_{\mathrm{D}} = 4$ para o caso de assumir uma CSI perfeita, com N_A e N_B igual a 2.

O efeito do coeficiente de correlação ρ sobre o desempenho de *outage* de sigilo pode ser observado melhor na Figura 17. Nota-se que, para diferentes configurações de antenas em Eve e variando o números de sinais interferentes, à medida que os valores de ρ aumentam (os atrasos de *feedback* diminuem até o caso de CSI perfeita com $\rho = 1$), melhora o desempenho de *outage* do sistema. Observa-se além, como as curvas experimentam uma queda importante a partir de $\rho = 0,8$, até chegar ao valor máximo de ganho de diversidade para $\rho = 1$.

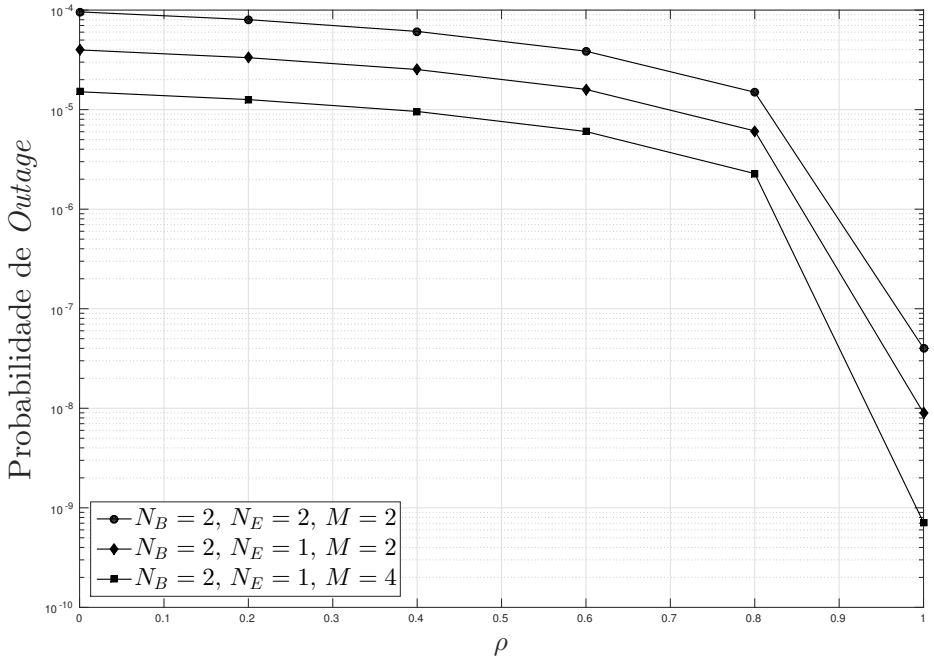
Figura 16: Probabilidade de *outage* de sigilo versus SNR média em Bob assumindo esquema MRC em Bob com CSI imperfeita para diferentes valores de ρ. Premissas: $\bar{\gamma}_E = 3$ dB; $R = 1$; $N_{\mathrm{A}} = N_{\mathrm{B}} = N_{\mathrm{E}} = 2$; sinais interferentes com distribuição de potências distintas com $\bar{\gamma}_i$=[1 2] dB.



Fonte: Próprio autor.

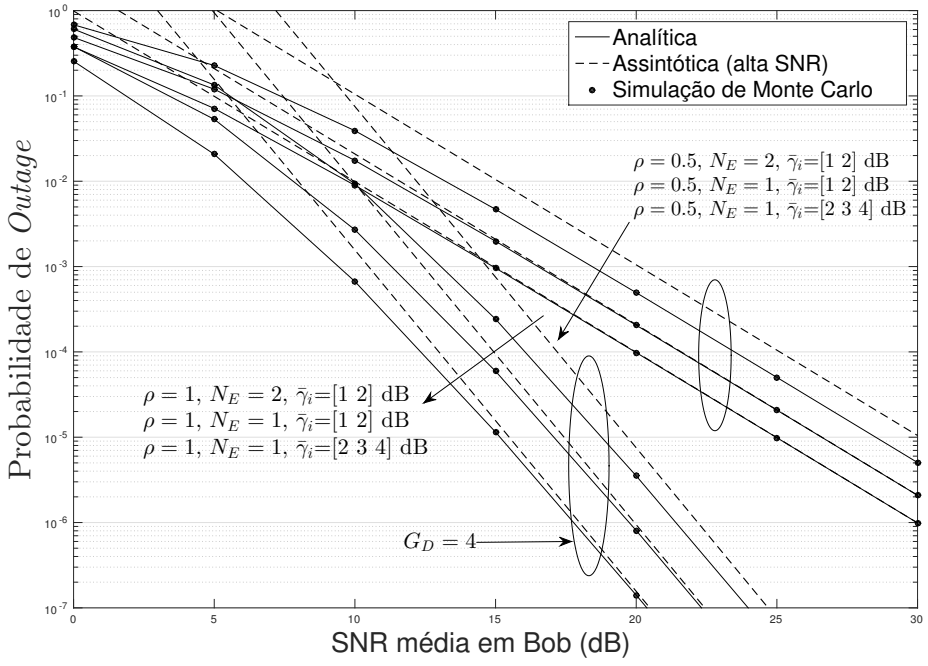
O efeito do número de antenas em Eve e o número de sinais de interferência no desempenho de *outage* de sigilo com uma CSI imperfeita é mostrado na Figura 18 . A Figura 18 representa a probabilidade de *outage* de sigilo em relação à SNR média em Bob. Como observado, mantendo inalterado o número de antenas em Alice e Bob, o ganho de diversidade mantém um valor constante, mesmo variando o número de sinais de interferência que chegam a Eve e/ou o número de antenas em Eve. Por exemplo, nas três curvas de nível superior, o ganho de diversidade é 2 ($G_{\mathrm{D}} = 2$), porque existe atraso de feedback e o ganho de diversidade apenas é governado pelo número de antenas em Bob ($N_B = 2$). No entanto, ao diminuir o número de antenas em Eve e/ou aumentar o número

Figura 17: Probabilidade de *outage* de sigilo versus ρ assumindo esquema MRC em Bob. Premissas: $\bar{\gamma}_E = 3$ dB; $R = 1$; $\bar{\gamma}_B = 25$ dB; sinais interferentes com distribuição de potências distintas.



Fonte: Próprio autor.

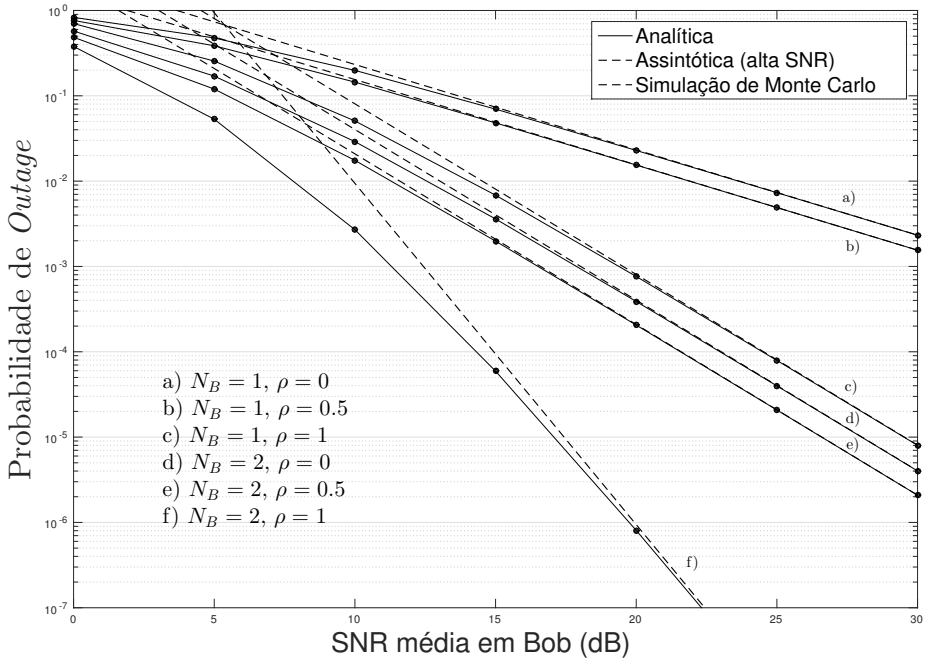
Figura 18: Probabilidade de *outage* de sigilo versus SNR média em Bob assumindo esquema MRC em Bob com CSI imperfeita. Premissas: $\bar{\gamma}_E = 3$dB; $R_0 = 1$; $N_{\mathrm{A}} = N_{\mathrm{B}} = 2$; $\bar{\gamma}_E = 3$dB; sinais interferentes com distribuição de potências distintas com $\bar{\gamma}_i = \{(1,2),(2,3,4)\}$dB para $M = 2, 3$.



