UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA
E INFORMÁTICA INDUSTRIAL

MARCOS EDUARDO PIVARO MONTEIRO

MÁXIMA TAXA EFETIVA DE TRANSMISSÃO SEGURA EM REDES MIMOME COM RESTRIÇÕES DE SIGILO

TESE

CURITIBA
2018

MARCOS EDUARDO PIVARO MONTEIRO

MÁXIMA TAXA EFETIVA DE TRANSMISSÃO SEGURA EM REDES MIMOME COM RESTRIÇÕES DE SIGILO

Tese apresentada ao Programa de Pós-Graduação em Engenharia Elétrica e Informática Industrial da Universidade Tecnológica Federal do Paraná como requisito parcial para obtenção do título de "Doutor em Engenharia Elétrica" – Área de Concentração: Telecomunicações e Redes.

Orientador: Prof. Dr. João Luiz Rebelatto

Coorientador: Prof. Dr. Richard Demo Souza

CURITIBA
2018

Dados Internacionais de Catalogação na Publicação

M775m Monteiro, Marcos Eduardo Pivaro
2018 Máxima taxa efetiva de transmissão segura em redes MIMOME com restrições de sigilo / Marcos Eduardo Pivaro Monteiro.— 2018.
77 f.: il.; 30 cm.

Disponível também via World Wide Web.
Texto em português com resumo em inglês.
Tese (Doutorado) - Universidade Tecnológica Federal do Paraná. Programa de Pós-graduação em Engenharia Elétrica e Informática Industrial, Curitiba. Área de Concentração: Telecomunicações e Redes, 2018.
Bibliografia: f. 73-77.

1. Sistemas de comunicação sem fio - Medidas de segurança. 2. Rádio - Transmissores e transmissão. 3. Sistemas MIMO. 4. Antenas (Eletrônica). 5. Interconexões ópticas de espaço livre. 6. Comunicações ópticas. 7. Sistemas de transmissão de dados – Medidas de segurança. 8. Métodos de simulação. 9. Engenharia elétrica - Teses. I. Rebelatto, João Luiz, orient. II. Souza, Richard Demo, coorient. III. Universidade Tecnológica Federal do Paraná. Programa de Pós-Graduação em Engenharia Elétrica e Informática Industrial. IV. Título.

CDD: Ed. 23 -- 621.3

Biblioteca Central do Câmpus Curitiba – UTFPR
Bibliotecária: Luiza Aquemi Matsumoto CRB-9/794

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Diretoria de Pesquisa e Pós-Graduação

TERMO DE APROVAÇÃO DE TESE Nº 169

A Tese de Doutorado intitulada **"Máxima Taxa Efetiva de Transmissão Segura em Redes MIMOME com Restrições de Sigilo",** defendida em sessão pública pelo(a) candidato(a) **Marcos Eduardo Pivaro Monteiro**, no dia 16 de maio de 2018, foi julgada para a obtenção do título de Doutor em Ciências, área de concentração Telecomunicações e Redes, e aprovada em sua forma final, pelo Programa de Pós-Graduação em Engenharia Elétrica e Informática Industrial.

BANCA EXAMINADORA:

Prof(a). Dr(a). João Luiz Rebelatto – Presidente – (UTFPR)
Prof(a). Dr(a). Bartolomeu Ferreira Uchôa-Filho – (UFSC)
Prof(a). Dr(a). Glauber Gomes de Oliveira Brante – (UTFPR)
Prof(a). Dr(a). Evelio Martin Garcia Fernandez – (UFPR)
Prof(a). Dr(a). Guilherme De Santi Peron – (UTFPR)

A via original deste documento encontra-se arquivada na Secretaria do Programa, contendo a assinatura da Coordenação após a entrega da versão corrigida do trabalho.

Curitiba, 16 de maio de 2018.

Gostaria de expressar meus agradecimentos a todos que, direta ou indiretamente, colaboraram para a realização deste trabalho.

a João Luiz Rebelatto, que mostrou-me o caminho a ser tomado, realizando seu papel de orientador de forma exemplar;

a Richard Demo Souza, que com seu apoio ajudou a trilhar o melhor caminho.

RESUMO

MONTEIRO, M. E. P.. MÁXIMA TAXA EFETIVA DE TRANSMISSÃO SEGURA EM REDES MIMOME COM RESTRIÇÕES DE SIGILO. 78 f. Tese – Programa de Pós-Graduação em Engenharia Elétrica e Informática Industrial, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

Neste trabalho, é proposta a utilização de uma versão aprimorada da taxa efetiva de transmissão segura (EST, do inglês *Effective Secrecy Throughput*) recentemente proposta na literatura como métrica de desempenho, a qual, além de levar em consideração a taxa de transmissão e a probabilidade de sigilo no receptor (Bob), também limita a probabilidade de que informações vazem para o espião (Eve). Desta forma, o modelo proposto limita, dentre todas as informações enviadas pelo transmissor (Alice), a quantidade máxima que poderá ser obtida por Eve. A nova métrica é chamada de taxa efetiva de transmissão segura com restrições de sigilo. Além de propor esta nova métrica de desempenho, é avaliado qual o impacto no desempenho do sistema quando consideradas transmissões em radiofrequência (RF, do inglês *Radio Frequency*) e transmissões ópticas em espaço livre (FSO, do inglês *Free-Space Optical*), em um cenário MIMOME (do inglês *Multiple-input Multiple-output Multi-antenna Eavesdropper*) que leva em consideração múltiplas antenas (ou aberturas) em Alice e Bob. Para o cenário FSO, é demonstrado como o uso de *relays* pode aumentar a EST do sistema. Resultados numéricos são então obtidos para verificar as expressões analíticas, demonstrando a influência no desempenho do sistema ao se limitar a quantidade máxima de informações que podem ser obtidas por Eve.

Palavras-chave: canal *wiretap*, múltiplas antenas, probabilidade de sigilo, óptica no espaço livre.

ABSTRACT

MONTEIRO, M. E. P.. MAXIMUM SECRECY THROUGHPUT WITH EAVESDROPPER OUTAGE CONSTRAINTS IN MIMOME NETWORKS. 78 f. Tese – Programa de Pós-Graduação em Engenharia Elétrica e Informática Industrial, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

In this work, an improvement in the recently proposed performance metric effective secrecy throughput (EST) is presented, which, more than taking into account the secrecy rate and the secrecy outage probability, also limits the outage probability of the eavesdropper (Eve). Thus, the proposed scheme limits the maximum amount of information that Eve might be able to obtain of all the information sent by Alice. Under this new metric, referred to as EST with eavesdropper outage constraints, the impact on the system performance when considering a multiple-input multiple-output multiple-antenna eavesdropper (MIMOME) radio frequency and free-space optical (FSO) scenarios are evaluated. For the FSO scenario, it is also shown how the use of relays can increase the EST. Numerical results are performed to validate the analytical expressions, demonstrating the influence of limiting the maximum amount of information that might be obtained by Eve.

Keywords: wiretap channel, multiple antennas, secrecy outage probability, free-space optical.

LISTA DE FIGURAS

LISTA DE SIGLAS

AR	retransmissão com todos ativos, do inglês *All-Active Relaying*
AWGN	ruído aditivo gaussiano branco, do inglês *Additive white Gaussian Noise*
bpcu	bits por uso do canal, do inglês *bits per channel use*
cdf	função de distribuição cumulativa, do inglês *cumulative distribution function*
CSI	conhecimento do estado do canal, do inglês *Channel State Information*
DF	decodifica e encaminha, do inglês *Decode-and-Forward*
EST	taxa efetiva de transmissão segura, do inglês *Effective Secrecy Throughput*
FSO	óptica no espaço livre, do inglês *Free-Space Optical*
MIMOME	do inglês *Multiple-Input Multiple-Output Multi-antenna Eavesdropper*
MISO	do inglês *Multiple-Input Sigle-Output*
MRC	combinação de máxima razão, do inglês *Maximal Ratio Combining*
MRT	transmissão de máxima razão, do inglês *Maximum Ratio Transmission*
pdf	função densidade de probabilidade, do inglês *probability density function*
RC	codificação de repetição, do inglês *Repetition Coding*
RF	radiofrequência, do inglês *Radio Frequency*
SC	combinação de seleção, do inglês *Selection Combining*
SISOME	do inglês *Single-input Single-output Multiple-antenna Eavesdropper*
SNR	relação sinal-ruído, do inglês *Signal to Noise Ratio*
SOP	probabilidade de *Outage* de Sigilo, do inglês *Secrecy Outage Probability*
SR	retransmissão seletiva, do inglês *Selective Relaying*
TAS	seleção de antena de transmissão, do inglês *Transmit Antenna Selection*
TLS	seleção de laser de transmissão, do inglês *Transmit Laser Selection*
WiMAX	do inglês *Worldwide interoperability for Microwave Access*
WLAN	rede de área local sem fio, do inglês *Wireless Local Area Network*
WTC	do inglês *Wire-Tap Channel*

LISTA DE SÍMBOLOS

C_B	capacidade instantânea do canal entre Alice e Bob
C_E	capacidade instantânea do canal entre Alice e Eve
$\mathcal{R}_B$	taxa de palavras código
$\mathcal{R}_E$	taxa de equivocação do espião
$\mathcal{R}$	taxa de sigilo alvo
Ψ	taxa efetiva de transmissão segura
C	capacidade do canal AWGN
B	largura de banda do canal
γ	relação sinal-ruído no receptor
$\mathcal{O}(\mathcal{R}_B)$	probabilidade de *outage* do canal
$\mathcal{O}^{sch}(\mathcal{R}_B)$	probabilidade de *outage* do esquema *sch*
D^{sch}	ordem de diversidade do esquema *sch*
K	chave secreta utilizada pelo modelo de Shannon
Y	palavra código recebida por Bob
Z	palavra código recebida por Eve
C_s	capacidade de sigilo
$I(\cdot;\cdot)$	informação mútua entre os argumentos da função
$\mathcal{S}(\cdot)$	probabilidade de *outage* de sigilo
$\Psi^f(\cdot)$	taxa efetiva de transmissão segura para o esquema de taxa fixa
$\Psi^a(\cdot)$	taxa efetiva de transmissão segura para o esquema adaptativo
N_A^t	número de antenas ou aberturas de transmissão de Alice
N_B^r	número de antenas ou aberturas de recepção de Bob
N_E^r	número de antenas ou aberturas de recepção de Eve
P	potência de transmissão
d_k	distância entre Alice e o nó k
ξ	expoente de perda de percurso
$\mathbf{x}$	vetor de informação a ser transmitido
$\mathbf{b}_k^j$	ruído gaussiano complexo com média zero
σ_k^2	variância do ruído gaussiano complexo
γ^{TAS}	SNR utilizando o esquema TAS
h_T^i	coeficiente quase estático do desvanecimento do canal para a antena transmissora i
r^2	energia por símbolo do sinal recebido em transmissões RF
γ^{SC}	SNR utilizando o esquema SC
h_R^j	coeficiente quase estático do desvanecimento do canal para a antena receptora j
ζ_j	coeficiente relacionado ao peso do sinal recebido pela antena j
γ^{MRC}	SNR instantânea quando utilizado o esquema MRC
$\bar{\gamma}_k$	SNR média por antena receptora
$\mathcal{S}^{\text{th}}$	máximo valor permitido de $\mathcal{S}(\cdot)$
$\mathcal{R}^{a^\star}$	taxa alvo ótima de sigilo

$\gamma(a,b)$	função gama incompleta inferior
$\Gamma(a,b)$	função gama incompleta superior
$\Gamma(\cdot)$	função gama completa
$\mathcal{R}_u^{a^\star}$	valor ótimo de $\mathcal{R}$ sem restrições de SOP
$\mathcal{R}^{th^\star}$	valor ótimo de $\mathcal{R}$ com restrições de SOP
$\Gamma^{-1}(a,b)$	função gama incompleta superior inversa
$\mathsf{G}(\mathcal{R}_{\mathsf{S}}^\star,\mathcal{R}_{\mathsf{M}}^\star)$	ganho do esquema MIMOME sobre o esquema SISOME
$\Psi_{rf}^{\mathsf{m}}(\mathcal{R}_{\mathsf{M}}^\star)$	máxima taxa efetiva de transmissão segura dos esquemas MIMOME em RF
$\Psi_{rf}^{\mathsf{s}}(\mathcal{R}_{\mathsf{S}}^\star)$	máxima taxa efetiva de transmissão segura dos esquemas SISOME em RF
λ	comprimento da onda
η_e	eficiência quântica do fotodetector
E_s	energia do símbolo em transmissões FSO
A	área do feixe
h	constante de Planck
f_o	frequência do sinal óptico recebido
Δ_f	largura de banda equivalente do ruído
A_0	fração da energia disponível no receptor para o fotodetector
ρ	raio da abertura de recebimento
ω_b	tamanho do feixe recebido
$r_{m,n}$	fração da potência disponível alocada para o nó de transmissão do salto n no caminho m
$\mathcal{Z}_{m,n}$	atenuação associada à perda de percurso
$d_{m,n}$	distância de cada salto
σ_l	coeficiente de atenuação
$I_{m,n}$	irradiância associada a um único salto
$I_{a,m,n}^{i,j}$	desvanecimento causado por turbulência atmosférica
$f_{m,n}^{\gamma\gamma}(\cdot)$	pdf da irradiância considerando a turbulência atmosférica
$K_c(\cdot)$	função Bessel modificada do segundo tipo e ordem c
$F_{m,n}^{\gamma\gamma}(\cdot)$	cdf da irradiância considerando a turbulência atmosférica
${}_1F_2(\cdot)$	função hipergeométrica generalizada
α	parâmetro de larga escala
β	parâmetro de pequena escala
α_p	parâmetro de ajuste em larga escala
β_p	parâmetro de ajuste em pequena escala
$\sigma_R^2(d_p)$	variância *Rytov*
ν	número de onda
C_n^2	índice de refração da estrutura
ω_e	largura de feixe equivalente
τ	deslocamento radial no receptor
σ_s	desvio padrão para o eixo vertical e horizontal
$f_{m,n}^p(\cdot)$	pdf da variável aleatória que representa os erros de alinhamento
γ_0	SNR livre de turbulência
$f_{m,n}^{\gamma\gamma p}(\cdot)$	pdf da irradiância quando os erros de alinhamento e a turbulência atmosférica são considerados
$G_{\cdot,\cdot}^{\cdot,\cdot}(\cdot)$	função Meijer-G

$F^{\gamma\gamma p}_{m,n}(\cdot)$	cdf da irradiância quando os erros de alinhamento e a turbulência atmosférica são considerados
${}_1\tilde{F}_2(\cdot)$	função hipergeométrica regularizada
X	variável relacionada à larga escala da variável aleatória gama-gama
Y	variável relacionada à pequena escala da variável aleatória gama-gama
κ	parâmetro de forma
θ	parâmetro de escala
Z	variável aleatória devido ao erro de alinhamento
$\mathcal{R}^{a^\star}_{E,u}$	valor ótimo sem restrições em $\mathcal{R}_E$
$\mathcal{R}^{th^\star}_{E}$	valor ótimo restringido de $\mathcal{R}_E$ para um dado máximo valor permitido de S^{th}
$\text{E}_\cdot(\cdot)$	função integral exponencial
θ^{AP}_k	parâmetro de escala da variável gama aproximada
κ^{AP}_k	parâmetro de forma da variável gama aproximada
$\mathcal{O}^f_\cdot(\cdot)$	probabilidade de *outage* em termos de confiabilidade para o esquema de taxa fixa
$Q(\cdot,0,\cdot)$	função gama incompleta regularizada generalizada
$\mathcal{R}^{f^\star}_{B,c}$	valor ótimo restringido de $\mathcal{R}_B$
$\text{W}(\cdot)$	função W de Lambert
N^t_R	número de aberturas de transmissão dos *relays* por caminho
N^r_R	número de aberturas de recepção dos *relays* por caminho
N_P	número de caminhos
R_N	número de *relays*
$R_{N,E}$	número de *relays* entre Alice e as Eves
$N_{P,E}$	número de Eves
$N^t_{m,n}$	número de aberturas transmissoras do canal $[m,n]$
$N^r_{m,n}$	número de aberturas receptoras do canal $[m,n]$
T_N	número de nós legítimos transmitindo para o receptor
$O^f_{m,n}(\cdot)$	probabilidade de transmissão confiável para um único salto
S_c	grupo de *relays*
$O^f(S_c)$	probabilidade de *outage* para Bob quando todos os *relays* em S_c transmitem a mensagem
$N^t_{g,E}$	número de aberturas do nó transmissor no qual o g-ésimo Eve obtém a mensagem.