Fonte: Próprio autor.

de sinais de interferência, é alcançada uma melhoria no desempenho de *outage* de sigilo devido ao aumento do ganho de *array*. Comparando as duas primeiras curvas, observa-se que uma variação no número de antenas em Eve (N_E varia de 2 a 1), implica uma melhoria da probabilidade de *outage* de sigilo com a diminuição de N_E. De forma semelhante, observa-se um melhor desempenho de *outage* de sigilo na última curva, uma vez que o número de sinais interferentes M aumenta de 2 para 3, aumentando o ganho de *array*. Um comportamento semelhante é observado para o grupo das três últimas curvas, do ponto de vista do número de antenas em Eve e M. No entanto, ao descrever o caso do feedback perfeito, obtém-se uma significativa melhoria no desempenho de *outage* de sigilo através da diversidade espacial, e o ganho de diversidade é governado pelo número de antenas no Tx e Rx legítimo, e seu valor quantitativo é o produto de ambas as configurações de antena. Neste grupo de curvas, com $N_B = N_A = 2$, o ganho de diversidade é 4 ($G_{\mathrm{D}} = 4$).

Figura 19: Probabilidade de *outage* de sigilo versus SNR média em Bob assumindo esquema MRC em Bob com diferentes configurações de antenas em Bob e diferentes valores de ρ. Premissas: $\bar{\gamma}_E = 3\mathrm{dB}$; $R_0 = 1$; $N_{\mathrm{A}} = N_{\mathrm{E}} = 2$; sinais interferentes com distribuição de potências iguais com $\bar{\gamma}_i = 2\mathrm{dB}$ para $M = 2$.



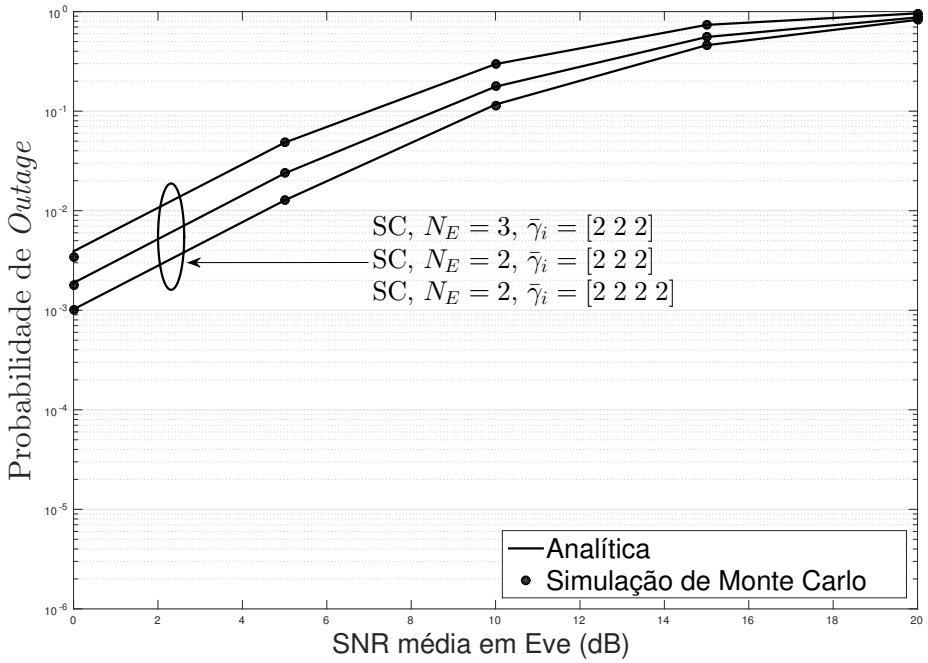
Fonte: Próprio autor.

A Figura 19 representa a probabilidade de *outage* de sigilo em relação à SNR média em Bob considerando uma distribuição de potências iguais nos sinais interferentes, em que diferentes configurações de antena em Bob e diferentes valores de ρ são assumidos, para ilustrar o impacto da diversidade de antenas e o coeficiente de correlação no desempenho de *outage* de sigilo do sistema. Nota-se que, um aumento no número de antenas em Bob, fornece uma ordem de diversidade adicional com atraso de feedback ou não. Por

exemplo, quando $\rho \neq 1$, comparando as curvas (a), (b), (d) e (e), é fácil observar que a ordem de diversidade é aumentada de 1 para 2 para $N_B = 1$ e $N_B = 2$, respectivamente. Assim, embora $N_A = 2$, o ganho de diversidade é limitado apenas por N_B para o caso de atraso no *feedback*. No entanto, quando $\rho = 1$, nas curvas (c) e (f), a ordem de diversidade é aumentada de 2 para 4 para $N_B = 1$ e $N_B = 2$, respectivamente, devido ao fato de que a ordem de diversidade completa poder ser alcançada e $G_{\mathrm{D}} = N_A N_B$.

A fim de reafirmar os resultados, as Figuras 20 e 21 mostram a probabilidade de *outage* de sigilo em relação à SNR média em Eve, assumindo um regime SC em Bob com distribuição de potências iguais nos sinais interferentes, e um esquema MRC no Rx legítimo com uma CSI perfeita e sinais de interferência com distribuição de potências diferentes. Nas Figuras 20 e 21, N_A e N_B, permanecem constantes, iguais a 2, e como esperado, observa-se uma melhora no desempenho de *outage* de sigilo quando: (a) o número de sinais de interferência aumenta; (b) a SNR média em Eve diminui; e/ou (c) o número de antenas em Eve diminui.

Figura 20: Probabilidade de *outage* de sigilo versus SNR média em Eve assumindo esquema SC em Bob. Premissas: $N_A = 2$; $N_B = 2$; $\bar{\gamma}_B = 10$dB; $R = 1$; sinais interferentes com distribuição de potências iguais.

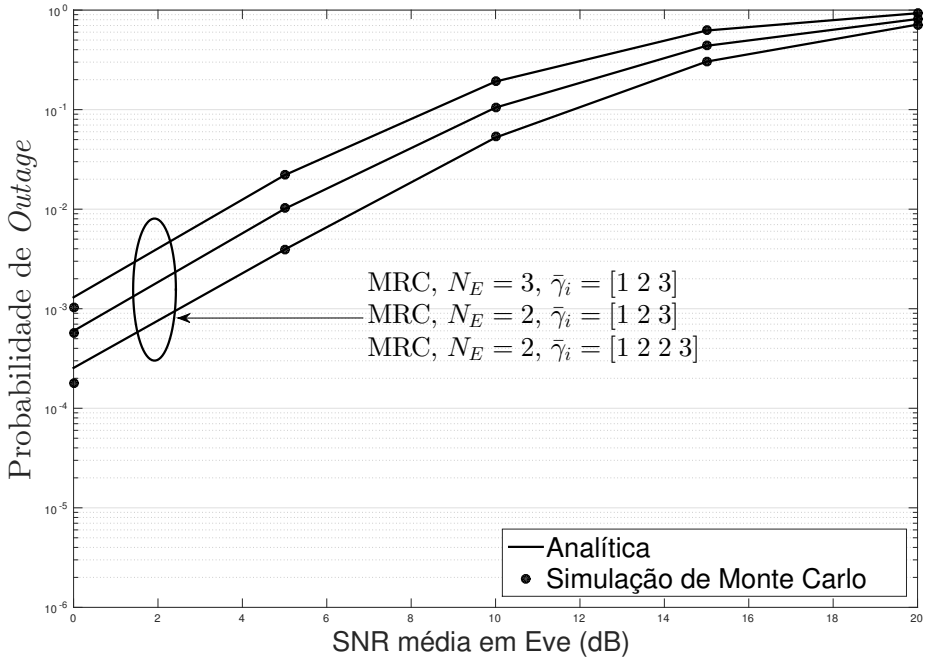


Fonte: Próprio autor.

Além disso, pode-se notar que a probabilidade de *outage* de sigilo converge para 1 quando a SNR média em Eve aumenta, mesmo com a SNR média em Bob fixa em 10 dB. Finalmente, a Figura. 21 para o regime MRC representa uma melhoria na probabilidade de *outage* em relação à Figura 20 para o esquema SC.

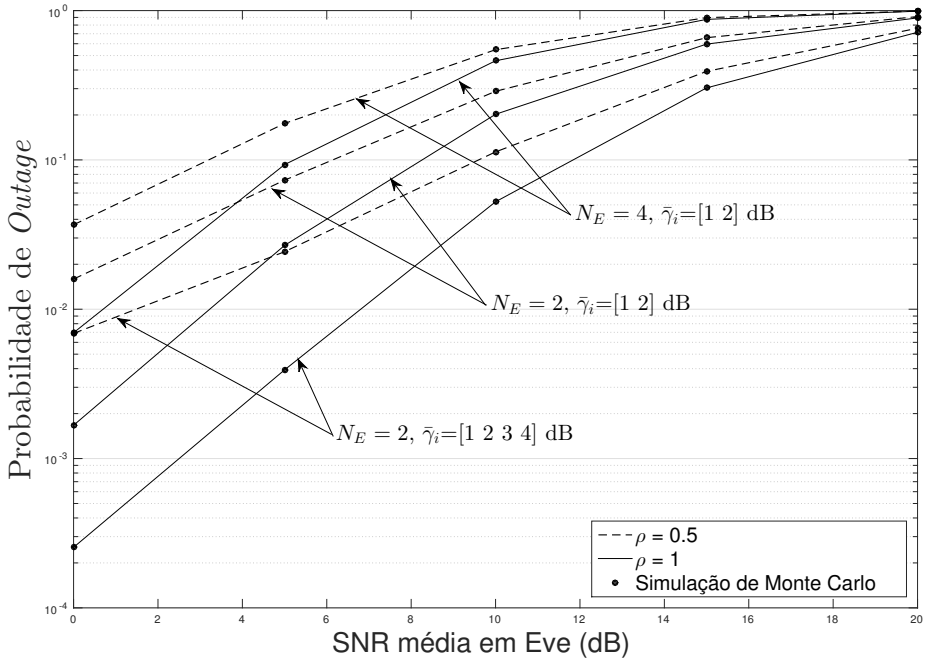
Uma análise similar é apresentada na Figura 22, mas destacando o efeito de

Figura 21: Probabilidade de *outage* de sigilo versus SNR média em Eve assumindo esquema MRC em Bob com CSI perfeita. Premissas: $N_A = 2$; $N_B = 2$; $\bar{\gamma}_B = 10$dB; $R = 1$; sinais interferentes com distribuição de potências distintas.



Fonte: Próprio autor.

Figura 22: Probabilidade de *outage* de sigilo versus SNR média em Eve assumindo esquema MRC em Bob com diferentes valores de ρ. Premissas: $\bar{\gamma}_E = 3$dB; $R = 1$; $N_\mathrm{A} = N_\mathrm{B} = 2$; $\bar{\gamma}_E = 3$dB; sinais interferentes com distribuição de potências distintas com $\bar{\gamma}_i = \{(1, 2), (1, 2, 3, 4)\}$dB para $M = 2, 4$.



Fonte: Próprio autor.

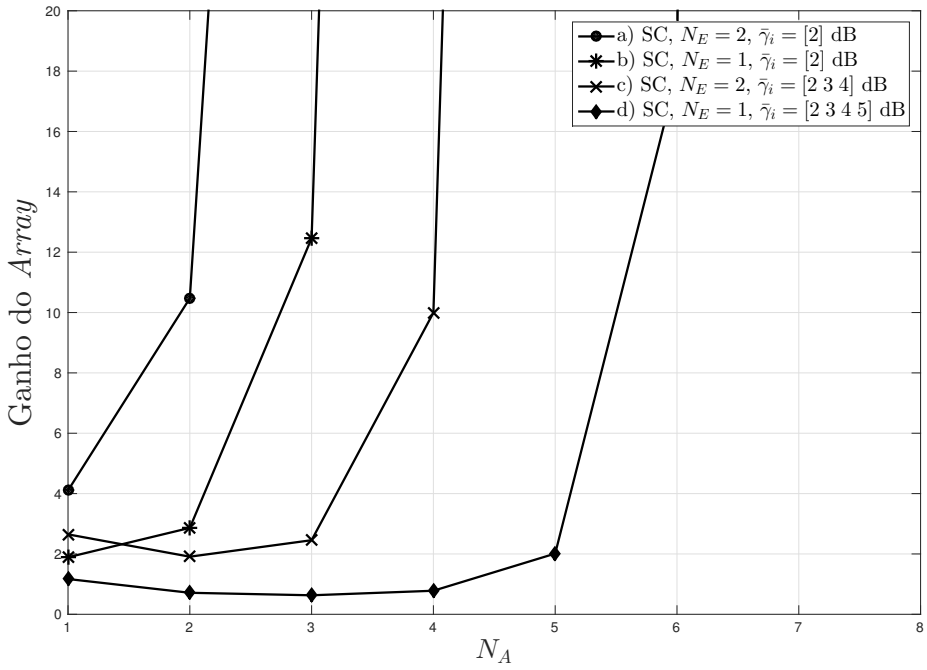
um *feedback* desatualizado. Comparando as curvas sólidas e tracejadas, podemos observar que o desempenho de *outage* de sigilo aumenta quando se considera um *feedback* perfeito ($\rho = 1$). No entanto, a probabilidade de *outage* de sigilo se aproxima para 1 quando a SNR média em Eve aumenta além da SNR média em Bob, e com a existência ou não de atraso no *feedback*. Por outro lado, Figura 22 mostra uma melhoria do desempenho de *outage* de sigilo quando a SNR média em Eve e/ou o número de antenas em Eve (N_E) diminuem. Além disso, observa-se que o aumento do número de sinais de interferência M tem um efeito direto na melhoria do desempenho de *outage* de sigilo.

Por outra parte, as Figuras 23 e 24 ilustram o ganho de *array* do sistema versus o número de antenas em Alice, assumindo os esquemas SC e MRC em Bob, e considerando o caso de sinais de interferência com distribuição de potências distintas. Em geral, ambas figuras mostram o mesmo comportamento. Basicamente, o ganho de *array* aumenta com o aumento de N_A. No entanto, ao aumentar o número de sinais de interferência M, a melhoria do ganho de *array* torna-se qualitativamente menos representativa, mesmo com o aumento de N_A. Por exemplo, este comportamento particular é observado claramente em ambas figuras nas curvas com $M = 4$, em que o ganho de *array* aumenta ligeiramente com o aumento de N_A. Além disso, ao comparar as curvas (a) e (b) de ambas figuras, mantendo o número de sinais de interferência M constante, perceba-se que, para configurações em que N_E é menor, o aumento do ganho de *array* é menos abrupto. Estas observasões permitem concluir que o número de antenas em Eve, bem como o número de sinais de interferência, afetam o ganho de *array* do sistema quando se aumenta o número de antenas em Alice N_A, mas as alterações são mais significativas para valores mais elevados de N_E e/ou valores mais baixos de M.

Para o esquema MRC na Figura 24, esse comportamento é mais evidente que para o regime SC na Figura 23. Por exemplo, note-se na curva (d), que o ganho de *array* permanece quase inalterado até $N_A = 6$, que é equivalente a $G_{\mathrm{D}} = 12$. Finalmente, perceba-se que, quando o número de antenas em Alice é igual a 1 (isto é, $N_A = 1$), o número de sinais de interferência afeta mais o ganho de *array* do que o número de antenas no nó intruso (mantendo o mesmo número de antenas em Bob). Em outras palavras, para um cenário em que $N_A = 1$, o número de sinais de interferência tem um papel crucial em termos de ganho de *array*. No entanto, de forma interessante, aumentando N_A de 1 para 2, o número de antenas no nó intruso torna-se mais influente sobre o ganho do *array* do que o número de sinais de interferência. Essa conclusão pode ser comprovada comparando as curvas (b) e (c) de ambas figuras. Até o momento, tais observações nunca foram relatadas na literatura ainda.

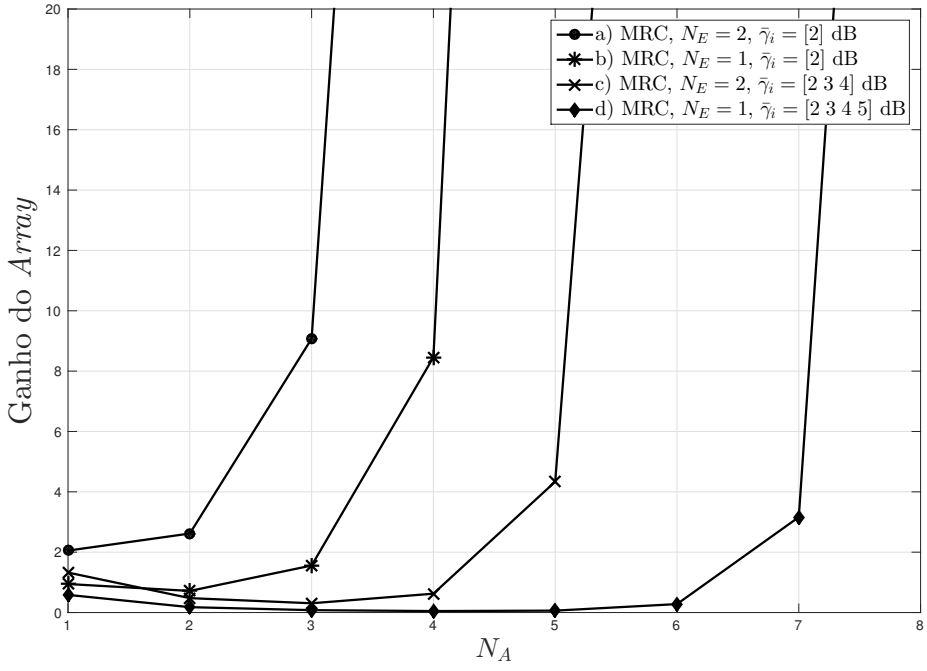
Para o caso especial MISO, uma análise similar à realizada nas Figuras 23 e 24 é realizada nas Figuras 25 e 26, representando os casos para os esquemas SC e MRC, respectivamente, e em que se mostra o comportamento do ganho de *array* do sistema proposto pelo número de antenas em Alice (N_A). Neste caso, mantendo constante o número

Figura 23: Ganho de *array* versus número de antenas em Alice (N_A) assumindo esquema SC em Bob. Premissas: $N_B = 2$; $\bar{\gamma}_E = -5$dB; sinais interferentes com distribuição de potências distintas.