SUMÁRIO

1 INTRODUÇÃO

A segurança na camada física em redes sem fio é um tema de crescente importância uma vez que permite, através de sua utilização, projetar redes que garantem a segurança das informações transmitidas sem a necessidade de se identificar a capacidade computacional de um possível espião. Manter a segurança em tais redes é um grande desafio, pois envolve encontrar meios de garantir que a mensagem chegue ao seu destino sem ser compreendida por quaisquer outros nós não autorizados. Tipicamente, utilizam-se algoritmos de criptografia para resolver problemas de segurança em redes de comunicação. Esses algoritmos normalmente não se alteram com as características do canal de comunicação e dependem unicamente de operações matemáticas que são difíceis de computar, como exemplo a fatoração de números primos (BLOCH; BARROS, 2011).

Recentemente, como uma alternativa (ou complemento) para a abordagem clássica relacionada às técnicas de criptografia, a segurança na camada física foi proposta para redes sem fio (BARROS; RODRIGUES, 2006; BLOCH; BARROS, 2011) demonstrando que, o desvanecimento, que é visto como um problema em termos de confiabilidade em tais redes, pode ser útil para aumentar a segurança das informações transmitidas. Assim, a segurança na camada física não depende da dificuldade do problema matemático em descriptografar a mensagem, e sim da incerteza inerente aos canais de comunicação.

De maneira similar às redes sem restrições de sigilo (do inglês *secrecy*), a máxima taxa de transmissão de dados de maneira segura (capacidade de sigilo) é afetada diretamente pelas condições do canal. Para que seja possível a existência de uma capacidade de sigilo não nula, os nós legítimos (o transmissor, Alice, e o receptor, Bob) precisam ter a qualidade instantânea do canal melhor que a do canal utilizado pelo espião (Eve), ou seja, a capacidade instantânea do canal entre Alice e Bob, C_B, deve ser maior que a capacidade instantânea do canal entre Alice e Eve, C_E.

Mais especificamente, a capacidade de sigilo pode ser obtida através da camada física com a utilização de *wiretap codes*, que são códigos capazes de garantir assintoticamente, com uma pequena probabilidade arbitrária de erro, que a mensagem será recebida corretamente por Bob de maneira sigilosa (BLOCH; BARROS, 2011). Tais códigos utilizam três taxas distintas, a saber, $\mathcal{R}_B$, $\mathcal{R}_E$ e $\mathcal{R}$, de maneira que $\mathcal{R}_E = \mathcal{R}_B - \mathcal{R}$. Enquanto $\mathcal{R}_B$ representa a taxa de palavras código (ou taxa de transmissão) utilizada por Alice, $\mathcal{R}_E$ representa a taxa de equivocação do espião, que é utilizada para confundir Eve,

e $\mathcal{R}$ corresponde à taxa de sigilo alvo.

Para que seja possível atingir uma comunicação perfeitamente sigilosa (do inglês *perfect secrecy*), dois requisitos são necessários: *i)* $\mathcal{R}_B \leq C_B$ (restrição de confiabilidade); *ii)* $\mathcal{R}_E > C_E$ (restrição de sigilo). Enquanto a restrição de confiabilidade garante que a mensagem enviada por Alice e recebida por Bob seja totalmente recuperada, a restrição de sigilo tem como objetivo certificar que Eve não será capaz de identificar quaisquer partes da informação transmitida por Alice.

Para que isso seja possível, Alice deve conhecer o estado instantâneo dos dois canais, de maneira que C_E e C_B possam ser determinados. Se tanto C_E e C_B são conhecidos no lado do transmissor, a máxima taxa de transmissão sigilosa pode ser obtida (KHISTI; WORNELL, 2010; OGGIER; HASSIBI, 2008). Entretanto, com exceção de alguns casos especiais, não é realista assumir que Alice conhece C_E e, desta maneira, a restrição de sigilo $\mathcal{R}_E \geq C_E$ não pode ser garantida para todas as transmissões. Neste caso, é necessário recorrer a uma análise probabilística, determinando a probabilidade de *outage* de sigilo (SOP, do inglês *Secrecy Outage Probability*) (BARROS; RODRIGUES, 2006; BLOCH; BARROS, 2011). A SOP representa a probabilidade de Eve entender quaisquer informações sobre a mensagem que está sendo transmitida, evento este que ocorre quando $\mathcal{R}_E < C_E$.

Em (YAN et al., 2014, 2015) três esquemas SISOME (do inglês *Single-input Single-output Multiple-antenna Eavesdropper*) para comunicação em radiofrequência (RF), a saber, ligado-desligado, taxa fixa e adaptativo, foram introduzidos. O esquema ligado-desligado transmite informações apenas quando a taxa de transmissão $\mathcal{R}_B$ for menor ou igual à capacidade do canal legítimo C_B, enquanto o esquema de taxa fixa transmite a uma taxa constante com base na capacidade média do canal. Por fim, o esquema adaptativo ajusta $\mathcal{R}_B$ de acordo com a capacidade instantânea do canal, de maneira que $C_B = \mathcal{R}_B$. Além dos esquemas apresentados, em (YAN et al., 2014) foi proposta uma nova métrica capaz de determinar o desempenho em termos de segurança, a taxa efetiva de transmissão segura Ψ (EST, do inglês *Effective Secrecy Throughput*), definida como a taxa alvo de transferência sigilosa $\mathcal{R}$ multiplicada pela probabilidade de se garantir tanto a restrição de confiabilidade quanto a restrição de sigilo.

Quando disponível, o conhecimento instantâneo do estado do canal (CSI, do inglês *Channel State Information*) legítimo pode ser utilizado para adaptar $\mathcal{R}$ e maximizar Ψ. Uma comparação entre os esquemas adaptativo e ligado-desligado, que assumem ter CSI do canal legítimo, é feita em (YAN et al., 2014), onde é demonstrado que o esquema

adaptativo sempre obtém melhores resultados. É importante notar que a taxa efetiva de transmissão segura não está limitada aos cenários propostos, e pode ser utilizada em diversos outros cenários, como exemplo na presença de um ruído artificial (YANG et al., 2015). Entretanto, a métrica de desempenho Ψ não tem nenhuma restrição com relação à SOP, o que significa que a quantidade de informação obtida por Eve quando o sistema está operando em valor ótimo de Ψ pode estar acima daquela tolerável por um determinado sistema.

Embora a segurança nas transmissões ópticas no espaço livre (FSO, do inglês *Free-Space Optical*) seja intrinsecamente maior que aquela observada nas transmissões em RF devido à alta direcionalidade dos feixes ópticos, a intercepção de sinais ópticos também é possível (LOPEZ-MARTINEZ et al., 2015), de maneira que torna-se necessário identificar meios de evitá-las. Para interceptar o link legítimo, dois cenários de ameaças principais podem ser distinguidos: i) Eve está próximo do transmissor legítimo (Alice) e bloqueia o raio laser para coletar uma grande quantidade de energia; ii) Eve está perto do receptor legítimo (Bob) e, assim, recebe parte do sinal destinado a Bob devido à radiação do feixe sendo refletida por partículas pequenas. O segundo caso é mais razoável como um cenário de ameaça real, pois, se Eve estiver perto de Alice, ela não poderá interceptar o feixe sem bloquear a linha de visão, o que poderia permitir que Alice detecte sua presença visualmente ou com base na variação da potência recebida por Bob (LOPEZ-MARTINEZ et al., 2015).

Neste trabalho, primeiramente é introduzida uma restrição à máxima SOP permitida quando Ψ é otimizado. Considerando redes em RF, o esquema de transmissão adaptativa de (YAN et al., 2014) é estendido para um cenário MIMOME (do inglês *Multiple-input Multiple-output Multi-antenna Eavesdropper*), que assume que tanto Alice quanto Bob têm múltiplas antenas operando, respectivamente, com os esquemas de seleção de antena de transmissão (TAS, do inglês *Transmit Antenna Selection*) e de combinação de seleção (SC, do inglês *Selection Combining*) (GOLDSMITH, 2005). Uma importante característica do TAS é a necessidade de uma quantidade mínima de *feedback* e, embora o espião seja capaz de ouvir o canal de *feedback*, a antena selecionada é ótima apenas para o canal principal, de maneira que o desempenho do espião não é aumentado (ALVES et al., 2012; YANG et al., 2013). No modelo utilizado, considera-se também que Eve utiliza a combinação de máxima razão (MRC, do inglês *Maximal Ratio Combining*).

Em seguida, um cenário de FSO coerente MIMOME é analisado, onde Alice adota a seleção de laser de transmissão (TLS, do inglês *Transmit Laser Selection*), enquanto

Bob e Eve operam utilizando o MRC. Adotando a métrica EST com restrições de sigilo e considerando a distribuição gama-gama para modelar o desvanecimento do canal FSO, é avaliado o desempenho dos esquemas de transmissão adaptativa e de taxa fixa. Por fim, motivado pelos resultados apresentados em (ABOU-RJEILY, 2015), que demonstram que é sempre melhor adicionar aberturas no transmissor e receptor ao invés de adicionar novos *relays*, o impacto do uso de *relays* em comunicações MIMOME FSO com restrições de sigilo é analisado para os esquemas adaptativo e de taxa fixa. Quando considerado o uso de *relays*, devido ao grande número de nós na rede, é assumido que Alice adota as técnicas codificação de repetição (RC, do inglês *Repetition Coding*) e TLS para, respectivamente, o esquema de taxa fixa e o adaptativo. Para realizar as retransmissões, são utilizadas as técnicas de retransmissão com todos ativos (AR, do inglês *All-Active Relaying*) e de retransmissão seletiva (SR, do inglês *Selective Relaying*) para, respectivamente, os esquemas de taxa fixa e adaptativo. Note que a escolha de tais técnicas está relacionada ao fato de que o CSI instantâneo do canal legítimo está disponível apenas quando considerado o esquema adaptativo.

Para comunicações por RF, os resultados analíticos e numéricos demonstram que a EST se deteriora de maneira significativa com a diminuição da máxima SOP permitida e que, quando utilizado o esquema MIMOME com TAS, esta diminuição é amenizada de forma que o sistema é capaz de operar próximo à taxa ótima de Ψ. Além do mais, a vantagem relativa entre os esquemas MIMOME e SISOME aumenta com o número de antenas em Eve. Em comunicações FSO, é demonstrada a importância do uso de múltiplas aberturas para maximizar a EST e minimizar a informação obtida por Eve. Por fim, quando considerado o uso de *relays*, é demonstrado que o esquema adaptativo se beneficia tanto do aumento do número de caminhos quanto do aumento do número de saltos, enquanto o esquema de taxa fixa beneficia-se apenas do aumento do número de saltos.

1.1 MOTIVAÇÃO

Problemas relacionados à segurança em redes de comunicação são de grande importância para a sociedade. Com o objetivo de resolver estes problemas, soluções voltadas para a criptografia das informações foram desenvolvidas. Entretanto, tais algoritmos dependem de operações matemáticas difíceis de resolver para garantir sua segurança, ignorando os possíveis benefícios da aleatoriedade proporcionada pelo canal de comunicação à segurança das informações transmitidas. Uma vez que a segurança é vista

como um fator essencial nas comunicações, todas as camadas do protocolo de comunicação devem ser utilizadas de uma maneira eficaz para melhorar o sigilo das informações transmitidas. Esses problemas são ainda maiores em redes sem fio em RF devido à natureza *broadcast* de tais redes, que permitem que todos os nós em uma determinada área sejam capazes de receber a informação transmitida. Assim, a segurança na camada física foi proposta recentemente em redes sem fio demostrando que, o desvanecimento, que normalmente é visto como um problema nas comunicações, pode ser utilizado com o objetivo de aumentar a segurança em tais redes. Ainda que a segurança em transmissões FSO seja intrinsecamente maior que a observada nas transmissões em RF, um espião pode capturar parte da informação transmitida por Alice, de maneira que uma análise da segurança em tais redes também deve ser considerada.

1.2 OBJETIVOS

1.2.1 Objetivo Geral

Melhorar a segurança de redes de comunicação sem fio através da utilização da segurança na camada física.

1.2.2 Objetivos Específicos

- Propor um limite máximo para a SOP, com intuito de limitar a quantidade máxima de informação capturada por Eve;
- Verificar o desempenho de sistemas MIMOME em termos da taxa efetiva de transmissão segura para transmissões em RF;
- Obter equações analíticas e compará-las com resultados numéricos com o objetivo de determinar o desempenho do sistema com restrições de SOP;
- Determinar a vantagem relativa entre os esquemas MIMOME e SISOME, identificando os benefícios de se adicionar mais antenas em Alice e Bob;
- Verificar a taxa efetiva de transmissão segura com restrições de SOP em redes FSO para os esquemas adaptativo e de taxa fixa;
- Determinar como o uso de *relays* pode aumentar a taxa efetiva de transmissão segura para os dois esquemas analisados.

1.3 PUBLICAÇÕES E SUBMISSÕES

Este trabalho foi organizado de maneira a apresentar os resultados das publicações e submissões realizadas durante o período de doutorado. Mais especificadamente, o Capítulo 3 apresenta os resultados publicados no seguinte artigo:

- MONTEIRO, M. E. P.; REBELATTO, J. L.; SOUZA, R. D.; BRANTE, G. *Maximum secrecy throughput of transmit antenna selection with eavesdropper outage constraints.* **IEEE Signal Processing Letters**, v. 22, n. 11, p. 2069-2072, Nov 2015. ISSN 1070-9908.

A primeira metade do Capítulo 4 está relacionada aos resultados do artigo abaixo, que foi aceito e encontra-se em processo final de publicação:

- MONTEIRO, M. E. P.; REBELATTO, J. L.; SOUZA, R. D.; BRANTE, G. *Maximum Secrecy Throughput of MIMOME FSO Communications with Outage Constraints.* **IEEE Transactions on Wireless Communications**, 2018. ISSN 1536-1276.

Já a segunda metade do Capítulo 4 apresenta os resultados da seguinte submissão, que ainda encontra-se em processo de revisão:

- MONTEIRO, M. E. P.; REBELATTO, J. L.; SOUZA, R. D.; BRANTE, G. *Effective Secrecy Throughput Analysis of Relay-Assisted Free-Space Optical Communications.* **IEEE Transactions on Vehicular Technology**, 2018.

Além das publicações e submissões listadas acima, outras publicações em temas não diretamente apresentados na tese, mas que foram obtidas ou submetidas durante o período de doutorado, são listadas a seguir:

- MONTEIRO, M. E. P.; REBELATTO, J. L.; SOUZA, R. D.; BRANTE, G. *Information-Theoretic Location Verification System With Directional Antennas for Vehicular Networks.* **IEEE Transactions on Intelligent Transportation Systems**, v. 17, p. 93-103, 2016.
- MONTEIRO, M. E. P.; REBELATTO, J. L. ; SOUZA, R. D. ; RAYEL, O. K. ; MORITIZ, G. L. ; UCHOA FILHO, B. F. *Secrecy Outage Probability of Network-Coded Cooperation without Channel State Information.* **IEEE International Symposium on Wireless Communication Systems**, 2015, Bruxelas.

- MONTEIRO, M. E. P.; REBELATTO, J. L. ; BRANTE, G. *On the Energy Efficiency of Relay-Assisted In-Vivo Nano-Networks Communications.* Submetido para: **IEEE International Symposium on Wireless Communication Systems**, 2018, Lisboa.

1.4 ESTRUTURA DO DOCUMENTO

O Capítulo 2 apresenta conceitos preliminares relacionados ao sigilo em redes de comunicação. No Capítulo 3 é apresentado o esquema MIMOME para comunicações por RF, incluindo uma análise da taxa efetiva de transmissão segura ótima quando uma máxima SOP é imposta. Primeiramente, o capítulo traz informações sobre o funcionamento do esquema MIMOME. Em seguida, é apresentado como uma restrição de SOP pode ser utilizada para limitar a quantidade máxima de informações obtidas por Eve. Resultados analíticos são então obtidos para o esquema apresentado e comparados com resultados numéricos, demonstrando a eficiência da utilização de mais de uma antena em Alice e em Bob. Uma vez que existem custos relacionados à utilização de várias antenas, comparações entre os benefícios trazidos pelo esquema MIMOME são feitas em relação ao esquema SISOME.