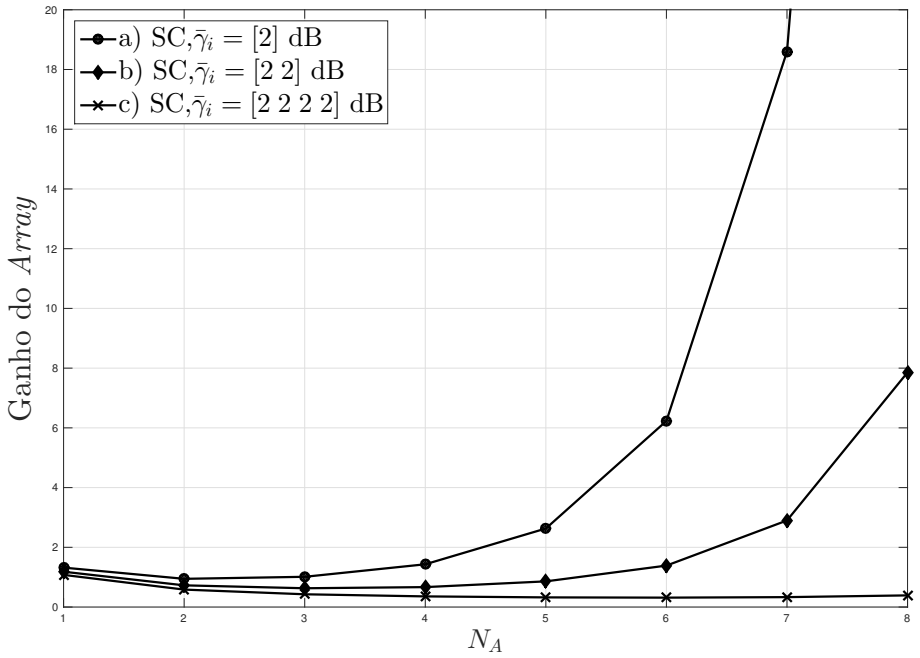
Fonte: Próprio autor.

Figura 24: Ganho de *array* versus número de antenas em Alice (N_A) assumindo esquema MRC em Bob. Premissas: $N_B = 2$; $\bar{\gamma}_E = -5$dB; sinais interferentes com distribuição de potências distintas.



Fonte: Próprio autor.

Figura 25: Ganho de *array* versus número de antenas em Alice (N_A) assumindo esquema SC em Bob e um canal MISO. Premissas: $N_B = 2$; $\bar{\gamma}_E = -5$dB; sinais interferentes com distribuição de potências distintas.



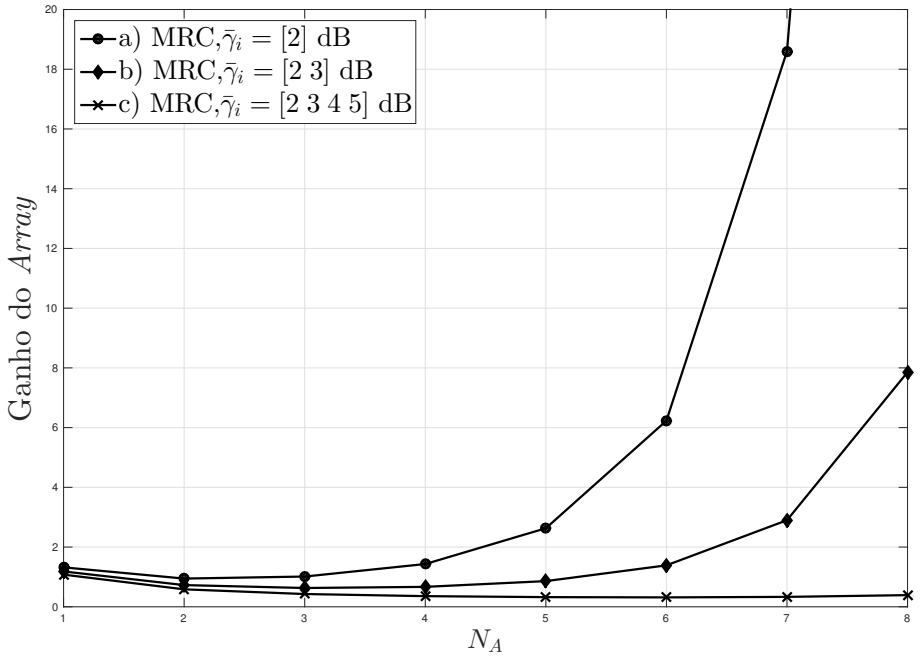
Fonte: Próprio autor.

de antenas no nó malicioso em $N_E = 1$, nota-se o efeito do número de sinais de interferência sobre o ganho de *array*. Similar ao observado para o caso MIMO, um aumento do número de antenas em Alice, implica em um aumento no ganho de *array*. No entanto, ao mesmo tempo, aumentando o número de sinais de interferência, a melhoria desta métrica torna-se menos representativa, mesmo com o aumento de N_A. Este comportamento é perceptível nas curvas (c) das Figuras 25 e 26, em que com $M = 4$, o ganho de *array* não sofre qualquer melhoria.

Observa-se também que, o aumento do ganho de *array* nas Figuras 25 e 26 é menos abrupto que nas Figuras 23 e 24, devido à influência limitada do número de antenas em Bob e Eve ($N_B = N_E = 1$), sendo essencialmente governado pelo número de sinais interferentes.

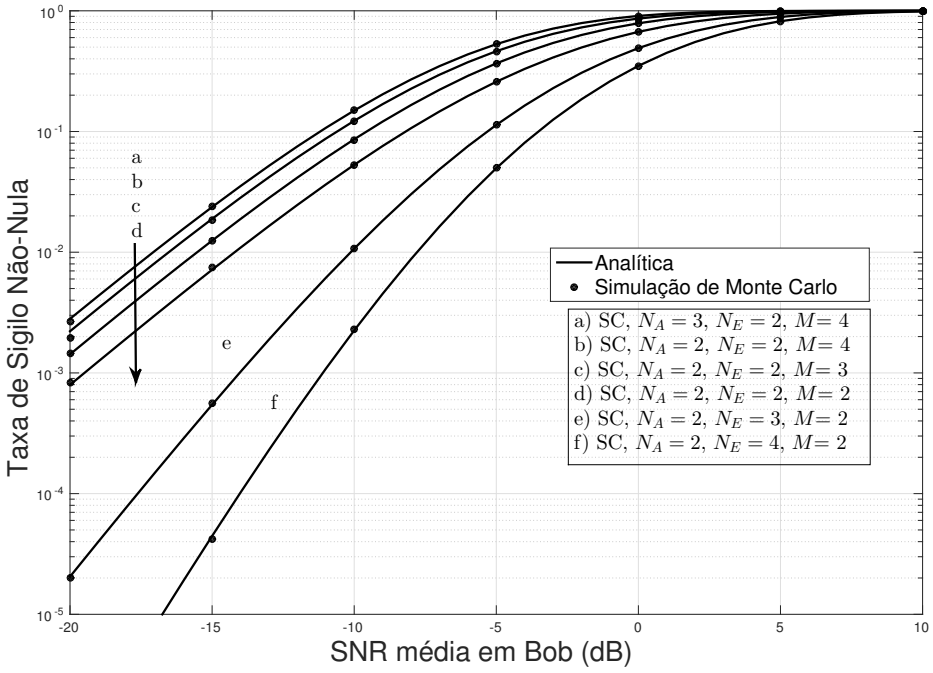
Figuras 27 e 28 mostram a probabilidade da taxa de sigilo não-nula em relação à SNR média em Bob, assumindo os esquemas SC e MRC em Bob com CSI perfeita, respectivamente. Além disso, um padrão de distribuição de potências iguais nos sinais de interferência é assumido para o esquema SC, enquanto um padrão de sinais com uma distribuição de potências diferentes é considerado para o caso MRC. Em geral, o mesmo comportamento é observado em ambas figuras. Em particular, observa-se que, mantendo constante N_E, quando o número de antenas em Alice N_A, ou o número de sinais de interferência M diminuem, a taxa de sigilo diferente de zero igualmente diminui. Por

Figura 26: Ganho de *array* versus número de antenas em Alice (N_A) assumindo esquema MRC em Bob e um canal MISO. Premissas: $\bar{\gamma}_E = -5$dB; sinais interferentes com distribuição de potências distintas.



Fonte: Próprio autor.

Figura 27: Taxa de sigilo não-nula versus SNR média em Bob, assumindo esquema SC em Bob. Premissas: $N_B = 3$; $\bar{\gamma}_E = 5$dB; sinais interferentes com distribuição de potências iguais com $\bar{\gamma}_i = 2$dB para $M = 2, 3, 4$.

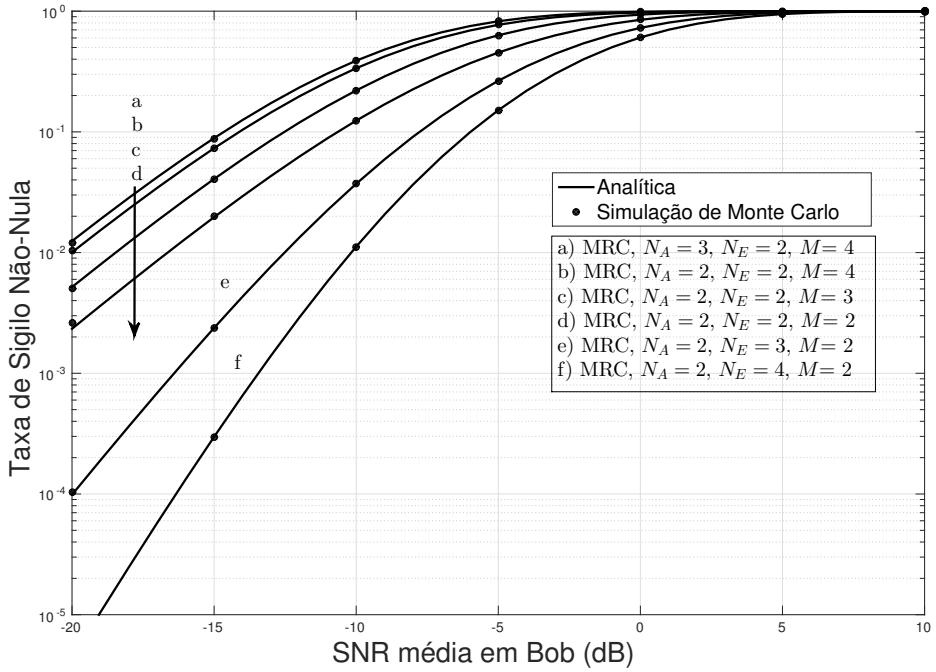


Fonte: Próprio autor.

outra parte, as curvas (d), (e) e (f) nas Figuras 27 e 28 mostram o efeito do número de antenas no nó malicioso (N_E) sobre a taxa de sigilo diferente de zero, observando-se uma diminuição importante nesta métrica com um aumento de N_E.

Conclusões iguais às comentadas anteriormente para as Figuras 27 e 28 podem ser observadas nas Figuras 29 e 30, em que a taxa de sigilo não-nula é analisada assumindo um canal MISO como caso especial. A Figura 29 representa a adoção de um regime SC com distribuição de potências iguais nos sinais interferentes, enquanto a Figura 30, adota um esquema MRC e sinais de interferência com distribuição de potências diferentes. Mantendo constante $N_E = 1$, a taxa de sigilo não-nula diminui com uma disminuição do número de antenas em Alice N_A, bem como pelo número de sinais interferentes atingindo Eve. No entanto, a diminuição da taxa de sigilo não-nula é mais significativa nas Figuras 27 e 28, com o aumento do número de antenas no nó malicioso para o caso MIMO.

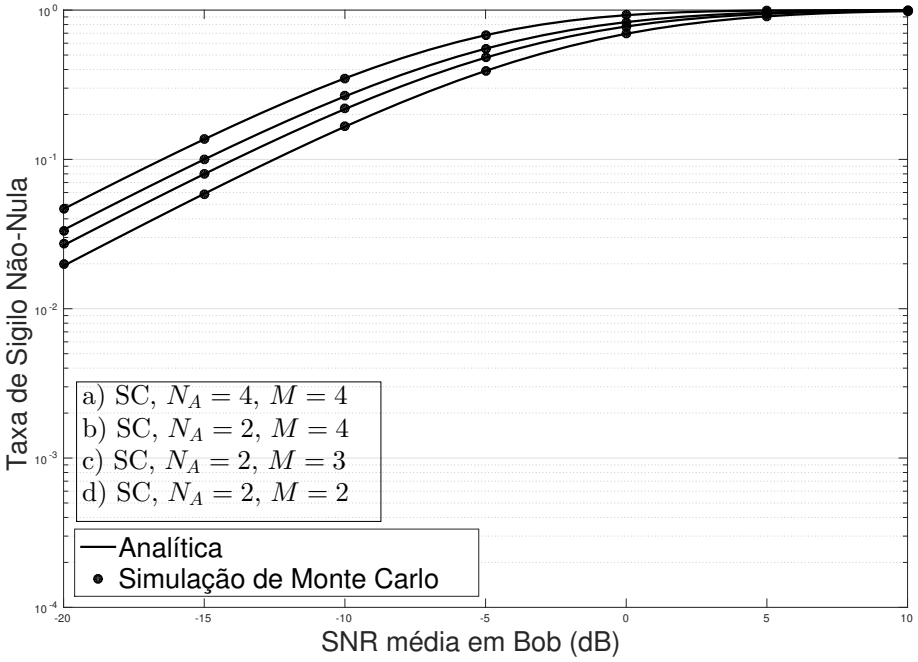
Figura 28: Taxa de sigilo não-nula versus SNR média em Bob, assumindo esquema MRC em Bob. Premissas: $N_B = 3$; $\bar{\gamma}_E = 5$dB; sinais interferentes com distribuição de potências distintas com $\bar{\gamma}_i = \{(2,3),(2,3,4),(2,3,4,5)\}$dB para $M = 2,3,4$ respectivamente.



Fonte: Próprio autor.

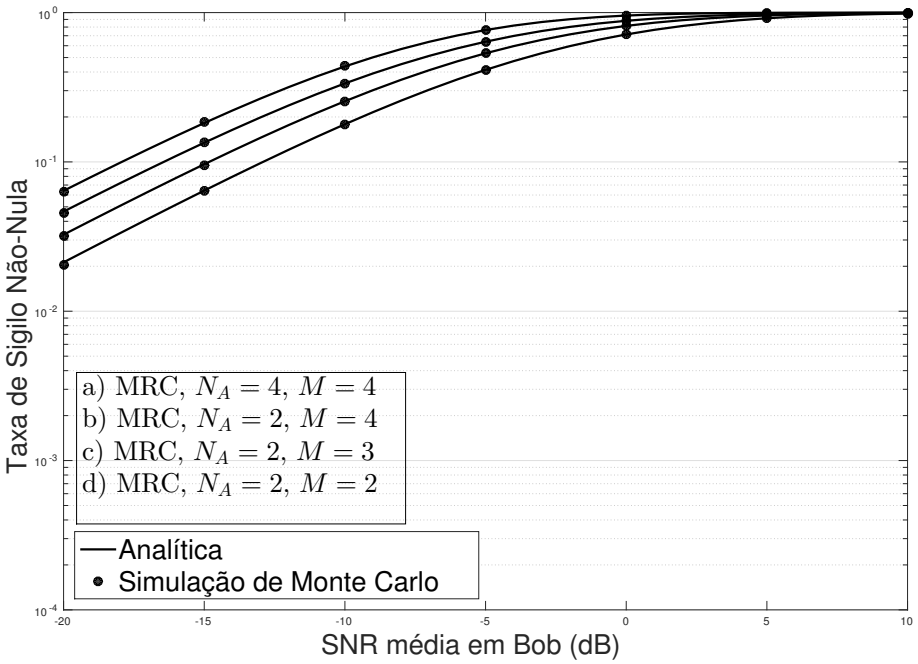
O impacto de um atraso no *feedback* é representado na Figura 31. A Figura 31 mostra a probabilidade da taxa de sigilo não-nula em relação à SNR média em Bob, assumindo o esquema MRC em Bob para diferentes valores de ρ e um padrão de distribuição de potências diferentes nos sinais de interferência. Pode-se observar que, com o um retardo ou não no *feedback*, quando o número de antenas no nó malicioso (N_E) é fixo, a taxa de sigilo não-nula diminui quando uma das seguintes condições ocorre: 1) o número de

Figura 29: Taxa de sigilo não-nula versus SNR média em Bob, assumindo esquema SC em Bob e um canal MISO. Premissas: $\bar{\gamma}_E = 5$dB; sinais interferentes com distribuição de potências iguais com $\bar{\gamma}_i = 2$dB para $M = 2, 3, 4$.



Fonte: Próprio autor.