A transmissão óptica no espaço livre é apresentada no Capítulo 4. A transmissão direta é primeiramente analisada, apresentando o modelo de sistema e expressões analíticas para as taxas ótimas, seguido pelos resultados numéricos que demonstram a precisão das equações obtidas. Em seguida, um cenário com múltiplos *relays* é apresentado, demonstrando que o uso de *relays* pode ser benéfico para comunicações FSO. Por fim, o Capítulo 5 apresenta as conclusões finais deste trabalho.

2 PRELIMINARES

Para facilitar a compreensão dos cenários apresentados nos próximos capítulos em comunicações por RF e FSO, este capítulo introduz diversos conceitos. Primeiramente, serão apresentados os conceitos de capacidade do canal, probabilidade de *outage* e ordem de diversidade. Enquanto a capacidade do canal e a probabilidade de *outage* serão usadas para definir a métrica de desempenho utilizada neste trabalho, a ordem de diversidade está relacionada com as técnicas de transmissão e recepção utilizadas que, por sua vez, são apresentadas em seguida. Por fim, será apresentada a métrica taxa efetiva de transmissão segura, que é apropriada para redes sem fio na presença de um espião.

2.1 CONFIABILIDADE

A confiabilidade é importante em qualquer rede de comunicação, e refere-se ao recebimento correto (livre de erros) das informações pelo receptor em um sistema de comunicação. Conforme apresentado no Capítulo 1, este é um dos requisitos para se atingir uma comunicação perfeitamente sigilosa. Nesta seção, em primeiro lugar são apresentados os conceitos de capacidade e a probabilidade de *outage*, que estão diretamente relacionados com a restrição de confiabilidade. Por fim, é apresentada a ordem de diversidade, que é calculada com base na probabilidade de *outage*.

2.1.1 Capacidade do Canal

A capacidade de um canal de comunicação define o limite máximo de comunicação alcançável. Este limite foi introduzido por Shannon em (SHANNON, 1948), quando se demonstrou que códigos corretores de erro podem ser utilizados para aumentar a taxa de comunicação com uma probabilidade de erro arbitrariamente pequena. Entretanto, a capacidade de comunicação confiável do canal nunca será maior que a capacidade definida por Shannon, não importa o quão eficiente seja o código. Assim, se a taxa de transmissão for maior que a capacidade do canal, a probabilidade de erro de transmissão será inevitavelmente maior que zero. A capacidade de Shannon para um canal com ruído aditivo gaussiano branco (AWGN, do inglês *Additive White Gaussian Noise*) é dada por (SHANNON, 1948)

$$C = B\log_2(1+\gamma), \tag{1}$$

onde C é a capacidade do canal em bits/segundo (bps), B representa a largura de banda em Hertz (Hz) e γ representa a relação sinal ruído no receptor (SNR, do inglês *Signal to Noise Ratio*). É importante notar que, para canais sem fio, a relação sinal-ruído γ apresentada na equação (1) deve incluir, também, os efeitos causados pelo desvanecimento do canal. Uma vez que tais efeitos variam de acordo com o modelo do sistema escolhido, este trabalho apresenta os detalhes sobre o desvanecimento separadamente nos Capítulos 3 e 4 para transmissões em RF e FSO, respectivamente. É importante ressaltar, também, que o restante deste trabalho considera a capacidade normalizada, de maneira que $B = 1$ Hz.

2.1.2 Probabilidade de *Outage*

Devido à natureza aleatória do canal sem fio, pode-se não ser possível garantir que a taxa de transmissão esteja abaixo da capacidade do canal C. Nestas situações, pode-se utilizar probabilidade de *outage* como métrica de desempenho. Esta probabilidade é definida como (GOLDSMITH, 2005)

$$\begin{aligned} \mathcal{O}(\mathcal{R}_B) &= \Pr\{C < \mathcal{R}_B\} \\ &= \Pr\{\log_2(1+\gamma) < \mathcal{R}_B\}, \\ &= \Pr\{\gamma < 2^{\mathcal{R}_B} - 1\} \end{aligned} \tag{2}$$

onde $\mathcal{O}(\mathcal{R}_B)$ é a probabilidade de *outage* e $\mathcal{R}_B$ representa a taxa de transmissão. Assim, um evento de *outage* ocorrerá toda vez que a taxa de transmissão for maior que a capacidade do canal definida por (1).

2.1.3 Ordem de Diversidade

Combater o desvanecimento do canal sem fio é uma das formas de se diminuir a *outage* e, com este propósito, técnicas de diversidade podem ser utilizadas. Em tais técnicas, múltiplas versões do sinal sujeitas a desvanecimentos independentes são obtidas pelo receptor, criando assim uma diversidade no receptor e aumentando a chance de se obter sucesso na transmissão. Tal efeito está diretamente ligado ao fato de que, ao obter diversas versões independentes de um mesmo sinal, a chance de todas estas versões estarem em desvanecimento profundo é diminuída de forma considerável. As técnicas de diversidade, que selecionam ou combinam as diversas versões recebidas do sinal, podem ser avaliadas em termos da ordem de diversidade. Para um determinado esquema *sch*

com probabilidade de *outage* dada por $\mathcal{O}^{sch}(\mathcal{R}_B)$, tem-se que a ordem de diversidade D^{sch} é obtida como:

$$D^{sch} = \lim_{\gamma \to \infty} -\frac{\log_2(\mathcal{O}^{sch}(\mathcal{R}_B))}{\log_2(\gamma)}. \tag{3}$$

2.2 TÉCNICAS DE DIVERSIDADE

Esta seção apresenta os esquemas de diversidade utilizados neste trabalho. Uma vez que esquemas distintos são utilizados de acordo com o tipo de transmissão, as técnicas apresentadas são divididas em duas categorias: comunicação por radiofrequência e comunicação óptica no espaço livre.

2.2.1 Comunicação por Radiofrequência (RF)

Transmitir informações em canais de comunicação sem fio pode ser visto como uma tarefa desafiadora devido ao desvanecimento de multipercurso causado por combinações destrutivas das múltiplas versões que chegam ao nó receptor. Conforme descrito na seção anterior, para diminuir os efeitos prejudiciais do desvanecimento, sistemas MIMO, com múltiplas antenas transmissoras e receptoras, foram incluídos em diversos padrões de comunicação sem fio, como o IEEE 802.11 para redes de área local sem fio (WLAN, do inglês *Wireless Local Area Network*), o IEEE 802.16 para redes WiMAX (do inglês *Worldwide interoperability for Microwave Access*), e outros (TAN et al., 2013).

Em um sistema MIMO, em que ambos transmissor e receptor são providos com múltiplas antenas, dependendo da maneira e da quantidade de antenas selecionadas para realizar a transmissão/recepção, pode-se estabelecer uma troca de benefícios (*tradeoff*) entre desempenho e complexidade. Na sequência serão apresentadas as características básicas de algumas técnicas para transmissão (TAS e MRT) e recepção (SC e MRC) em sistemas MIMO.

2.2.1.1 Seleção de Antena de Transmissão (TAS)

No esquema TAS, como o próprio nome sugere, apenas um subconjunto dentre todas as antenas transmissoras disponíveis é selecionado para efetivamente transmitir dados. Esta seleção é geralmente realizada com base em informações enviadas pelo destino através de um canal de retorno.

É possível mostrar que, mesmo que este esquema não seja ótimo em termos da

probabilidade de *outage*, ele consegue obter a máxima ordem de diversidade disponível, que neste caso equivale à quantidade total de antenas transmissoras. Isto é possível mesmo que apenas uma antena seja selecionada para transmitir. Uma vez que um número menor de antenas transmissoras está sendo ativado em um dado momento, o esquema TAS é capaz de reduzir o número de cadeias de transmissão de RF, que são compostas por um amplificador de baixo ruído, conversores de frequência, conversores analógico-digital e digital-analógico, filtros e outros elementos (SANAYEI; NOSRATINIA, 2004). Dessa forma, pode-se dizer que o esquema TAS prima por uma menor complexidade/custo de implementação, às custas de um pior desempenho em termos de probabilidade de *outage* que o esquema que será visto a seguir.

2.2.1.2 Transmissão de Máxima Razão (MRT)

A técnica transmissão de máxima razão (MRT, do inglês *Maximum Ratio Transmission*) obtém diversidade na transmissão através da distribuição ponderada da potência de transmissão entre todas as antenas. Assim, para cada uma das antenas transmissoras, o sinal transmitido será multiplicado por um ganho complexo proporcional ao ganho do canal correspondente. Esta multiplicação complexa realiza tanto o processo de remoção das fases associadas a cada caminho (processo de *co-phasing*), quanto a ponderação do ganho de transmissão em relação ao ganho de cada canal (GOLDSMITH, 2005). Este esquema obtém ordem de diversidade máxima e atinge o mínimo valor possível para a probabilidade de *outage*. Entretanto, esta técnica requer o envio, além de cada SNR, das fases por antena. Essa informação, segundo (ZHANG et al., 2014) e diferente da técnica TAS, é difícil de ser obtida livre de erros.

2.2.1.3 Combinação de Seleção (SC)

A técnica SC é análoga à técnica TAS, mas agora aplicada na recepção. Ela consiste em selecionar apenas um subconjunto das antenas receptoras (geralmente apenas uma, aquela que apresentar a melhor SNR) para efetivamente realizar a recepção. Dessa forma, similarmente ao TAS, abre-se mão de um desempenho ótimo em termos de probabilidade de *outage* para que os custos e complexidade de implementação sejam reduzidos. Vale ressaltar que, apesar de não atingir valores ótimos em termos de probabilidade de *outage*, o esquema SC é capaz de obter a maior ordem de diversidade possível, que neste caso é igual à quantidade de antenas receptoras.

2.2.1.4 Combinação de Máxima Relação (MRC)

Conforme descrito na subseção anterior, para a técnica SC o sinal utilizado será aquele recebido pela antena com a maior SNR. Entretanto, é possível também utilizar a técnica MRC, que é mais elaborada quando comparada à técnica SC. Para a técnica MRC, similar à técnica MRT, o sinal resultante será uma soma ponderada de todos os sinais recebidos pelas diversas antenas receptoras.

Dessa forma, tem-se que o esquema MRC é capaz de atingir o menor valor possível para a probabilidade de *outage* (e obviamente também a maior ordem de diversidade), às custas de uma maior complexidade de implementação, visto que o destino necessita das informações de ganho e fase do canal de todas as antenas receptoras. Note ainda que, embora tanto o MRC quanto o MRT atinjam ordem de diversidade máxima, o desempenho do MRC é superior ao desempenho do MRT uma vez que, para o esquema MRT, a potência de transmissão terá que ser dividida de forma ponderada entre todas as antenas.

2.2.2 Comunicação Óptica no Espaço Livre (FSO)

De maneira similar às técnicas de diversidade para comunicações em RF, as técnicas de diversidade para transmissões em FSO buscam mitigar efeitos da turbulência causada na propagação dos sinais ópticos. Para a transmissão, são apresentadas as técnicas TLS e RC. Na presença de vários caminhos entre o transmissor original (fonte) e o receptor final (destino), considerando que a fonte conhece o melhor caminho até destino, é apresentada a técnica SR. Quando a fonte não conhece os estados dos canais, é utilizada a técnica AR. No receptor, é utilizada a técnica MRC descrita na Seção 2.2.1.4.

2.2.2.1 Seleção de Laser de Transmissão (TLS)

A técnica TLS, de maneira similar à técnica TAS apresentada na Seção 2.2.1.1, consiste em selecionar o laser de transmissão que resulta na maior SNR no lado do receptor. Ainda de maneira similar ao TAS, a SNR final é obtida como o máximo entre todas as possíveis SNRs utilizando individualmente cada uma das aberturas de transmissão.

2.2.2.2 Codificação de Repetição (RC)

A técnica RC é utilizada quando a fonte e os *relays* não conhecem o estado instantâneo do canal. Assim, os nós legítimos transmitem o mesmo sinal por todas as suas aberturas.

2.2.2.3 Retransmissão Seletiva (SR)

A retransmissão seletiva é utilizada quando existem múltiplos caminhos entre a fonte e o destino, e a fonte conhece qual é o melhor caminho. De maneira similar à técnica TLS, a SNR resultante será a máxima SNR entre todas as SNR dos caminhos disponíveis entre a fonte e o destino.

2.2.2.4 Retransmissão com Todos Ativos (AR)

A técnica AR é utilizada quando os nós legítimos transmissores não conhecem o estado dos canais utilizados. Assim, a informação é transmitida através de todos os caminhos entre a fonte e o destino. Neste caso, para manter uma comparação justa com a técnica SR, a potência total de transmissão é dividida entre todos os nós transmissores.

2.3 SIGILO (*SECRECY*)

Nesta Seção, conceitos relacionados ao sigilo serão definidos, incluindo a capacidade de sigilo e a probabilidade de *outage* de sigilo. O conceito de sigilo em redes de comunicação foi introduzido por Shannon em (SHANNON, 1949). O modelo utilizado por Shannon, e apresentado na Figura 1, considerava que Alice, para enviar a informação M para Bob, codificava a mensagem na palavra código X através da chave secreta K. Durante a transmissão, Eve era capaz de ouvir a palavra código sem qualquer tipo de atenuação ou ruído. Entretanto, em sistema reais, alguma forma de ruído está sempre presente, e a suposição de Shannon foi feita levando em consideração um código corretor de erro extremamente eficiente, de forma que a informação poderia ser recuperada com uma taxa de erro arbitrariamente baixa.

Em (WYNER, 1975) foi introduzido o modelo denominado WTC (do inglês *Wire-Tap Channel*), que considerava a existência de um ruído nos canais entre o transmissor e o receptor, e entre o transmissor e o espião. Em (WYNER, 1975), foi demonstrado que

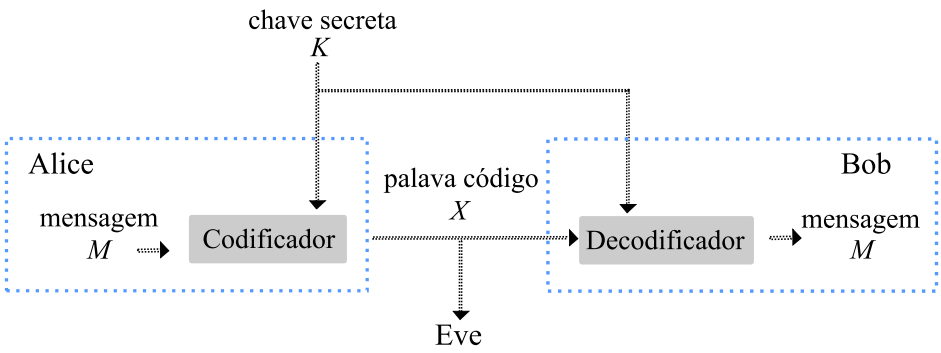


Figura 1 – Modelo do sistema utilizado em (SHANNON, 1949).
Fonte: Autoria própria.

existe um código capaz de garantir assintoticamente uma probabilidade arbitrariamente baixa de erro no receptor e de segurança. Conforme descrito no Capítulo 1, esses códigos são chamados de *wiretap codes* (BARROS; RODRIGUES, 2006).

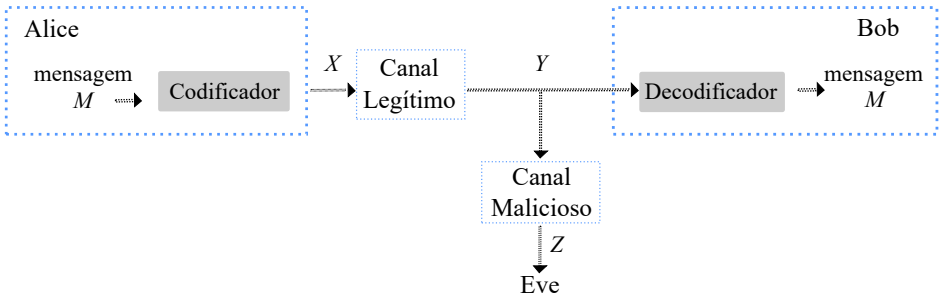


Figura 2 – Modelo WTC, proposto em (WYNER, 1975). Fonte: Autoria própria.

Assume-se que Alice deseja enviar a mensagem M com k-bits através do canal legítimo. Para isso, esta mensagem é codificada em uma palavra código X com n-bits. A mensagem codificada observada por Bob é dada então por Y, enquanto a mensagem observada por Eve é dada por Z, conforme ilustrado na Figura 2. Nestes termos, um *wiretap code* deve garantir que: *i)* Z não pode fornecer quaisquer informações sobre a mensagem original M; *ii)* Y pode ser decodificado em M com uma probabilidade de erro ϵ arbitrariamente pequena (THANGARAJ et al., 2007). Em (WYNER, 1975) foi demonstrado que ambos os objetivos podem ser obtidos sem o uso de chaves de segurança para determinadas condições dos canais legítimo e malicioso.

2.3.1 Capacidade de Sigilo

Uma medida de desempenho comumente utilizada para se avaliar o desempenho de sistemas em termos de sigilo é a capacidade de sigilo (do inglês *Secrecy Capacity*),

definida em (BARROS; RODRIGUES, 2006) como a taxa máxima de transmissão em que o espião não é capaz de obter quaisquer informações sobre a mensagem original, podendo também ser representada através da informação mútua relacionada aos canais legítimo e malicioso.

A capacidade de sigilo C_s é dada como (LAI; GAMAL, 2008)

$$\begin{aligned} C_s &= \max\ I(X;Y|Z) \\ &= \max\ (I(X;Y) - I(X;Z)), \end{aligned} \tag{4}$$

onde $I(\cdot;\cdot)$ representa a informação mútua entre os argumentos da função. Note que a capacidade de sigilo só é maior que zero quando a capacidade instantânea do canal legítimo (entre Alice e Bob) é maior que a capacidade instantânea do canal malicioso (entre Alice e Eve). Outra métrica comumente utilizada, quando apenas as capacidades médias estão disponíveis, é a probabilidade de existência da capacidade de sigilo. Esta probabilidade é dada como (BARROS; RODRIGUES, 2006)

$$\begin{aligned} \Pr\{C_s > 0\} &= \Pr\{C_B - C_E > 0\} \\ &= \Pr\{C_B > C_E\}. \end{aligned} \tag{5}$$

onde C_B é a capacidade do canal legítimo e C_E é a capacidade do canal malicioso.

Note que, se a capacidade média de Bob for igual a capacidade média de Eve, então a probabilidade de existência da capacidade de sigilo é igual a 0,5. Além disso, de (5), é possível se obter uma comunicação segura mesmo quando a capacidade média do espião é maior que a capacidade média de Bob.

2.3.2 Probabilidade de *Outage* de Sigilo

A probabilidade de *outage* de sigilo, introduzida em (BLOCH et al., 2008), é uma métrica de desempenho que mede a probabilidade do nó espião obter quaisquer informações sobre a mensagem original. Conforme apresentado na subseção 2.1.2, um evento de *outage* de confiabilidade, no qual a informação é transmitida sem erros, ocorre quando a capacidade do canal legítimo é inferior a uma dada taxa $\mathcal{R}_B$ bpcu (do inglês *bits per channel use*). Assim, tem-se

$$\mathcal{O}(\mathcal{R}_B) = \Pr\{C_B < \mathcal{R}_B\}. \tag{6}$$

De maneira equivalente, a SOP $\mathcal{S}(\cdot)$ pode ser definida pela probabilidade da taxa

de equivocação do espião $\mathcal{R}_E$ ser menor que a capacidade do canal malicioso C_E sendo, assim, dada por

$$\mathcal{S}(\mathcal{R}_E) = \Pr\{C_E > \mathcal{R}_E\}. \tag{7}$$

A probabilidade de *outage* de sigilo sozinha não é capaz de definir os valores ótimos de $\mathcal{R}_B$ e $\mathcal{R}_E$, de maneira que uma métrica mais eficaz, que considere tanto as restrições de sigilo quanto as restrições de confiabilidade, torna-se necessária.

2.4 TAXA EFETIVA DE TRANSMISSÃO SEGURA

Em (YAN et al., 2014) foi proposta uma nova métrica de desempenho, a taxa efetiva de transmissão segura Ψ, que é definida como a taxa de transferência segura alvo $\mathcal{R}$ multiplicada pela probabilidade de se garantir tanto a restrição de confiabilidade quanto a restrição de sigilo, de forma que

$$\Psi(\mathcal{R}_E, \mathcal{R}_B) = \mathcal{R}(1 - \mathcal{O}(\mathcal{R}_B))(1 - \mathcal{S}(\mathcal{R}_E)). \tag{8}$$

Conforme o nome sugere, esta métrica mede a quantidade de bits por uso do canal que, simultaneamente, Eve não foi capaz de obter e Bob foi capaz de decodificar.

2.4.1 Esquema com Taxa Fixa

Para o esquema de transmissão de taxa fixa, Alice não tem informações sobre o estado instantâneo do(s) canal(is) legítimo(s) (C_B) e do(s) canal(is) utilizado(s) pelo espião (C_E), o que significa que Alice possui apenas a SNR média de tais canais. Note também que tanto as restrições de confiabilidade quanto as restrições de sigilo não são garantidas, e é preciso determinar $\mathcal{R}_B$ e $\mathcal{R}_E$ que maximizem conjuntamente a EST. A EST para o esquema de taxa fixa $\Psi^f(\cdot)$ é obtida como

$$\Psi^{\mathsf{f}}(\mathcal{R}_E, \mathcal{R}_B) = (\mathcal{R}_B - \mathcal{R}_E)\Pr\{C_B \geq \mathcal{R}_B\}\Pr\{C_E \leq \mathcal{R}_E\}. \tag{9}$$

2.4.2 Esquema Adaptativo

No esquema adaptativo, é assumido que a capacidade do canal legítimo é conhecida (ou seja, existe um canal de retorno), de maneira que é possível sempre garantir

que $\Pr\{C_B \geq \mathcal{R}_B\} = 1$. Assim, a taxa efetiva de transmissão segura para o esquema adaptativo $\Psi^a(\cdot)$ pode ser definida como

$$\begin{aligned}\Psi^a(\mathcal{R}_E, \mathcal{R}_B) &= \mathcal{R}\Pr\{C_B \geq \mathcal{R}_B\}\Pr\{C_E \leq \mathcal{R}_E\} \\ &= \mathcal{R}\Pr\{C_E \leq \mathcal{R}_E\} \\ &= (\mathcal{R}_B - \mathcal{R}_E)\Pr\{C_E \leq \mathcal{R}_E\}.\end{aligned} \tag{10}$$

É importante notar ainda que garantir $\Pr\{C_E \leq \mathcal{R}_E\}$ exigiria ter o CSI instantâneo sobre o canal de Eve, o que normalmente não é possível. Por fim, é importante ressaltar que a métrica EST não limita a probabilidade máxima de *outage* de sigilo, de maneira que, para uma dada aplicação, um possível espião pode ser capaz de obter uma quantidade de informações maior que a máxima quantidade aceitável.

2.5 COMENTÁRIOS

Neste Capítulo, primeiramente conceitos relacionados com a confiabilidade nas transmissões foram apresentados, incluindo a capacidade do canal, a probabilidade de *outage* e a ordem de diversidade. Em seguida, foram apresentadas algumas das principais técnicas de diversidade para comunicações em RF, começando com as técnicas TAS e MRT onde o transmissor, respectivamente, seleciona a antena que maximiza a SNR no receptor, e aloca de maneira ponderada a potência de transmissão de cada antena. Em seguida, técnicas de combinação de diversidade no receptor foram apresentadas, mais especificamente, SC e MRC. Enquanto a combinação de seleção seleciona a antena receptora com maior SNR, a combinação de máxima relação utiliza a soma ponderada dos sinais obtidos por todas as antenas receptoras. Em seguida, técnicas de diversidade para comunicações FSO foram apresentadas, começando pela técnica TLS, que é equivalente à técnica TAS para comunicações FSO, seguida pela técnica RC, onde o mesmo sinal é enviado por todas as aberturas do nó transmissor. As técnicas de retransmissão AR e SR foram então apresentadas onde, respectivamente, a fonte transmite para todos os *relays* em sua vizinhança e a fonte transmite apenas para o *relay* que está no melhor caminho.

Conceitos relacionados ao sigilo em redes de comunicação foram então abordados, incluindo a capacidade de sigilo e a probabilidade de *outage* de sigilo. Com base nestes conceitos, foi então apresentada a taxa efetiva de transmissão segura, que é uma métrica proposta em (YAN et al., 2014) capaz de determinar o desempenho em termos da capacidade de transmissão de dados sigilosos em redes de comunicação. Por fim, foram

apresentados os esquemas adaptativo e de taxa fixa, que serão utilizados nos Capítulos 3 e 4 para transmissões em, respectivamente, RF e FSO.

É importante notar que os conceitos que foram apresentados neste capítulo servirão como base para a análise realizada em seguida. Mais especificamente, a métrica taxa efetiva de transmissão segura será aprimorada no próximo capítulo, adicionando restrições à máxima probabilidade de *outage* de sigilo permitida. Enquanto o próximo capítulo abordará o uso desta nova métrica para redes em RF, o Capítulo 4 irá propor o uso da nova métrica em comunicações FSO.

3 MÁXIMA TAXA DE TRANSMISSÃO SEGURA PARA COMUNICAÇÕES MIMOME RF UTILIZANDO TAS COM RESTRIÇÕES DE SIGILO

A taxa efetiva de transmissão segura apresentada na Seção 2.4, embora seja baseada na teoria da informação e na capacidade de sigilo, não tem limitações relacionadas à SOP, o que significa que, quando o sistema trabalha no valor ótimo de Ψ, Eve pode ser capaz de obter uma quantidade de informação maior do que o máximo valor tolerável pelo sistema. Assim, neste capítulo uma nova restrição é imposta à taxa efetiva de transmissão segura, limitando a máxima SOP aceita pelo sistema, e este conceito é aplicado à redes de comunicação sem fio em RF. Com base nos resultados numéricos e analíticos que serão apresentados neste capítulo, tem-se que a utilização de múltiplas antenas no transmissor e no receptor legítimo permite que o sistema opere com uma SOP muito menor que aquela apresentada para sistemas SISOME.

3.1 MODELO DO SISTEMA

Para comunicações em RF, considera-se uma rede de comunicação sem fio formada por um transmissor, Alice (A), comunicando com um receptor legítimo, Bob (B), na presença de um espião, Eve (E). Alice está equipada com N_A^t antenas utilizando o esquema TAS, enquanto Bob utiliza o esquema SC nas suas N_B^r antenas, e Eve está equipada com N_E^r antenas e utiliza o esquema MRC, o que representa um cenário de pior caso. Note que estas técnicas de diversidade foram descritas na Seção 2.2. O modelo do sistema é ilustrado na Figura 3.

O pacote transmitido pela i-ésima antena de Alice e recebido pela j-ésima antena do nó $k \in \{B,E\}$ é dado como

$$\mathbf{y}_k^{i,j} = \sqrt{P\, d_k^{-\xi}}\, h_k^{i,j}\, \mathbf{x} + \mathbf{b}_k^j, \tag{11}$$

onde P é a potência de transmissão, que é alocada para a antena de transmissão que maximiza a SNR em Bob (informado através de um canal público de retorno), d_k é a distância entre Alice e o nó k, ξ é o expoente de perda de percurso, $h_k^{i,j}$ é o coeficiente de desvanecimento quase-estático, cujo envelope é modelado como uma variável aleatória *Rayleigh* independente e identicamente distribuída, $\mathbf{x}$ é o vetor de informação a ser transmitido[1], e $\mathbf{b}_k^j$ é o ruído gaussiano complexo com média zero e variância σ_k^2.

[1]Um quadro pode ser definido como um conjunto de bits agrupados, que são utilizados para

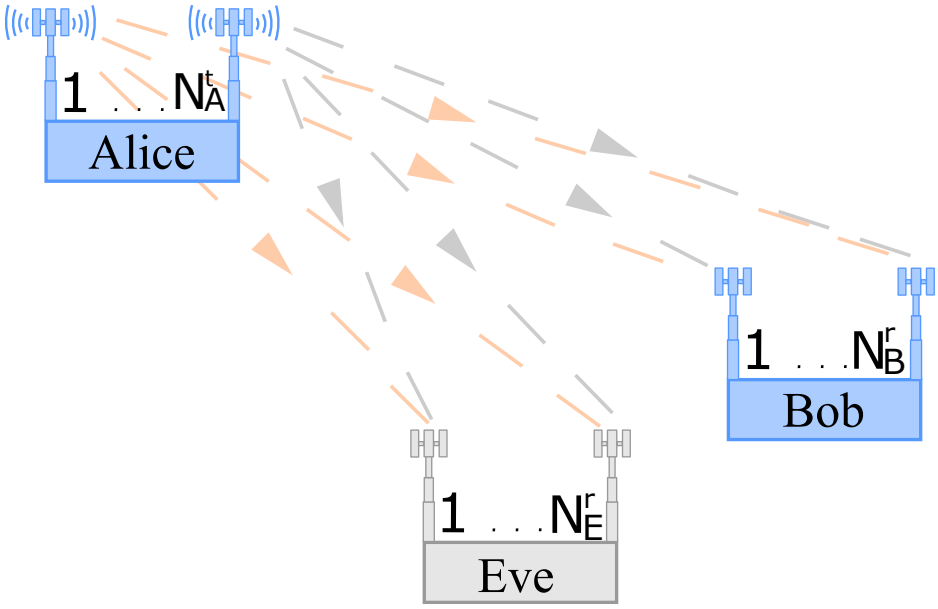


Figura 3 – Sistema MIMOME, composto por um par de nós legítimos, sendo um transmissor (Alice, com N_A^t antenas) e um receptor (Bob, com N_B^r antenas), comunicando-se na presença de um espião (Eve, com N_E^r antenas).
Fonte: Autoria própria.

Para se obter as SNRs para Bob e Eve, primeiro é necessário identificar os efeitos causados pelas técnicas de diversidade apresentadas na Seção 2.2. Considerando somente o esquema TAS na transmissão e que o receptor tem apenas uma antena (MISO, do inglês *Multiple-Input Sigle-Output*), a SNR γ^{TAS} recebida pelo nó receptor é dada como

$$\gamma^{TAS} = \frac{r^2}{\sigma_k^2} \max_{1 \leq i \leq N_A^t} |h_T^i|^2, \tag{12}$$

onde h_T^i representa o coeficiente quase estático do desvanecimento do canal quando considerado que a antena transmissora i está sendo utilizada, r^2 é a energia por símbolo do sinal recebido desprezando o desvanecimento em pequena escala.

Quando utilizada a técnica SC na recepção, a SNR γ^{SC} instantânea é dada como

$$\gamma^{SC} = \frac{r^2}{\sigma^2} \max_{1 \leq j \leq N_k^r} |h_R^j|^2, \tag{13}$$

onde h_R^j representa o coeficiente quase estático do desvanecimento do canal para a antena receptora j do nó receptor. Por fim, quando utilizada a técnica MRC na recepção, sendo $\zeta_j \colon j \in \{1,...,N_k^r\}$ o coeficiente relacionado ao peso do sinal recebido pela antena j, tem-se

comunicação entre os nós da rede.

que a SNR γ^{MRC} do sinal recebido é dada como

$$\gamma^{MRC} = \frac{r^2}{\sigma^2} \frac{\sum_{j=1}^{N_k^r} |\zeta_j h^j|^2}{\sum_{j=1}^{N_k^r} \zeta_j^2}. \tag{14}$$

Utilizando os valores para cada um dos pesos ζ_j que maximizam a SNR, o valor resultante é simplesmente a soma das SNRs em cada uma das antenas (GOLDSMITH, 2005).