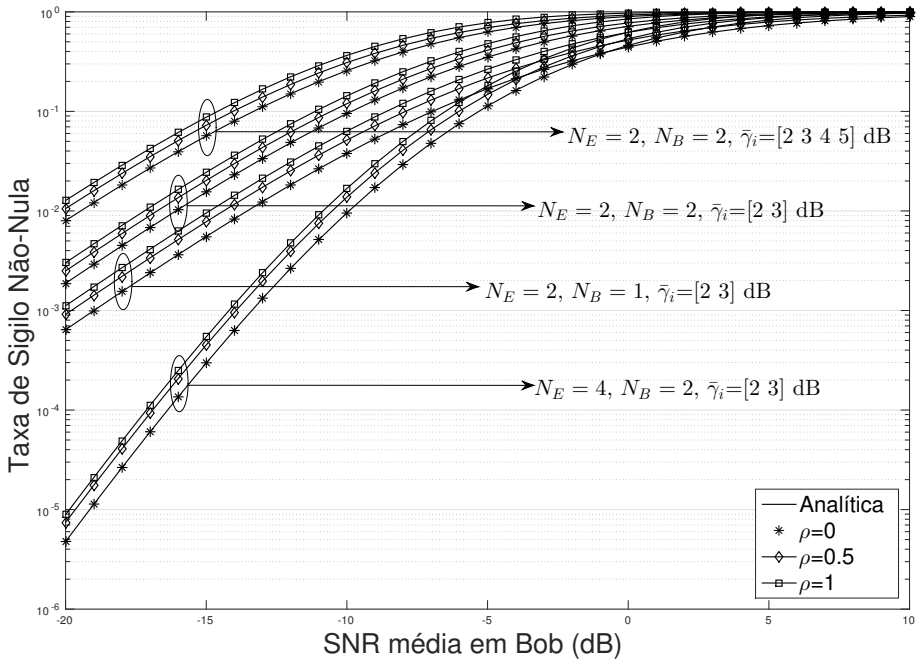
Figura 30: Taxa de sigilo não-nula versus SNR média em Bob, assumindo esquema MRC em Bob e um canal MISO. Premissas: $\bar{\gamma}_E = 5$dB; sinais interferentes com distribuição de potências distintas com $\bar{\gamma}_i = \{(2, 3), (2, 3, 4), (2, 3, 4, 5)\}$dB para $M = 2, 3, 4$ respectivamente.



Fonte: Próprio autor.

sinais de interferências diminui; 2) o número de antenas em Bob (N_B) diminui. Por outro lado, nota-se que a última curva fornece uma diminuição significativa da taxa de sigilo não-nula com o aumento do número de antenas em Eve. Em termos do coeficiente de correlação, observa-se que para valores menores de ρ, menor é a probabilidade da taxa de sigilo não-nula, e esta métrica existiria mesmo quando o *feedback* estiver completamente desatualizado, ou seja, $\rho = 0$. Além disso, observa-se que, com uma CSI perfeita ou imperfeita, a taxa de sigilo não-nula converge para 1 no regime de alta SNR. Finalmente, todas as curvas são verificadas por simulações de Monte Carlo.

Figura 31: Taxa de sigilo não-nula versus SNR média em Bob, assumindo esquema MRC para diferentes valores de ρ. Premissas: $\bar{\gamma}_E = 3$dB; $R = 1$; $N_{\mathrm{A}} = 2$; sinais interferentes com distribuição de potências distintas com $\bar{\gamma}_i = \{(2,3),(2,3,4,5)\}$dB para $M = 2, 4$.



Fonte: Próprio autor.

4.4 Conclusões

Resumindo, ao longo deste capítulo foram apresentados uma variedade de resultados numéricos com o objetivo de esclarecer a influência dos parâmetros sistêmicos sobre o desempenho de *outage* de sigilo de um canal MIMO *wiretap*, bem como, do caso especial MISO. Entre os parâmetros avaliados, achavam-se, o número de antenas nos nós que compõem o sistema, o número de sinais de interferência e o padrão de distribuição de potências de interferência. Pelas curvas traçadas, observou-se uma melhoria no desempenho de *outage* de sigilo ao aumentar o número de sinais interferentes M e/ou diminuir o número de antenas no nó malicioso (N_E). Foi igualmente percebida uma superioridade

no desempenho de *outage* de sigilo quando assumiu-se um regime MRC, em vez de um esquema SC, ao manter similares configurações nos parâmetros. Em relação ao ganho de diversidade, foi possível demonstrar que, quando o nó intruso é afetado por sinais de interferência e ruído, o ganho de diversidade é igual ao produto do número de antenas em Alice e Bob, isto é, $G_{\mathrm{D}} = N_A N_B$ quando é assumida uma CSI perfeita, enquanto, para o caso especial MISO, é reduzido para $G_{\mathrm{D}} = N_A$. Porém, foi demonstrado que ao assumir um *feedback* desatualizado, o parâmetro ρ tem um impacto importante sobre o desempenho de *outage* de sigilo, e uma perda no desempenho de *outage* de sigilo é visível à medida que os valores de ρ diminuem, ou seja, os atrasos de feedback aumentam. Em outras palavras, em condições práticas com uma CSI imperfeita, o ganho de diversidade máximo não pode ser alcançado, e é reduzido para $G_{\mathrm{D}} = N_B$. Estes resultados mostraram que o ganho de diversidade é governado apenas pelo número de antenas no Tx e no Rx legítimo para o caso de $\rho = 1$, e é limitado apenas pelo número de antenas no Rx legítimo para o caso de $\rho \neq 1$, e não sofrerá qualquer alteração, embora variando o número de sinais de interferência M. Por outro lado, o ganho de *array* do sistema, como esperado, aumentou com o aumento do número de antenas em Alice (N_A), no entanto, ao aumentar o número de sinais de interferência M, esta melhoria tornou-se menos representativa, mesmo aumentando N_A. O oposto aconteceu com o aumento do número de antenas no nó malicioso. Um aumento de N_E implicou diretamente um aumento abrupto do ganho de *array* do sistema, sendo este comportamento mais evidente no esquema MRC. Pode-se resumir então, ao aumentar N_A, aumenta o ganho de *array*, mas este aumento é bem mais significativo para configurações elevadas de N_E e/ou valores menores de M. Finalmente, foi igualmente importante notar que para $N_A = 1$, o ganho de *array* é principalmente governado pelo número de sinais de interferência M, no entanto, ao aumentar o número de antenas em Alice, o número de antenas no nó intruso passou desempenhar um papel crucial em termos de ganho de *array*. Todas as curvas foram verificadas através de simulações de Monte Carlo, evidenciando-se uma excelente concordância entre as curvas analíticas e as simuladas.

5 CONCLUSÕES E TRABALHOS FUTUROS

Nesta dissertação foi investigada a segurança da camada física de canais *wiretap* MIMO em termos da probabilidade de *outage* de sigilo. O cenário considerado consistiu em um nó malicioso tentando interceptar a troca de informações entre o Tx e o Rx legítimo. Além disso, considerou-se a presença de ruído e de múltiplos sinais de interferência. Em paralelo, foi analisado o cenário MISO como caso especial, em que apenas o transmissor é equipado com múltiplas antenas.

Especificamente, no Capítulo 1, foi introduzida uma visão geral da estratégia de segurança na camada física e sua eficácia em garantir um nível aceitável de sigilo

em redes sem fio. Uma revisão da literatura foi realizada, verificando-se a variedade de modelos sistêmicos e métodos aplicáveis com esta estratégia, sendo o método do envio de sinais de interferência para o nó intruso, um dos mais efetivos em aumentar a taxa de sigilo. A ausência de pesquisas que analisaram o desempenho de *outage* de sigilo, considerando a influência de sinais interferentes e ruído sobre o nó malicioso foi a principal motivação no desenvolvimento desta dissertação.

Uma breve caracterização dos sistemas MIMO foi conduzida no Capítulo 2, constituindo a base teórica deste trabalho. Foram apresentados alguns conceitos importantes utilizados ao longo da pesquisa, tais como o ganho de *array* e o ganho de diversidade espacial, aprofundando na diversidade espacial em transmissão e recepção, respectivamente, como métodos para reduzir os desvanecimentos e melhorar a confiabilidade do canal. Além disso, foram introduzidos conceitos importantes em relação à estratégia de segurança da camada física.

No Capítulo 3, foi apresentado o modelo sistêmico proposto, em que o Tx empregou um esquema TAS; o Rx legítimo utilizou SC e MRC como técnicas de combinação de sinal; e o nó intruso adotou apenas o regime MRC. Uma revisão estatística foi realizada, com base na qual foram derivadas as expressões analíticas exatas que descrevem a probabilidade de *outage* de sigilo e a taxa de sigilo não-nula do sistema. Além disso, uma análise assintótica foi desenvolvida, através da qual se determinou a ordem de diversidade do sistema, e foram obtidos o ganho de diversidade e o ganho de *array*. Foi notado que, assumindo sinais interferentes e ruído no nó intruso, o ganho de diversidade é limitado pelo número de antenas no Tx e Rx legítimo para o caso em que foi assumida uma CSI perfeita, enquanto é reduzido apenas ao número de antenas no Rx legítimo quando é considerado um atraso no *feedback*. Em ambos os casos, a ordem de diversidade é independentemente do número de sinais de interferência que afetam o nó malicioso.