Com base nas equações (12), (13) e (14), tem-se que as SNRs instantâneas vistas por Bob (TAS/SC) e por Eve (MRC) são dadas como

$$\gamma_B = \bar{\gamma}_B \max_{\substack{1 \leq i \leq N_A^t \\ 1 \leq j \leq N_B^r}} |h_B^{i,j}|^2, \tag{15}$$

e

$$\gamma_E = \bar{\gamma}_E \sum_{1 \leq j \leq N_E^r} |h_E^{i,j}|^2, \tag{16}$$

onde $\bar{\gamma}_k = P/(d_k^{\xi} \sigma_k^2)$ é a SNR média por antena receptora (assumida como igual para todas as antenas do nó k). Por fim, utilizando (5) e quando considerada a transmissão direta com um canal *Rayleigh* quase-estático, a probabilidade de existência da capacidade de sigilo é dada como (BARROS; RODRIGUES, 2006)

$$\begin{aligned} \Pr\{C_s > 0\} &= \Pr\{C_B - C_E > 0\} \\ &= \frac{\bar{\gamma}_B}{\bar{\gamma}_B + \bar{\gamma}_E}. \end{aligned} \tag{17}$$

3.2 ESQUEMA PROPOSTO

Seguindo o esquema adaptativo descrito em (YAN et al., 2014, 2015), para transmissões em RF é assumido que Alice tem a CSI instantânea apenas do canal legítimo e da antena selecionada, e tem apenas a SNR média $\bar{\gamma}_E$ do canal utilizado por Eve, o que é plausível quando Eve é um espião passivo. Assim, Alice é capaz de calcular a capacidade instantânea do canal legítimo C_B e, consequentemente ajustar $\mathcal{R}$ de acordo com C_B e $\bar{\gamma}_E$, sujeito à restrição $0 \leq \mathcal{R} \leq C_B$. Isso indica que a restrição de confiabilidade é garantida. Assim, a taxa $\mathcal{R}$ é adaptada de acordo com a SNR instantânea do canal legítimo, que é assumida como disponível para Alice. Entretanto, a restrição de sigilo não pode ser garantida, uma vez que a quebra desta restrição ocorre quando a taxa de equivocação do espião $\mathcal{R}_E$ é menor que a capacidade do canal do espião C_E.

Uma vez que Eve utiliza a técnica MRC, que foi descrita na Seção 2.2, a SOP definida em (7) pode ser reescrita como (GOLDSMITH, 2005)

$$\begin{aligned}\mathcal{S}_{rf}(\mathcal{R}) &= \Pr\{C_E > \mathcal{R}_E\} = \Pr\left\{\gamma_E > 2^{C_B-\mathcal{R}} - 1\right\} \\ &= \exp\left(-\frac{2^{C_B-\mathcal{R}}-1}{\bar{\gamma}_E}\right)\sum_{j=0}^{N_E^r-1}\frac{1}{j!}\left[\frac{2^{C_B-\mathcal{R}}-1}{\bar{\gamma}_E}\right]^j.\end{aligned} \tag{18}$$

Utilizando (10), a taxa efetiva de transmissão segura pode ser definida para o esquema adaptativo em RF como (YAN et al., 2014)

$$\Psi_{rf}^{a}(\mathcal{R}) = \mathcal{R}\left[1 - \mathcal{S}_{rf}(\mathcal{R})\right]. \tag{19}$$

Embora a taxa efetiva de transmissão segura para o esquema adaptativo Ψ^a apresentada em (19) seja uma métrica de desempenho útil, ela não restringe a máxima SOP permitida. Ou seja, pode ser possível que Eve opere em uma probabilidade muito baixa de *outage* obtendo, possivelmente, uma quantidade grande de informação e comprometendo a segurança da comunicação. Para prevenir essa situação, é imposta neste trabalho uma nova restrição, definindo a taxa efetiva de transmissão segura com restrições de sigilo $\Psi^{\mathsf{m}}(\mathcal{R})$ como

$$\Psi_{rf}^{\mathsf{m}}(\mathcal{R}) = \begin{cases} \Psi_{rf}^{a}(\mathcal{R}), & \text{se } \mathcal{S}_{rf}(\mathcal{R}) \leq \mathcal{S}_{rf}^{\text{th}}; \\ 0 & \text{se } \mathcal{S}_{rf}(\mathcal{R}) > \mathcal{S}_{rf}^{\text{th}}, \end{cases} \tag{20}$$

onde $\mathcal{S}^{\text{th}}$ é o máximo valor permitido de $\mathcal{S}_{rf}(\mathcal{R})$.

3.2.1 Taxa Alvo Ótima de Sigilo $\mathcal{R}^{a^\star}$

Existe um valor ótimo de $\mathcal{R}$ que maximiza a taxa efetiva de transmissão segura de (20), uma vez que (19) é uma função côncava conforme descrito a seguir no Lema 1. Para determinar $\mathcal{R}^{a^\star}$, primeiro deve-se obter o valor ótimo de $\mathcal{R}$ sem quaisquer restrições, independente da SOP, que é apresentada como segue.

Lema 1. *O valor de $\mathcal{R}$ sem restrições de SOP que maximiza $\Psi_{rf}^{a}(\mathcal{R})$ é obtido através da*

solução da seguinte equação de ponto fixo[2]*:*

$$\mathcal{R}_u^{a^\star} = \frac{[\bar{\gamma}_E]^{N_E^r}\,\gamma\left(N_E^r, \frac{\chi}{\bar{\gamma}_E}\right)\exp\left(\frac{\chi}{\bar{\gamma}_E}\right)}{\chi^{N_E^r-1}\,[\chi+1]\log(2)}, \tag{21}$$

onde $\chi = 2^{C_B-\mathcal{R}_u^{a^\star}} - 1$ *e* $\gamma(a,b) = \int_0^b e^{-t}t^{a-1}dt$ *corresponde a função gama incompleta inferior.*

Demonstração. Para obter (21), primeiro é importante perceber que a probabilidade de (18) pode ser reescrita como (GOLDSMITH, 2005; WANG; GIANNAKIS, 2003)

$$\mathcal{S}_{rf}(\mathcal{R}) = \frac{\Gamma\left(N_E^r, \frac{2^{C_B-\mathcal{R}}-1}{\bar{\gamma}_E}\right)}{\Gamma\left(N_E^r\right)}, \tag{22}$$

onde $\Gamma(a,b) = \int_b^\infty e^{-t}t^{a-1}dt$ é a função gama incompleta superior e $\Gamma(\cdot)$ é a função gama completa. Uma vez que a SOP em (22) é uma função monotonicamente crescente de $\mathcal{R}$ para $\mathcal{R} < C_B$, que pode ser visto uma vez que $\partial\mathcal{S}_{rf}(\mathcal{R})/\partial\mathcal{R} > 0$, $\forall\,\mathcal{R} < C_B$, ocorre que (19) é uma função côncava, de maneira que o valor ótimo de $\mathcal{R}$ que maximiza $\Psi_{rf}^a(\mathcal{R})$ é obtido igualando a primeira derivada de (19) a zero e resolvendo para $\mathcal{R}^{a^\star}$. Assim, ocorre que a primeira derivada de $\Psi_{rf}^a(\mathcal{R})$ é dada como

$$\frac{\partial\Psi_{rf}^a(\mathcal{R})}{\partial\mathcal{R}} = 1 - \frac{1}{\Gamma(N_E^r)}\left[\Gamma\left(N_E^r, \frac{2^{C_B-\mathcal{R}}-1}{\bar{\gamma}_E}\right) + \frac{2^{C_B}\exp\left(\frac{1-2^{C_B-\mathcal{R}}}{\bar{\gamma}_E}\right)\left(\frac{2^{C_B-\mathcal{R}}-1}{\bar{\gamma}_E}\right)^{N_E^r}\mathcal{R}\log(2)}{2^{C_B}-2^{\mathcal{R}}}\right], \tag{23}$$

e, depois de realizar manipulações algébricas em (23) e com o fato de que $\Gamma(a) = \gamma(a,b) + \Gamma(a,b)$, obtém-se (21). □

Teorema 1. *O valor ótimo de* $\mathcal{R}$ *que maximiza a taxa efetiva de transmissão segura* $\Psi_{rf}^m(\mathcal{R})$ *para o esquema MIMOME sujeito a um limiar de SOP* $\mathcal{S}^{th}$ *é dado como*

$$\mathcal{R}^{a^\star} = \min\left(\mathcal{R}_u^{a^\star}, \mathcal{R}^{th^\star}\right), \tag{24}$$

onde $\mathcal{R}_u^{a^\star}$ *é obtido de* (21) *e* $\mathcal{R}^{th^\star}$ *é o valor máximo restrito de* $\mathcal{R}$*, que é obtido como*

$$\mathcal{R}^{th^\star} = \log_2\left(\frac{2^{C_B}}{1+\bar{\gamma}_E\Gamma^{-1}\left(N_E^r, \mathcal{S}^{th}\Gamma(N_E^r)\right)}\right), \tag{25}$$

[2]Uma equação de ponto fixo é uma função tal que $f : X \to X$, ou seja, f mapeia X em X, de forma que existe pontos x tais que $x = f(x)$. Os pontos que satisfazem essa equação são chamados de pontos fixos de f (BARATA, 2016).

onde $\Gamma^{-1}(a,b)$ *corresponde a função gama incompleta superior inversa.*

Demonstração. Com base no fato de que $\mathcal{S}_{rf}(\mathcal{R})$ é uma função monotonicamente crescente de $\mathcal{R}$ para $\mathcal{R} < C_B$, pode-se ver que a taxa em um dado limiar $\mathcal{S}^{\text{th}}$ é a máxima taxa permitida. Usando (18), pode-se encontrar a função inversa com relação à $\mathcal{S}^{\text{th}}$, que é dada como (25). Obtendo a derivada primeira de (23), pode-se ver que, em um cenário sem restrições, $\Psi^{\mathsf{m}}_{rf}(\mathcal{R})$ é uma função côncava, o que significa que $\Psi^{\mathsf{m}}_{rf}(\mathcal{R})$ aumenta para $\mathcal{R} < \mathcal{R}_u^{a^\star}$ e diminui para $\mathcal{R} > \mathcal{R}_u^{a^\star}$. Assim, sem restrições, $\mathcal{R}_u^{a^\star}$ representa a máxima taxa de sigilo, no sentido de que qualquer valor maior que $\mathcal{R}_u^{a^\star}$ irá resultar em um valor menor de $\Psi^{\mathsf{m}}_{rf}(\mathcal{R})$. Percebendo que $\mathcal{R}^{a^\star}$ não pode ser maior que (25) devido à restrição de SOP, pode-se ver que $\mathcal{R}^{a^\star}$ é o menor valor entre (21) e (25), que é dado por (24). □

3.2.2 Ganho de MIMOME sobre SISOME

Definição 1. *O ganho do esquema MIMOME sobre o esquema SISOME* $\mathsf{G}(\mathcal{R}^\star_{\mathsf{S}},\mathcal{R}^\star_{\mathsf{M}})$ *em termos da taxa efetiva de transmissão segura pode ser definido como*

$$\mathsf{G}(\mathcal{R}^\star_{\mathsf{S}},\mathcal{R}^\star_{\mathsf{M}}) \triangleq \frac{\Psi^{m}_{rf}(\mathcal{R}^\star_{\mathsf{M}})}{\Psi^{s}_{rf}\left(\mathcal{R}^\star_{\mathsf{S}}\right)}, \tag{26}$$

onde $\Psi^{m}_{rf}(\mathcal{R}^\star_{\mathsf{M}})$ *e* $\Psi^{s}_{rf}(\mathcal{R}^\star_{\mathsf{S}})$ *correspondem, respectivamente, à máxima taxa efetiva de transmissão segura dos esquemas MIMOME e SISOME, operando com as respectivas taxas ótimas de sigilo* $\mathcal{R}^\star_{\mathsf{M}}$ *e* $\mathcal{R}^\star_{\mathsf{S}}$.

Assim, tem-se que $\mathsf{G}(\mathcal{R}^\star_{\mathsf{S}},\mathcal{R}^\star_{\mathsf{M}})$ aumenta com o aumento de N^t_A ou com o aumento de N^r_B, uma vez que $\Psi^{\mathsf{m}}_{rf}(\mathcal{R}^\star_{\mathsf{M}})$ aumenta com N^t_A ou N^r_B, enquanto $\Psi^{\mathsf{s}}_{rf}(\mathcal{R}^\star_{\mathsf{S}})$ não depende de N^t_A e de N^r_B. Entretanto, quando N^r_E aumenta, tanto $\Psi^{\mathsf{m}}_{rf}(\mathcal{R}^\star_{\mathsf{M}})$ quanto $\Psi^{\mathsf{s}}_{rf}(\mathcal{R}^\star_{\mathsf{S}})$ diminuem.

Proposição 1. *Para o esquema MIMOME com* $N^t_A \geq 2$*, o ganho relativo* $\mathsf{G}(\mathcal{R}^\star_{\mathsf{S}},\mathcal{R}^\star_{\mathsf{M}})$ *sobre o esquema SISOME aumenta com o aumento de* N^r_E.

Demonstração. Para se perceber isso, primeiramente é importante notar que $\partial\mathsf{G}(\mathcal{R}^\star_{\mathsf{S}},\mathcal{R}^\star_{\mathsf{M}})/\partial N^r_E \geq 0 \forall N^r_E$, provando que $\mathsf{G}(\mathcal{R}^\star_{\mathsf{S}},\mathcal{R}^\star_{\mathsf{M}})$ é uma função monotonicamente crescente de N^r_E. De maneira equivalente, com a ajuda de (20), (22) e (26), pode-se

escrever esse ganho como

$$\mathsf{G}\left(\mathcal{R}_{\mathsf{S}}^{\star},\mathcal{R}_{\mathsf{M}}^{\star}\right)=\frac{\mathcal{R}_{\mathsf{M}}^{\star}\,\gamma\left(N_E^r,\frac{2^{C_B^{\mathrm{TAS}}-\mathcal{R}_{\mathrm{M}}^{\star}}-1}{\bar{\gamma}_E}\right)}{\mathcal{R}_{\mathsf{S}}^{\star}\,\gamma\left(N_E^r,\frac{2^{C_B^{\mathrm{SISO}}-\mathcal{R}_{\mathsf{S}}^{\star}}-1}{\bar{\gamma}_E}\right)}. \tag{27}$$

Então, depois de utilizar a aproximação $\gamma(a,b)\approx(1/a)(b)^a$ (WANG; GIANNAKIS, 2003), que é válida para pequenos valores de b, e percebendo que $C_B^{\mathrm{TAS}}\geq C_B^{\mathrm{SISO}}$, pode-se configurar o esquema MIMOME para operar com $\mathcal{R}_{\mathsf{S}}^{\star}$ ao invés de $\mathcal{R}_{\mathsf{M}}^{\star}$ obtendo o limiar inferior de (27) como:

$$\mathsf{G}\left(\mathcal{R}_{\mathsf{S}}^{\star},\mathcal{R}_{\mathsf{S}}^{\star}\right)\approx\left[\frac{2^{C_B^{\mathrm{TAS}}-\mathcal{R}_{\mathsf{S}}^{\star}}-1}{2^{C_B^{\mathrm{SISO}}-\mathcal{R}_{\mathsf{S}}^{\star}}-1}\right]^{N_E^r}. \tag{28}$$

Uma vez que $C_B^{\mathrm{TAS}}-\mathcal{R}_{\mathsf{S}}^{\star}\geq C_B^{\mathrm{SISO}}-\mathcal{R}_{\mathsf{S}}^{\star}$ (sendo iguais quando $N_A^t=N_B^r=1$), pode-se ver que o argumento de (28) é maior ou igual a um, que significa que o ganho é uma função monotonicamente crescente do expoente N_E^r. □

3.3 RESULTADOS NUMÉRICOS

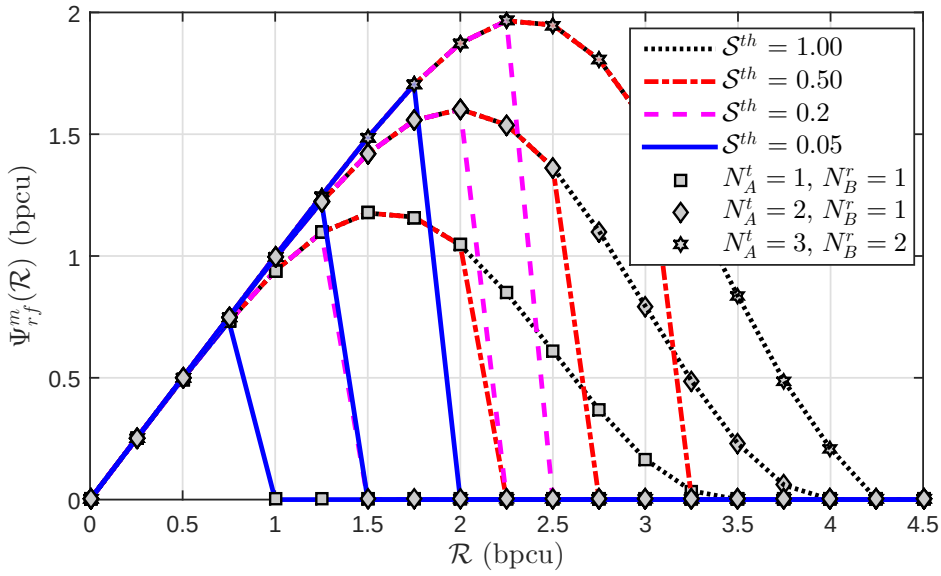


Figura 4 – $\Psi_{rf}^{\mathbf{m}}(\mathcal{R})$ em função de $\mathcal{R}$ para $N_E^r=2$, $\gamma_B=10$ dB, $\bar{\gamma}_E=0$ dB e $\mathcal{S}^{\mathrm{th}}\in\{1,0.5,0.2,0.05\}$.
Fonte: Autoria própria.

Esta seção apresenta resultados numéricos para comprovar as análises descritas neste Capítulo. A Figura 4 apresenta a taxa EST em função da taxa de sigilo alvo para

os esquemas MIMOME ($N_A^t = 2$, $N_B^r = 1$ e $N_A^t = 3$, $N_B^r = 2$) e SISOME ($N_A^t = 1$), para diferentes valores de $\mathcal{S}^{\text{th}}$. Pode-se ver que, quando existe uma máxima SOP permitida, o esquema SISOME de (YAN et al., 2014) pode não ser capaz de prover o valor ótimo da taxa de transferência, tendo seu desempenho prejudicado de maneira significativa quando $\mathcal{S}^{\text{th}}$ diminui. Para $\mathcal{S}^{\text{th}} = 0.05$, por exemplo, menos que 0.8 bpcu é obtido pelo SISOME, enquanto é possível obter 1.2 bpcu e 1.9 bpcu quando utilizados os valores $N_A^t = 2$, $N_B^r = 1$ e $N_A^t = 3$, $N_B^r = 2$, respectivamente.

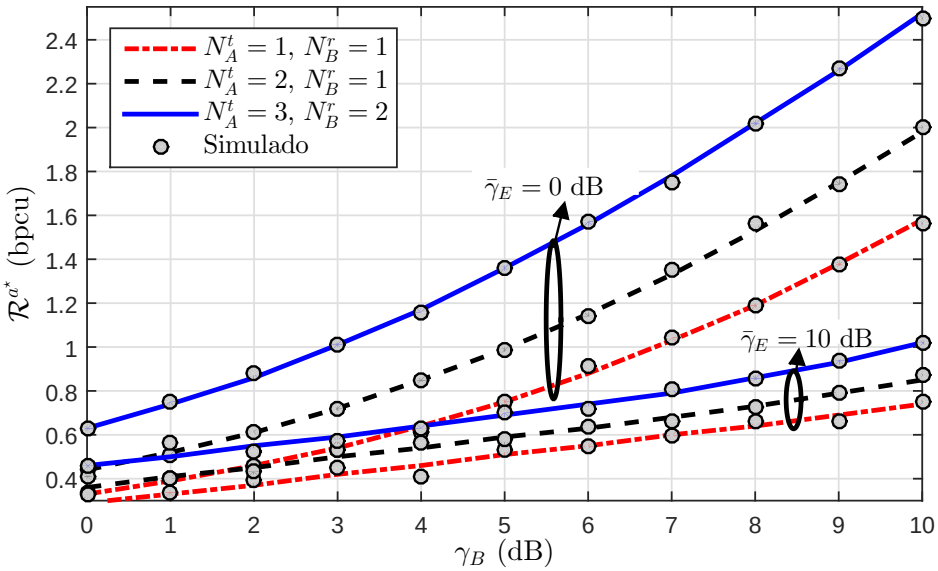


Figura 5 – Taxa de sigilo ótima alvo em função da SNR instantânea em Bob para $N_E^r = 2$, $\mathcal{S}^{\text{th}} = 1$ e $\bar{\gamma}_E \in \{0{,}10\}$ dB.
Fonte: Autoria própria.

A taxa de sigilo ótima alvo $\mathcal{R}^{a^\star}$ que maximiza a taxa de sigilo efetiva é apresentada na Figura 5 em função de γ_B. Pode-se ver que $\mathcal{R}^{a^\star}$ para MIMOME diverge de SISOME com o aumento de γ_B (ou, de maneira alternativa, quando $\bar{\gamma}_E$ diminui). Assim, além de permitir que o sistema opere em um valor melhor de $\Psi_{rf}^{\mathsf{m}}(\mathcal{R})$, o uso de múltiplas antenas em Alice e Bob também permite que o sistema opere em um valor maior da taxa de sigilo. Comparando a Figura 4 com a Figura 5, pode-se ver que, ainda que o ganho em termos de $\mathcal{R}^{a^\star}$ (ou seja, $\mathcal{R}_{\mathsf{M}}^\star/\mathcal{R}_{\mathsf{S}}^\star$) não seja tão grande quanto o ganho obtido utilizando (26), $\Psi_{rf}^{\mathsf{m}}(\mathcal{R})$ é uma métrica de desempenho melhor para sistemas sigilosos uma vez que esta representa a taxa que não pode ser obtida por Eve. Também pode-se ver que os valores teóricos obtidos utilizando (24) são confirmados com boa precisão pelos resultados das simulações.

Uma vez que antenas adicionais poderiam ser inseridas tanto em Bob quanto em Alice, a Figura 6 investiga qual a melhor distribuição das antenas em termos de $\Psi_{rf}^{\mathsf{m}}(\mathcal{R})$,

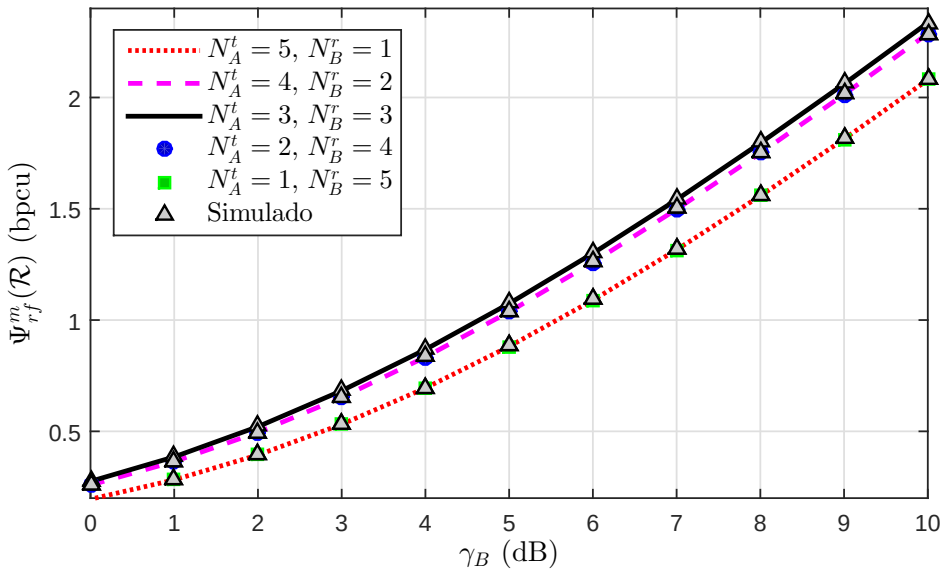


Figura 6 – $\Psi_{rf}^{\mathsf{m}}(\mathcal{R})$ em função da SNR instantânea em Bob para $N_E^r = 2$ e $\bar{\gamma}_E = 0$ dB, utilizando um total de $N_A^t + N_B^r = 6$ antenas.
Fonte: Autoria própria.

para um total de $N_A^t + N_B^r = 6$ antenas utilizadas no canal legítimo. Pode-se esperar que, uma vez que Alice realiza TAS e Bob utiliza SC, adicionar antenas em Bob tem o mesmo efeito de adicionar antenas em Alice. Entretanto, conforme demonstrado na Figura 6, o melhor desempenho é obtido quando $N_A^t = N_B^r$, ou seja, quando o número de antenas Bob é igual ao de Alice. Este resultado é justificado pelo fato de que a maior ordem de diversidade possível para um dado número total de antenas ocorre quando $N_A^t = N_B^r$.

Na Figura 7 é apresentada a taxa efetiva de transmissão segura em função de $\mathcal{S}^{\text{th}}$. Pode-se ver que, quando o número de antenas aumenta, o máximo limiar $\mathcal{S}^{\text{th}}$ para se obter o máximo $\Psi_{rf}^{\mathsf{m}}(\mathcal{R})$ diminui, além do fato de que o máximo $\Psi_{rf}^{\mathsf{m}}(\mathcal{R})$ aumenta com o número de antenas. Para o esquema SISOME com $\bar{\gamma}_E = 0$ dB, a taxa de transmissão segura diminui de maneira significativa para $\mathcal{S}^{\text{th}} < 0.5$, que indica que é necessário escolher entre diminuir significativamente a taxa de transmissão segura ou permitir que Eve intercepte boa parte da informação transmitida. Para o esquema MIMOME, pode-se obter de maneira simultânea um valor maior de $\Psi_{rf}^{\mathsf{m}}(\mathcal{R})$ e menor de $\mathcal{S}^{\text{th}}$, que indica que existe um ganho na taxa efetiva de transmissão segura e na probabilidade de Eve não ser capaz de interceptar a comunicação. Assim, pode-se ver que, comparando os esquemas MIMOME e SISOME, a mesma taxa de transmissão segura pode ser obtida com um valor muito menor de $\mathcal{S}^{\text{th}}$ para o primeiro esquema e, como consequência, existe menos informações sigilosas vazadas para Eve.

Na Figura 8 é apresentada a EST em função de $\bar{\gamma}_E$ (dB) para diferentes valores de

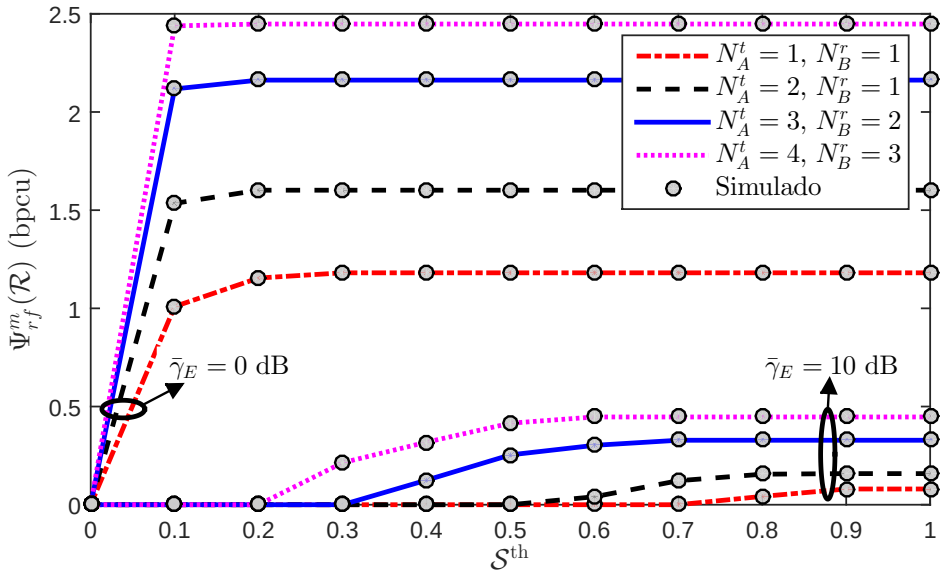


Figura 7 – $\Psi^{\mathbf{m}}_{rf}(\mathcal{R})$ em função de $\mathcal{S}^{\text{th}}$ para $N_E^r = 2$, $\gamma_B = 10$ dB, $\bar{\gamma}_E \in \{0{,}10\}$ dB e para diversos valores de N_A^t e N_B^r.
Fonte: Autoria própria.

N_A^t e N_B^r, com $\mathcal{S}^{\text{th}} = 1$ para o esquema SISOME (que significa que não existem restrições de SOP), e $\mathcal{S}^{\text{th}} = 0.2$ para o esquema MIMOME. Pode-se ver que, para $\bar{\gamma}_E = 5$, MIMOME com $N_A^t = 2$ e $N_B^r = 1$ consegue ter uma taxa próxima daquela obtida pelo esquema SISOME, mesmo tendo um limiar $\mathcal{S}^{\text{th}}$ muito mais restrito. Pode-se ver também que, com o aumento de $\bar{\gamma}_E$, deve-se aumentar N_A^t para se obter o mesmo desempenho que o esquema SISOME que trabalha sem restrições, o que é esperado uma vez que a SOP depende de C_B.

Por fim, a Figura 9 apresenta a influência de N_A^t e N_E^r no ganho $\mathsf{G}(\mathcal{R}_{\mathsf{S}}^{\star}, \mathcal{R}_{\mathsf{M}}^{\star})$. Pode-se ver que, como esperado, o ganho aumenta com o aumento da ordem de diversidade D_O. Note ainda que $N_A^t = D_O$ para $N_B^r = 1$. Para $N_E^r = 2$ e $D_O = 4$, $\mathsf{G}(\mathcal{R}_{\mathsf{S}}^{\star}, \mathcal{R}_{\mathsf{M}}^{\star}) \approx 2.1$, que está de acordo com a Figura 4. Pode-se ver que o ganho é uma função crescente de N_E^r, confirmando os resultados obtidos neste Capítulo e fazendo com que o esquema MIMOME seja menos suscetível ao aumento da capacidade do espião.

3.4 COMENTÁRIOS

Neste capítulo, baseando-se na métrica taxa efetiva de transmissão segura introduzida em (YAN et al., 2014), foi proposta uma nova métrica que limita o valor máximo da SOP permitida, sendo chamada de taxa de transmissão segura com restrições de sigilo.

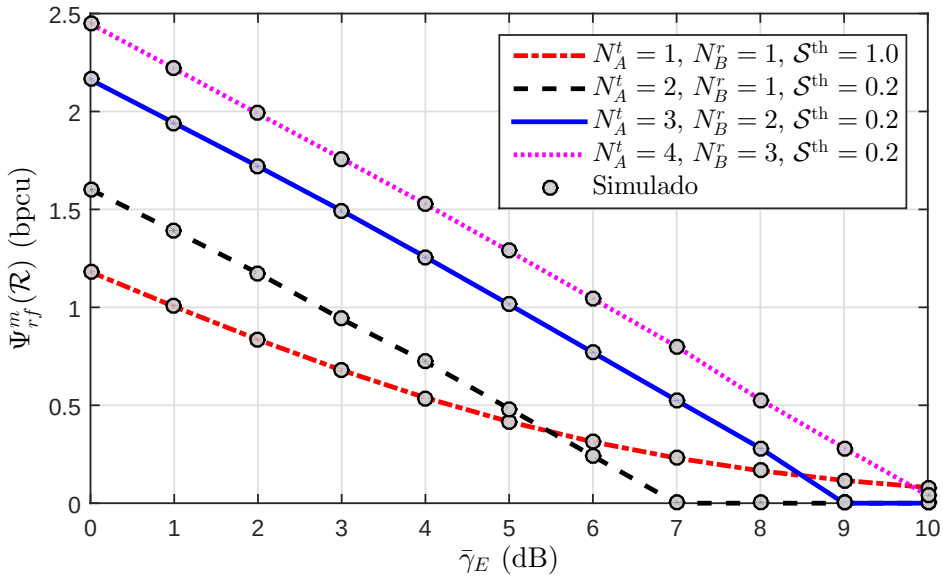


Figura 8 – $\Psi^{\mathbf{m}}_{rf}(\mathcal{R})$ em função de $\bar{\gamma}_E$ para $N_E^r = 2$, $\gamma_B = 10$ dB, $\mathcal{S}^{\text{th}} = 1$ para o esquema SISOME e $\mathcal{S}^{\text{th}} = 0.2$ para o esquema MIMOME.
Fonte: Autoria própria.