No Capítulo 4, foram apresentados os resultados numéricos mais representativos que ajudaram a esclarecer a influência de cada parâmetro chave sobre o desempenho de *outage* de sigilo. As curvas traçadas representaram diferentes configurações de antenas nos nós do sistema, diferentes quantidades de sinais de interferência e os dois padrões de distribuição de potências de interferência propostos: distribuição de potências iguais e diferentes. Mantendo configurações similares nos parâmetros, as curvas mostraram uma superioridade no desempenho de *outage* de sigilo quando foi assumido um esquema MRC, em detrimento do regime SC. Em geral, foi observado uma melhoria no desempenho de *outage* quando se incrementou o número de sinais de interferência e/ou diminuiu o número de antenas no nó intruso. Em relação ao ganho de diversidade, foi comprovada numericamente a conclusão derivada da análise assintótica antes desenvolvida, isto é, com o nó malicioso afetado por sinais de interferência e ruído, o ganho de diversidade é igual ao produto do número de antenas em Alice e em Bob ($G_{\mathrm{D}} = N_A N_B$) para o caso com CSI perfeita. Este resultado foi reduzido para o caso especial MISO, em que $G_{\mathrm{D}} = N_A$. No

entanto, no caso em que foi assumida uma CSI imperfeita, $G_{\mathrm{D}} = N_B$, e o ganho de diversidade esperado não pode ser alcançado. Analisando o ganho de *array*, comprovou-se um aumento desta métrica com o aumento do número de antenas em Alice N_A, no entanto, um aumento da quantidade de sinais de interferência M, implicou que essa melhoria não fosse tão representativa, mesmo aumentando N_A. Por outra parte, um aumento no número de antenas no nó intruso N_E, provocou um aumento vertiginoso do ganho de *array* do sistema, especialmente no regime MRC. Neste sentido, foi notado que para configurações com menor número de antenas em Alice N_A, o número de sinais de interferência M é o parâmetro que tem maior influência sobre o ganho de *array*, no entanto, ao aumentar o número de antenas em Alice, o ganho de *array* é fortemente governado pelo número de antenas no nó malicioso N_E. Para uma validação adicional dos resultados alcançados, todas as curvas traçadas neste capítulo foram verificadas por meio de simulações de Monte Carlo, em que evidenciou-se uma excelente concordância entre as curvas analíticas e as simuladas.

Visando a obter uma maior quantidade de dados para uma melhor avaliação do desempenho de *outage* de sigilo em canais *wiretap*, este trabalho poderia ser estendido de diversas formas. Por exemplo, mantendo um modelo sistêmico similar ao proposto, e com a mudança de algumas das estratégias e modelos assumidos. Investigações futuras poderiam estudar o desempenho de *outage* de sigilo por outras perspectivas, que poderiam ser:

- Utilizar outros esquemas de combinação de sinal no receptor legítimo, como por exemplo, combinação por ganho igual (EGC, do inglês, *Equal Gain Combining*) ou GSC. Isto permitiria uma comparação com os esquemas estudados nesta dissertação.
- Adotar outros esquemas de transmissão, como códigos espaço-temporais ortogonais (ST, do inglês, *Space-Time codes*) ou *beamforming*.
- Em relação ao canal de desvanecimento, empregar o modelo de desvanecimento Nakagami-m, que resultaria em um modelo mais geral que o *Rayleigh*.
- Analisar o caso com uma CSI imperfeita no canal entre o receptor legítimo e o nó amigo.
- Assumir outros esquemas de combinação de sinal no nó intruso.
- Adotar múltiplos nós maliciosos com cooperação tentando interceptar a troca de informações entre os nós legítimos.

REFERÊNCIAS

[1] SILVA, E.; DOS SANTOS, A.; ALBINI, L. C. P.; LIMA, M. N. ,Identity- based key management in mobile ad hoc networks: Techniques and applications. **IEEE Trans. Wireless Commun.**, v. 15, n. 5, p. 46-52, Out. 2008.

[2] SHANNON, C., Communication theory of secrecy systems. **Bell System Technical Journal**, v. 28, p. 656-715, Out. 1949.

[3] WYNER, A., The wire-tap channel. **Bell System Technical Journal**, v. 54, n. 8, p. 1355-1387, Out. 1975.

[4] LEUNG-YAN-CHEONG, S. K.; HELLMAN, M. E., The Gaussian wiretap channel. **IEEE Trans. Inf. Theory**, v. 24, p. 451-456, Jul. 1978.

[5] LIANG, Y.; POOR, H. V.; SHAMAI, S., Secure communication over fading channels. **IEEE Trans. Inf. Theory**, v. 54, n. 6, p. 2470-2492, Jun. 2008.

[6] LIANG, Y.; POOR, H. V.; SHAMAI, S., Physical layer security in broadcast networks. **Security and Communication Networks**, v. 2, p. 227-238, 2009.

[7] LIU, R.; LIU, T.; POOR, H. V.; SHAMAI, S., MIMO Gaussian broadcast channels with confidential messages. *In*: IEEE INT. SYMP. INF.THEORY: ISIT, 2009, Seoul, Anais...Seoul, 2009.

[8] LIU, T.; SHAMAI, S., A note on the secrecy capacity of the multiple-antenna wiretap channel. **IEEE Trans. Inf. Theory**, v. 55, n. 6, p. 2547-2553, Jun. 2009.

[9] OGGIER, F.; HASSIBI, B., The secrecy capacity of the MIMO wiretap channel. **IEEE Trans. Inf. Theory**, v. 57, n. 8, p. 4961-4972, Ago. 2011.

[10] HE, F.; MAN, H.; WANG W., Maximal ratio diversity combining enhanced security. **IEEE Commun. Lett.**, v. 15, n. 5, p. 509-511, Maio 2011.

[11] ALVES, H.; SOUZA, R. D.; DEBBAH, M.; BENNIS, M., Performance of transmit antenna selection physical layer security schemes. **IEEE Signal Process. Lett.**, v. 19, n. 6, p. 372-375, Jun. 2012.

[12] YANG, N.; et al., Transmit antenna selection for security enhancement in MIMO wiretap channels. **IEEE Trans. Commun.**, v. 61, n. 1, p. 144-154, Jan. 2013.

[13] SADEQUE, N.; LAND, I.; SUBRAMANIAN, R., Asymptotic analysis of average secrecy capacity under transmit antenna selection for the MIMO wiretap channel. *In*: IEEE 80. VEH. TECHNOL. CONF.: VTC, 2014, Vancouver, Anais...Vancouver, 2014.

[14] YANG, N.; et al., MIMO wiretap channels: Secure transmission using transmit antenna selection and receive generalized selection combining. **IEEE Commun. Lett.**, v. 17, n. 9, p. 1754-1757, Set. 2013.

[15] YAN, N.; et al., Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels. **IEEE Trans. Wireless Commun.**, v. 13, n. 3, p. 1656-1667, Mar. 2014.

[16] YANG, N.; et al., Artificial noise: Transmission optimization in multi-input single-output wiretap channels. **IEEE Trans. Commun.**, v. 63, n. 5, p. 1771-1783, Mai 2015.

[17] DA COSTA, D. B.; et al., Secrecy outage performance of MIMO wiretap channels with multiple jamming signals. **Journal Commun. Inf. Syst.**, v. 31, n. 1, p. 30-40, 2016.

[18] HUANG J.; SWINDLEHURST, A. L., Cooperative jamming for secure communications in MIMO relay networks. **IEEE Trans. Signal Proces.**, v. 59 p. 4871-4884, 2011.

[19] TEKIN E.; YENER, A., The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming. **Trans. Inform. Theory**, v. 54, p. 2735-2751, Jun. 2008.

[20] HAN, Z.; et al., Physical layer security game: interaction between source, eavesdropper, and friendly jammer. **Journal Wireless Commun. and Net.**, v. 2009, p. 1-10, Mar. 2009.

[21] KHISTI A.; WORNELL, G., Secure transmission with multiple antennas - Part II: The MIMOME wire-tap channel. **IEEE Trans. Inf. Theory**, v. 56, n. 11, p. 5515-5532, Nov. 2010.

[22] KHISTI A.; ZHANG, A. D., Artificial-noise alignment for secure multicast using multiple antennas. **IEEE Commun. Lett.**, v. 17, n. 8, p. 1568-1571, Ago. 2013.

[23] LI, W.; TANG, Y.; WEI, J., Secure communications via sending artificial noise by both transmitter and receiver: Optimum power allocation to minimise the insecure region. **IET Commun.**, v. 8, n. 16, p. 2858-2862, Nov. 2014.

[24] ORTEGA, Y. R.; et al., MISO TAS wiretap channels with jamming and noise at the eavesdropper. *In*: IEEE INT. CONF. TELECOMMUN.: ICT, 2016, Thessaloniki, Anais...Thessaloniki, 2016.