Esta nova métrica torna-se importante uma vez que, sem restrições de sigilo, Eve pode ser capaz de obter uma quantidade de informações maior que a máxima taxa tolerável pelo sistema. Além disso, o sistema adaptativo descrito em (YAN et al., 2014) foi estendido para um cenário MIMOME, onde tanto Bob quanto Alice têm múltiplas antenas. Por fim, foi apresentado o ganho do esquema MIMOME sobre o esquema SISOME, indicando que este aumenta com o aumento do número de antenas em Eve.

Foram então apresentados resultados numéricos para confirmar as análises descritas neste capítulo. Inicialmente, a taxa de transmissão segura com restrições de sigilo foi obtida para os esquemas SISOME e MIMOME demonstrando que, conforme o valor do limiar $\mathcal{S}^{\text{th}}$ diminui, a taxa de transmissão segura com restrições de sigilo máxima para o esquema SISOME diminui de maneira muito mais significativa que quando comparado com o esquema MIMOME. Foram feitas também análises demonstrando que o esquema MIMOME, além de ser capaz de obter uma taxa de transmissão segura maior, é menos suscetível ao aumento da capacidade do espião e é capaz de trabalhar com valores muito menores do limiar $\mathcal{S}^{\text{th}}$, quando considerada uma mesma taxa de sigilo que o esquema SISOME.

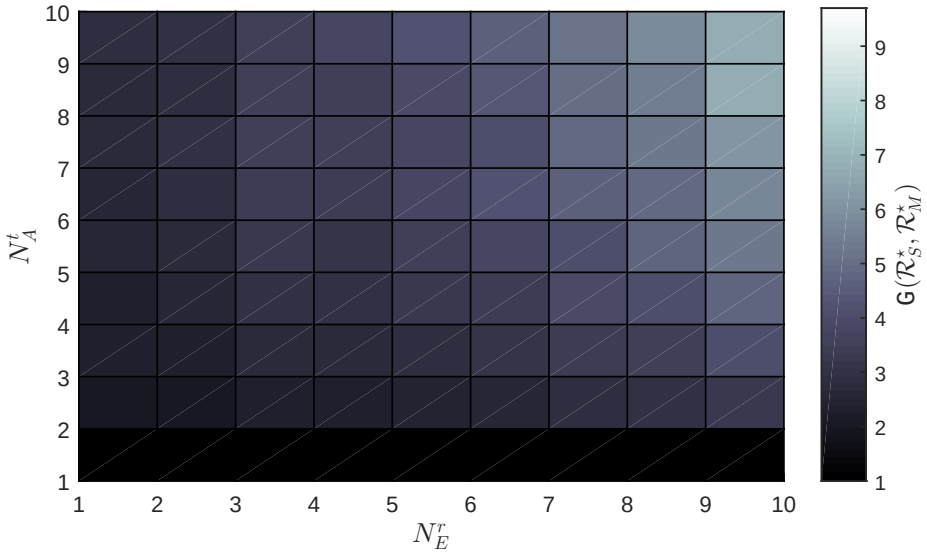


Figura 9 – Ganho do esquema MIMOME sobre o esquema SISOME em função de N_A^t e N_E^r, para $\gamma_B = 10$ dB, $\bar{\gamma}_E = 0$ dB, $N_B^r = 1$ e $\mathcal{S}^{\text{th}} = 0.75$.
Fonte: Autoria própria.

4 MÁXIMA TAXA DE TRANSMISSÃO SEGURA PARA COMUNICAÇÕES MIMOME FSO COM RESTRIÇÕES DE SIGILO

No Capítulo 3, foi apresentado como a presença de uma espião pode comprometer a comunicação em termos de sigilo para redes em RF. Para aumentar a segurança em tais redes, na Seção 3.2 foi proposta uma nova métrica de desempenho, a taxa efetiva de transmissão segura com restrições de sigilo, que foi então aplicada para tais redes. Neste capítulo, a métrica proposta será aplicada em redes de comunicação FSO considerando dois cenários. No primeiro cenário, Alice comunica-se diretamente com Bob na presença de Eve. Já no segundo cenário, múltiplos *relays* ajudam na comunicação entre Alice e Bob, e considera-se a presença de múltiplos espiões. Com base nos resultados numéricos e analíticos que serão apresentados neste capítulo, uma vez que a SNR de Eve diminui conforme Eve se distancia do alinhamento perfeito com Alice, tem-se que a EST dependerá da distância entre Bob e Eve. Além disso, será demonstrado que o uso de *relays* pode aumentar o desempenho do sistema através do aumento no número de saltos entre Alice e Bob em ambos os esquemas que serão analisados, e que apenas o esquema adaptativo com retransmissão seletiva beneficia-se com o aumento do número de caminhos.

4.1 O CANAL FSO

O interesse da comunidade científica na utilização de comunicações FSO já dura mais de três décadas. Começando na década de 60, após o surgimento do laser, a NASA realizou estudos para viabilizar a utilização de sistemas FSO na comunicação com satélites (KAZEMLOU et al., 2011). Anos depois, outra importante utilização de sistemas FSO ocorreu após os atentados ao World Trade Center, quando sistemas FSO foram utilizados para suprir problemas de comunicação causados pelo rompimento de fibras ópticas até que o cabeamento óptico pudesse ser reestabelecido (MAJUMDAR; RICKLIN, 2010).

Embora a comunicação por fibra óptica seja uma das principais tecnologias utilizadas para atender à crescente demanda por largura de banda, o processo de instalação destas fibras é lento e caro, necessitando da abertura de valas, perfurações e obtenção de direitos para a passagem da fibra. Uma possível solução é a utilização de sistemas de comunicação por RF. Porém, esta é uma solução muitas vezes cara e ineficiente uma vez que ela já é utilizada em larga escala em grandes metrópoles, causando assim possíveis interferências, tem a necessidade de obtenção de licenças de determinadas faixas de

espectro e apresenta interferência de sinal nas frequências de livre uso. Assim, a utilização da comunicação FSO é motivada pelas vantagens inerentes deste tipo de transmissão quando comparado com a comunicação por RF, como a necessidade da utilização de uma área menor para a instalação de antenas, alto ganho obtido pelos lasers e altas taxas de transmissão. Desta forma, o uso da comunicação FSO é indicado em aplicações que necessitem de altas taxas de transmissão e em ambientes onde a instalação de fibra óptica não é possível (LAMBERT; CASEY, 1995; EDELSON et al., 1996).

A base de funcionamento da comunicação FSO é a mesma da comunicação por fibra óptica, com a única diferença relacionada ao canal de comunicação que, neste caso, é a atmosfera (WILLEBRAND; GHUMAN, 2001). Para uma comunicação FSO, tem-se dois transceptores que recebem e emitem luz em comprimento de onda na faixa de 850nm a 10μm, estabelecendo assim comunicação sem fio a uma elevada taxa de transmissão entre dois nós fixos e distantes entre si, com distâncias que variam de algumas centenas de metros até vários quilômetros (VAVOULAS et al., 2012).

Entretanto, a comunicação FSO está sujeita a condições adversas causadas pela atmosfera, resultando em oscilações e perturbações na transmissão das informações através do feixe de luz. Diversos fatores podem interferir na qualidade da comunicação como, por exemplo, chuvas e nevoeiros (GRABNER; KVICERA, 2014). Dentre os principais efeitos que prejudicam a performance de sistemas FSO, tem-se:

- A atenuação atmosférica, que aumenta com a distância entre o transmissor e o receptor;
- A absorção, que está relacionada à absorção ocasionada pela interação do feixe de luz com diversas partículas e é dependente do comprimento de onda do feixe, podendo assim ser evitada ou mitigada;
- O espalhamento, que correspondente ao redirecionamento da luz;
- A atenuação geométrica, decorrente da divergência do feixe de luz transmitido;
- A turbulência devido a cintilação, que é resultado da propagação do feixe através da atmosfera e representa um dos principais problemas da comunicação FSO (NISTAZAKIS et al., 2009; AL-HABASH et al., 2001).

Estes efeitos atmosféricos aumentam com a distância entre os nós e causam grande variação na qualidade do sinal recebido (SHAULOV et al., 2005). Dos efeitos

apresentados, o mais importante é a cintilação. Para que seja possível estimar a turbulência em sistemas FSO, diversos modelos de distribuição foram desenvolvidos na literatura. Em (ANDREWS et al., 1999), o modelo log-normal é usado para representar um cenário onde a turbulência é fraca. Porém, conforme a turbulência aumenta, tem-se também um aumento no número de efeitos de espalhamento que devem ser considerados, fazendo com que o modelo log-normal não represente o canal FSO de maneira apropriada. Assim, para forte turbulência, em (JAKEMAN; PUSEY, 1976) é apresentada utilização da distribuição K, que melhor se encaixa neste cenário.

Buscando encontrar um conceito genérico e útil para diversos cenários, em (AL-HABASH et al., 2001) é apresentado um modelo utilizando a distribuição gama-gama, onde as flutuações da irradiação em larga-escala e em pequena-escala são governadas por distribuições gama individuais. Desta forma, este modelo de distribuição pode ser utilizado em cenários com turbulência variável e é, por este motivo, amplamente utilizado na literatura (AL-HABASH et al., 2001).

Com o objetivo de mitigar o efeito do canal FSO, estudos propõem a utilização de diversas técnicas como, por exemplo, MIMO e retransmissores (*relays*). Em (SAFARI; UYSAL, 2008), sistemas MIMO FSO são associados ao método RC e, em (GARCIA-ZAMBRANA et al., 2009), ao método TLS. Enquanto com RC o mesmo símbolo é transmitido por várias aberturas, utilizando TLS apenas o laser que proporciona a máxima irradiação no receptor será selecionado. Um cenário utilizando *relays* com decodifica e encaminha (DF) é demonstrado em (KARIMI; NASIRI-KENARI, 2009), onde nós vizinhos ajudam na transmissão da informação da fonte até o destino. Com objetivo de comparar a performance entre as técnicas MIMO RC, MIMO TLS e as técnicas utilizando *relays*, um estudo buscando comparar a probabilidade de *outage* foi realizado em (ABOU-RJEILY, 2015). O estudo concluiu que, nos cenários analisados, é melhor adicionar mais aberturas no receptor e no transmissor do que adicionar mais nós *relays*.

É importante notar que os sistemas FSOs podem ser utilizados para resolver diversos problemas relacionados à comunicação entre pontos distantes, mas sua viabilidade depende especificamente do cenário analisado e, para se implementar estes sistemas, devem-se levar em consideração suas vantagens, desvantagens, características e os diversos efeitos causados pelo meio atmosférico mencionados neste capítulo.

Assim como visto no Capítulo 3 para redes de comunicação sem fio em RF, as restrições de confiabilidade e de sigilo devem ser garantidas para se obter uma comunicação perfeitamente sigilosa em sistemas FSO. Como é assumido que Alice não tem o CSI

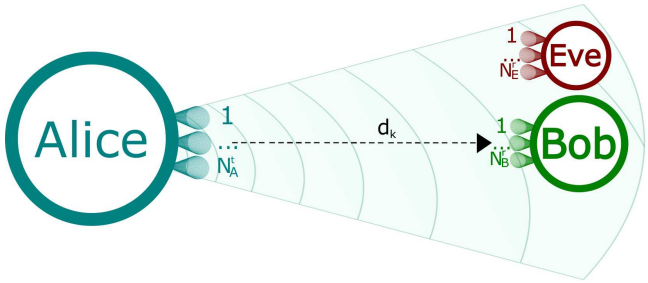


Figura 10 – Comunicação FSO ponto-a-ponto MIMOME, composta por um transmissor legítimo (Alice, com N_A^t aberturas de transmissão) e um receptor legítimo (Bob, com N_B^r aberturas de recepção), comunicando-se na presença de um espião (Eve, com N_E^r aberturas).
Fonte: Autoria própria.

instantâneo referente ao canal de Eve, a taxa de transmissão segura com restrições de sigilo, que foi proposta neste trabalho e é baseada no trabalho realizado em (YAN et al., 2014), pode ser então utilizada.

4.2 ÚNICO SALTO

4.2.1 Modelo do Sistema

O modelo adotado neste Capítulo quando considerado um único salto é composto por um transmissor legítimo, Alice (A), comunicando-se com um receptor legítimo, Bob (B), na presença de um espião, Eve (E). Alice está equipada com N_A^t aberturas de transmissão trabalhando sob esquema TLS, enquanto Bob e Eve são fornecidos, respectivamente, N_B^r e N_E^r aberturas de recepção, usando o esquema MRC. Este cenário MIMOME está ilustrado na Figura 10.

Seguindo (FRIED, 1967; BELMONTE; KAHN, 2008; AGHAJANZADEH; UYSAL, 2010), foi utilizada neste trabalho a detecção coerente que, apesar de ser mais complexa do que a detecção direta, oferece flexibilidade já que a amplitude, frequência ou fase podem ser usadas na modulação. Em tais sistemas, ainda que a capacidade inicialmente aumente com o aumento do diâmetro da abertura do receptor, este aumento tende a saturar, justificando o uso de múltiplas aberturas no receptor (KAUR et al., 2014). Foi também considerado que a irradiância recebida nas aberturas em Bob e Eve são independentes, ou seja, os efeitos em larga escala e em pequena escala experimentados por Bob são independentes daquela vista em Eve, que se mantém em um cenário onde a distância entre Bob e Eve é maior do que o comprimento de correlação

$d_0 \approx \sqrt{\lambda d_k}$ (NAVIDPOUR et al., 2007), onde λ é o comprimento da onda (ABOU-RJEILY, 2015). Nas comunicações em FSO através de uma atmosfera turbulenta, a taxa máxima alcançável por unidade de largura de banda é dada por $\log_2(1+\gamma)$ bits/s/Hz, conforme apresentado no Capítulo 2, onde γ é considerada aleatória devido à natureza do canal (BELMONTE; KAHN, 2009). Se o ruído é dominado pelo ruído do oscilador local, a SNR em Bob e Eve pode ser expressa como

$$\gamma_{m,n} = \frac{r_{m,n} A_0 \eta_e E_s \mathcal{Z}_{m,n} A}{h\ f_o\ \Delta_f} I_{m,n}, \tag{29}$$

onde η_e é a eficiência quântica do fotodetector, E_s é a energia do símbolo, A é a área do feixe, h indica a constante de Planck, f_o indica a frequência do sinal óptico recebido, Δ_f é a largura de banda equivalente do ruído, $A_0 = \mathrm{erf}^2(\sqrt{\pi 2}\rho/\omega_b)$ representa a fração da energia disponível no receptor para o fotodetector quando não há desalinhamento entre o transmissor e o receptor, $\mathrm{erf}(\cdot)$ é a função erro, ρ é o raio da abertura de recebimento, ω_b é o tamanho do feixe recebido, $r_{m,n}$ representa a fração da potência disponível alocada para o nó de transmissão do salto n no caminho m, $\mathcal{Z}_{m,n} = \exp(-\sigma_l\ d_{m,n})$ é a atenuação associada à perda de percurso utilizada para cenários com *relays*, $d_{m,n}$ é a distância para cada salto, $\sigma_l \approx 0.1$ é o coeficiente de atenuação para uma atenuação de 0.44 dB/km. Observe que, para a transmissão direta, $m = 1$, $n = 1$, $r_{m,n} = 1$ e $\mathcal{Z}_{m,n} = 1$, enquanto que, para a transmissão utilizando *relays*, a fração da potência é dividida entre todos os nós transmissores legítimos e a perda de percurso é considerada para que as comparações sejam justas. Finalmente, $I_{m,n}$ representa a irradiância associada a um único salto. Para uma dada i-ésima abertura de transmissão do nó transmissor e j-ésima abertura de recepção do nó receptor, $I^{i,j}_{m,n} = I^{i,j}_{a,m,n}\ I^{i,j}_{p,m,n}$, onde $I^{i,j}_{a,m,n}$ é o desvanecimento causado por turbulência atmosférica e $I^{i,j}_{p,m,n}$ é o erro de alinhamento. Para cada canal, os efeitos em larga escala estão totalmente correlacionados entre as aberturas de recepção (PRIYADARSHANI et al., 2017). É assumido ainda que $I^{i,j}_{p,m,n} = 1$ para o canal legítimo, que pode ser obtido na prática por meio de um alinhamento perfeito (SANDALIDIS et al., 2009). No entanto, isso não é válido para a Eve, que está sujeita a erros de alinhamento. Também é assumido que as aberturas de recepção de Eve estão próximas o suficiente de modo que todas elas sejam afetadas pelo mesmo erro de alinhamento. Assim, para o modelo MIMOME sem *Relays*, $I_{m,n}$ pode ser escrito como (NIU et al., 2013, 2012; GARCIA-ZAMBRANA et al.,