[25] CHU, Z.; et al., Robust outage secrecy rate optimizations for a MIMO secrecy channel. **IEEE Wireless Commun. Lett.**, v. 4, n. 1, p. 86-89, Fev. 2015.

[26] HE, B.; ZHOU, X.; ABHAYAPALA, T. D., Achieving secrecy without knowing the number of eavesdropper antennas. **IEEE Trans. Wireless Commun.**, v. 14, n. 12, p. 7030-7043, Dez. 2015.

[27] FERDINAND, N. S.; DA COSTA, D. B.; LATVA-AHO, M., Effects of outdated CSI on the secrecy performance of MISO wiretap channels with transmit antenna selection. **IEEE Commun. Lett.**, v. 17, n. 5, p. 864-867, Maio 2013.

[28] FERDINAND, N. S.; et al., Secrecy outage performance of MISO wiretap channels with outdated CSI. *In*: IEEE INT. CONF. COMMUN.: ICC, 2014, Sydney, Anais...Sydney, 2014.

[29] AMARASURIYA, G.; TELLAMBURA, C.; ARDAKANI, M., Feedback delay effect on dual-hop MIMO AF relaying with antenna selection. **IEEE Global Commun. Conf.**, p. 1-10 Dez. 2010.

[30] WANG, L.; et al., Outage Analysis of Transmit Beamforming and Relay Selection with Outdated Channel Estimates over Nakagami-Fading Channels. **International Journal of Distributed Sensor Networks**, v. 2015, p. 1-6, Jul. 2015.

[31] XIONG J., et al., Secrecy performance analysis for TAS-MRC system with imperfect feedback. I**EEE Trans. Info. Forenc. Secur.**, v. 10, n. 8, p. 1617-1629, Ago. 2015.

[32] HUANG, Y.; AL-QAHTANI, F. S.; DUONG, T. Q., Secure Transmission in MIMO Wiretap Channels Using General-Order Transmit Antenna Selection With Outdated CSI. **IEEE Transactions on Communications**, v. 63, n. 8, Ago. 2015.

[33] FOSCHINI, G. J.; GANS, M. J., On Limits of Wireless Communications in a Fading Environment when Using Multiple Antennas. **Wireless Personal Communications**, v. 6, p. 311-335, Mar. 1998.

[34] RAILEGH, G. G.; CIOFFI, J. M., Spatio-Temporal Coding for Wireless Communications. **IEEE Transactions on Communications**, v. 46, p. 357-366, Mar. 1998.

[35] FOSCHINI, G. J., Layered space-time architecture for wireless communication in fading environments when using multi-element antennas. **Bell Labs Technology Journal**, p. 41-59, 1996.

[36] TELATAR, I. E., Capacity of multi-antenna Gaussian channels. **Europ. Trans. Telecommun.**, v. 10, p. 585-596, Nov.-Dez. 1999.

[37] WEICHSELBERGER, W., **Spatial Structure of Multiple Antenna Radio Channels. A signal Processing Viewpoint.** 2003. Dissertacão (Doutorado) - Universidade Técnica de Viena, Disponível em: $< http : //www.nt.tuwien.ac.at/mobile/theses_finished >$. Dez. 2003.

[38] ZHENG L.; TSE, D. N. C., Diversity and Multiplexing: A Fundamental Tradeoff in Multiple-Antenna Channels. **IEEE Transactions on Information Theory**, v. 49, n. 5, p. 1073-1096, Maio 2003.

[39] ANDERSEN, J. B. , Antenna Arrays in Mobile Communications: Gain, Diversity, and Channel Capacity. **IEEE Antennas and Propagation Magazine**, v. 42, n. 2, p. 12-16, Abr. 2000.

[40] PROAKIS, J. G.; SALEHI, M., **Digital Communication.**, 5. ed. McGraw-Hill, 2008.

[41] JAKES, W. C., **Microwave Mobile Communications.**, Wiley, New York, 1974, IEEE reissue 1994.

[42] VUCETIC, B.; YUAN, J., **Space-Time Coding**. John Wiley and Sons Inc., 2003.

[43] PARSONS J.D., et al., Diversity Techniques for Mobile Radio Reception. **IEEE Transactions on Vehicular Technology**, v. 25, n. 3, p. 75-84, Ago. 1976.

[44] BRENNAN, D. G. , Linear Diversiy Combining Techniques. **Proceedings of the IRE**, v. 47, n. 1, p. 1075-1102, Jul. 1959.

[45] RAPPAPORT T.S., **Wireless Communications: Principles and Practice.**, New Jersey: Prentice-Hall Inc, 1996.

[46] WIN M. Z.; WINTERS, J. H. , Virtual branch analysis of symbol error probability for hybrid selection/maximal-ratio combing in Rayleigh fading. **IEEE Trans. Commun.**, v. 49, p. 1926-1934, Nov. 2001.

[47] ALOUINI, M. S.; SIMON, M. K. , An MGF-based performance analysis of generalized selection combining over Rayleigh fading channels. I**EEE Trans. Commun.**, v. 48, p. 401-415, Mar. 2000.

[48] WITTNEBEN, A., A New Bandwidth Efficient Transmit Antenna Modulation Diversity Scheme for Linear Digital Modulation. *In*: IEEE INT. CONF. COMMUN.: ICC, 1993, Ginebra, Anais...Ginebra, 1993.

[49] PAULRAJ, A.; NABAR, R.; GORE, D., Introduction to Space-Time Wireless Communications. **Cambridge University Press**, 2003.

[50] GERSHMAN, A. B.; SIDIROPOULOS, N. D. "**Space-Time Processing for MIMO Communications.**", John Wiley and Sons, 2005.

[51] SANAYEI, S.; NOSRATINIA, A., Antenna Selection in MIMO Systems. **IEEE Communications Magazine**, Out. 2004.

[52] GHARAVI-ALKHANSARI, M.; GERSHMAN, A. B., Fast antenna subset selection in MIMO wireless systems. **IEEE Trans. Signal Proc.**, v. 52, n. 2, p. 339-347, Feb. 2004.

[53] PREMANANDA, S. P.; MCLOUGHLIN I, Performance Analysis of Adaptive Modulation and Transmit Antenna Selection with Channel Prediction Errors and Feedback Delay. **IET Communications**, v. 7. n. 16, p. 1852-1862, Nov. 2013.

[54] PAULRAJ, A. J.; et al., "**An Overview of MIMO Communications- A Key to Gigabit Wireless.**", Proceedings of the IEEE, v. 92, v. 2, p. 198-218, Feb. 2004.

[55] ALAMOUTI, S., A simple transmit diversity technique for wireless communications. **IEEE Journal on Selected Areas on Communications**, v. 16, , p. 1451-1458, Out. 1998

[56] TAROKH, V.; JAFARKHANI, H.; CALDERBANK, A., Space-Time block coding for wireless communications: Performance results. **IEEE Journal on Selected Areas on Communications**, v. 17, n. 3, p. 451-460, Mar. 1999.

[57] TAROKH, V.; JAFARKHANI, H.; CALDERBANK, A., Space-Time codes for high data rate wireless communications: Performance criterion and code construction. **IEEE Transactions on Information Theory**, v. 44, p. 744-765, Mar. 1998.

[58] FRIEDLANDER, B.; SCHERZER, S., Beamforming versus transmit diversity in the downlink of a cellular communication. **IEEE Transactions on Vehicular Technology**, v. 53, n. 53, p.1023-1034, 2004.

[59] BARROS, J.; RODRIGUES, M. R. D., Secrecy capacity of wireless channels. IEEE INT. SYMP. INF. THEORY: ISIT, 2006, Seattle, Anais...Seattle, 2006.

[60] DING, X.; et al., "**Security-Reliability Tradeoff for Friendly Jammer Assisted User-Pair Selection in the Face of Multiple Eavesdroppers.**", IEEE Access , v. PP, n.99, p.1-1, Jun. 2016.

[61] HADZI-VELKOV, Z., Level crossing rate and average fade duration of EGC systems with cochannel interference in Rayleigh fading. **IEEE Trans. Commun.**, v. 55, n. 11, p. 2104-2113, Nov. 2007.

[62] GRADSHTEYN, I. S.; RYZHIK, I. M., **Table of Integrals, Series, and Products.**, 7. ed., San Diego, CA: Academic, 2007.

[63] SIMON, M. K.; ALOUINI, M.S., **Digital communications over fading channels**: A unified approach to performance analysis., 1. ed., New York: John Wiley and Sons, 2000.

[64] FERDINAND, N. S.; RAJATHEVA, N., Unified performance analysis of two-hop amplify-and-forward relay systems with antenna correlation. **IEEE Trans. Wireless Commun**., v. 10, n. 9, p. 3002-3011, 2011.

[65] PAPOULIS, A., **Probability, Random Variables, and Stochastic Processes.**, 4. ed., 2002.

[66] TRANTER, W. H.; et al., **Principles of Communication Systems Simulation with Wireless Applications.**, 1. ed., New Jersey: Prentice Hall, 2004.