2009; ABOU-RJEILY, 2011)

$$I_{m,n} = \begin{cases} I_{p,m,n} \sum_{j=1}^{N_E^r} I_{a,m,n}^{i,j}, & \text{Eve;} \\ \max_{i=1,\ldots,N_A^t} \sum_{j=1}^{N_B^r} I_{a,m,n}^{i,j}. & \text{Bob-TLS.} \end{cases} \tag{30}$$

É importante notar que, embora o espião possa ser capaz de acessar o canal de *feedback* de Bob para Alice, a abertura selecionada é otimizada para o canal legítimo somente, de modo que o índice da abertura utilizada não pode ser explorado pelo espião (ALVES et al., 2012). Esse comportamento é representado pelo termo $\max_{i=1,\ldots,N_A^t}$ na equação (30). Seguindo (TSIFTSIS, 2008; ABOU-RJEILY, 2015; KHALIGHI et al., 2009; AL-HABASH et al., 2001), é adotado o modelo de desvanecimento gama-gama para representar a turbulência induzida pela cintilação, na qual a função densidade de probabilidade (pdf, do inglês *probability density function*) da turbulência $f_{m,n}^{\gamma\gamma}(\cdot)$ em um único link para $(I \geq 0)$ é dada por

$$f_{m,n}^{\gamma\gamma}(I, \alpha_p, \beta_p) = \frac{2(\alpha\beta)^{(\alpha+\beta)/2}}{\Gamma(\alpha)\Gamma(\beta)} I^{(\alpha+\beta)/2-1} K_{\alpha-\beta}(2\sqrt{\alpha\beta I}), \tag{31}$$

onde $K_c(\cdot)$ é a função Bessel modificada do segundo tipo e ordem c. A função de distribuição cumulativa (cdf, do inglês *cumulative distribution function*) da equação (31) $F_{m,n}^{\gamma\gamma}(\cdot)$ é dada por

$$\begin{aligned} F_{m,n}^{\gamma\gamma}(\mathcal{X}, \alpha_p, \beta_p) &= \frac{\pi}{\Gamma(\alpha)\Gamma(\beta)\sin(\pi(\alpha-\beta))} \\ &\left[\frac{(\mathcal{X}\alpha\beta)^{\beta}\, {}_1F_2(\beta; \beta+1, -\alpha+\beta+1; \alpha\beta\mathcal{X})}{\beta\Gamma(-\alpha+\beta+1)} - \frac{(\mathcal{X}\alpha\beta)^{\alpha}\, {}_1F_2(\alpha; \alpha+1, \alpha-\beta+1; \alpha\beta\mathcal{X})}{\alpha\Gamma(\alpha-\beta+1)}\right], \end{aligned} \tag{32}$$

onde ${}_1F_2(\cdot)$ indica a função hipergeométrica generalizada, $\alpha = \alpha_f(d_{m,n})\alpha_p$ e $\beta = \beta_f(d_{m,n})\beta_p$ representam, respectivamente, os parâmetros de larga escala e de pequena escala relacionados ao número de células no processo de dispersão, e α_p e β_p são parâmetros de ajuste relacionados ao número de aberturas de transmissão e recepção. As funções $\alpha_f(\cdot)$ e $\beta_f(\cdot)$ são dadas por (ABOU-RJEILY, 2015)

$$\alpha_f(d_p) = \left[\exp\left(\frac{0.49\sigma_R^2(d_p)}{(1+1.11\sigma_R^{12/5}(d_p))^{7/6}}\right) - 1\right]^{-1}, \tag{33a}$$

$$\beta_f(d_p) = \left[\exp\left(\frac{0.51\sigma_R^2(d_p)}{(1+0.69\sigma_R^{12/5}(d_p))^{5/6}}\right) - 1\right]^{-1}, \tag{33b}$$

onde $\sigma_R^2(d_p)$= $1.23C_n^2\nu^{7/6}d_{m,n}^{11/6}$ é a variância Rytov, ν é o número de onda e C_n^2= 1.7×10^{-14} $\mathrm{m}^{-2/3}$ indica o índice de refração da estrutura, que é usado para caracterizar a turbulência atmosférica. De (FARID; HRANILOVIC, 2007), o erro de alinhamento é dada por $I_{p,m,n} = \exp(-\frac{2\tau^2}{\omega_e^2})$, com o largura de feixe equivalente dada por $\omega_e = (\sqrt{\pi}\omega_b^2\mathrm{erf}(\nu)/(2\nu\exp\left(-\nu^2\right)))^{1/2}$ e o deslocamento radial no receptor dado por τ. Considerando que o deslocamento de Eve segue uma distribuição gaussiana independente e idêntica com desvio padrão σ_s para o eixo vertical e horizontal, a pdf da variável aleatória que representa os erros de alinhamento $f_{m,n}^p(\cdot)$ pode então ser expressa como (SANDALIDIS et al., 2009)

$$f_{m,n}^p(I_{p,m,n}) = \xi^2 I_{p,m,n}^{\xi^2-1}, \tag{34}$$

onde $\xi = \omega_e/(2\sigma_s)$. Além disso, a SNR da equação (29) pode ser reescrita como

$$\gamma_{m,n} = z_{m,n}A_0 r_{m,n}\gamma_0 I_{m,n} = \frac{z_{m,n}A_0 r_{m,n} I_{m,n}}{N_0}, \tag{35}$$

onde γ_0= $\frac{1}{N_0} = \frac{\eta_e E_s A}{h f_o \Delta_f}$ é a SNR livre de turbulência que não leva em conta a perda de percurso, a irradiância $I_{m,n}$, a fração da potência disponível $r_{m,n}$ (alocada para o nó de transmissão) e a fração A_0. Uma vez que o laser emitido por Alice sofre divergência devido a difração óptica, seguindo a abordagem descrita em (LOPEZ-MARTINEZ et al., 2015), é assumido que Eve está localizada na região de divergência, o que implica que Eve está perto de Bob (ANDREWS et al., 1999) e é capaz de obter parte do laser não capturado por Bob, como mostrado na Figura 10. Em tal abordagem, a comunicação é intrinsecamente segura para pequenos ângulos de divergência, mas, para longas distâncias, Eve tem uma melhor chance de capturar as mensagens transmitidas.

De (GAPPMAIR, 2011), tem-se que, em um cenário em que os erros de alinhamento e a turbulência atmosférica são considerados, ou seja, $I_{m,n}^{i,j} = I_{a,m,n}^{i,j}\, I_{p,m,n}^{i,j}$, a pdf da irradiância $f_{m,n}^{\gamma\gamma p}(\cdot)$ é então dada por

$$f_{m,n}^{\gamma\gamma p}(I,\alpha_p,\beta_p) = \frac{\left(\alpha\beta\xi^2\right) G_{1,3}^{3,0}\left((\alpha\beta)I \middle| \begin{matrix}\xi^2\\ \xi^2-1,\alpha-1,\beta-1\end{matrix}\right)}{\Gamma(\alpha)\Gamma(\beta)}, \tag{36}$$

onde $G_{\cdot,\cdot}^{\cdot,\cdot}(\cdot)$ é a função Meijer-G. A cdf da irradiância $F_{m,n}^{\gamma\gamma p}(\cdot)$ em (36) é dada por

$$\begin{aligned} F_{m,n}^{\gamma\gamma p}(\mathcal{X},\alpha_p,\beta_p) = \frac{\pi}{\Gamma(\alpha)\Gamma(\beta)}\Bigg(& -\csc(\pi(\alpha-\beta)) \\ & \sum_{u=1}^{2}\sum_{v=1}^{2} c_u c_v \mathcal{X}^{b_u}(\alpha\beta)^{b_u}\Big(\Gamma(a_v)\,{}_1\tilde{F}_2(a_v;d_v,e_v;\mathcal{X}\alpha\beta)\Big) \\ & +\frac{\pi\mathcal{X}^{\xi^2}(\alpha\beta)^{\xi^2}\csc\Big(\pi\Big(\alpha-\xi^2\Big)\Big)\csc\Big(\pi\Big(\beta-\xi^2\Big)\Big)}{\Gamma(\xi^2-\alpha+1)\Gamma(\xi^2-\beta+1)}\Bigg), \end{aligned} \tag{37}$$

onde ${}_1\tilde{F}_2(\cdot)$ indica a função hipergeométrica regularizada e a_x, $x \in \{u,v\}$ representa o x-ésimo elemento do vetor $\boldsymbol{a} = \left[b_u, b_u - \xi^2\right]$, que também é válido para os vetores $\boldsymbol{b} = [\alpha,\beta]$, $\boldsymbol{c} = [-1,1]$, $\boldsymbol{d} = [b_u+1, (\beta-\alpha)c_u+1]$ e $\boldsymbol{e} = \left[(\beta-\alpha)c_u+1, b_u-\xi^2+1\right]$. Finalmente, é assumido que a distorção de fase é insignificante, o que pode ser alcançado na prática através do uso de técnicas de compensação modal como, por exemplo, polinômios de Zernike (NOLL, 1976).

4.2.2 Taxa Efetiva de Transmissão Segura com Restrições de Sigilo

A taxa efetiva de transmissão segura com restrições de sigilo representada em (20) no Capítulo 3 pode ser reescrita como

$$\Psi_{fso}^{\mathsf{m}}(\mathcal{R}_E,\mathcal{R}_B) = \begin{cases} \Psi_{fso}(\mathcal{R}_E,\mathcal{R}_B), & \text{se } \mathcal{S}_{fso}(\mathcal{R}_E) \le \mathcal{S}^{\text{th}}; \\ 0, & \text{se } \mathcal{S}_{fso}(\mathcal{R}_E) > \mathcal{S}^{\text{th}}. \end{cases} \tag{38}$$

4.2.3 Esquema Adaptativo

Como Alice possui o CSI instantâneo do canal legítimo, a restrição de confiabilidade é sempre garantida no esquema adaptativo. De (10), a EST para o esquema adaptativo em transmissões FSO pode então ser reescrita como

$$\Psi_{fso}^{a}(\mathcal{R}_E) = (C_B - \mathcal{R}_E)\left[1 - \mathcal{S}_{fso}(\mathcal{R}_E)\right]. \tag{39}$$

Obter uma expressão em forma fechada para a EST em (39) requer avaliar o SOP que, para comunicações FSO com um único salto, é dada como

$$\begin{aligned} \mathcal{S}_{fso}(\mathcal{R}_E) &= \Pr\{C_E > \mathcal{R}_E\} = \Pr\left\{\gamma_E > 2^{\mathcal{R}_E} - 1\right\} \\ &= \Pr\left\{\frac{I_{m,n}A_0}{N_0} > 2^{\mathcal{R}_E} - 1\right\}. \end{aligned} \tag{40}$$

Lema 2. *A SOP do esquema adaptativo*[1] *é dada por*

$$\mathcal{S}_{fso}(\mathcal{R}_E) = 1 - F^{\gamma\gamma p}_{m,n}(\mathcal{X}_E^{fso}, 1, N_E^r), \tag{41}$$

onde $\mathcal{X}_E^{fso} = \frac{N_0\left(2^{\mathcal{R}_E}-1\right)}{N_E^r A_0}$.

Demonstração. Para obter (41), primeiro recorre-se ao fato de que a probabilidade de (40) pode ser reescrita como

$$\mathcal{S}_{fso}(\mathcal{R}_E) = \Pr\left\{ Z\sum_{g=1}^{N_E^r} X_g Y_g > \frac{N_0\left(2^{\mathcal{R}_E}-1\right)}{A_0} \right\}, \tag{42}$$

onde $X, Y \sim \Gamma(\cdot)$ são, respectivamente, os parâmetros em larga escala e em pequena escala da variável aleatória gama-gama, ambas com distribuição gama com o parâmetro de forma κ inversamente proporcional ao parâmetro de escala θ, ou seja, $\theta = \frac{1}{\kappa}$, e Z representa a variável aleatória devido ao erro de alinhamento, no qual a pdf é dada pela equação (34). Devido à proximidade espacial das aberturas e à natureza inerente LOS dos sistemas FSO, os efeitos em larga escala podem ser assumidos iguais em todas as aberturas de recebimento (GARRIDO-BALSELLS et al., 2014), de modo que (42) pode ser reescrita como

$$\mathcal{S}_{fso}(\mathcal{R}_E) = \Pr\left\{ ZX\sum_{g=1}^{N_E^r} Y_g > \frac{N_0\left(2^{\mathcal{R}_E}-1\right)}{A_0} \right\}. \tag{43}$$

Usando a propriedade de soma das variáveis gama, onde o somatório de uma variável com forma κ e escala θ pode ser expressa como uma única variável gama em que o parâmetro de forma é a soma de todos os parâmetros de forma (MOSCHOPOULOS, 1985), isto é, $\sum_{g=1}^{N_E^r} X_g \sim \Gamma\left(\sum_{g=1}^{N_E^r}\kappa_g, \theta\right)$, (43) pode ser reescrito como

$$\mathcal{S}_{fso}(\mathcal{R}_E) = \Pr\left\{ ZX_\alpha \frac{1}{N_E^r} Y_\beta > \frac{N_0\left(2^{\mathcal{R}_E}-1\right)}{N_E^r A_0} \right\}, \tag{44}$$

onde $X_\alpha \sim \Gamma\left(\alpha, \frac{1}{\alpha}\right)$ e $Y_\beta \sim \Gamma\left(N_E^r\beta, \frac{1}{\beta}\right)$. Para obter $\theta = \frac{1}{\kappa}$ como proposto em (AL-HABASH et al., 2001) e usado em (31), recorre-se à propriedade da escala, onde o produto de uma variável gama e uma constante pode ser reescrito como uma variável gama, onde o parâmetro de escala θ é o produto da escala original pela constante, isto é, $cX \sim \Gamma(\kappa, c\theta)$

[1] A SOP apresentada no Lema 2 também é válida para o esquema de taxa fixa, já que apenas a SNR média da canal malicioso é assumida como conhecida por Alice em ambos os esquemas.

e, portanto,

$$\mathcal{S}_{fso}(\mathcal{R}_E) = \Pr\left\{ ZX_\alpha Y_{\beta_E} > \frac{N_0\left(2^{\mathcal{R}_E}-1\right)}{N_E^r A_0} \right\}, \tag{45}$$

onde $Y_{\beta_E} \sim \Gamma\left(N_E^r\beta, \frac{1}{N_E^r\beta}\right)$. A pdf de $ZX_\alpha Y_{\beta_E}$ é dada pela equação (36), de forma que a cdf correspondente pode ser obtida como

$$F_{m,n}^{\gamma\gamma p}(\mathcal{X}, \alpha_p, \beta_p) = \int_0^x f_{m,n}^{\gamma\gamma p}(I, \alpha_p, \beta_p) dI, \tag{46}$$

o que resulta em (37) e pode ser usada diretamente para obter (41), concluindo a prova. □

A EST é então obtido substituindo (41) em (39).

4.2.3.1 Taxa Alvo Ótima De Redundância

Ao avaliar a EST de (39), pode-se ver que enquanto um $\mathcal{R}_E$ maior leva a um valor menor de $(C_B - \mathcal{R}_E)$, simultaneamente aumenta-se $1 - \Pr\{C_E > \mathcal{R}_E\}$. Assim, pode-se esperar que exista um valor ótimo de $\mathcal{R}_E$ que maximize a EST. No entanto, ao considerar um cenário com restrições de sigilo, é necessário verificar se esse valor ótimo atende a restrição ou não. Nesse sentido, tem-se o seguinte resultado.

Teorema 2. *O valor de $\mathcal{R}_E$ que maximiza a EST com restrições de sigilo para o esquema adaptativo MIMOME FSO é dado por*

$$\mathcal{R}_E^{a^\star} = \max\left(\mathcal{R}_{E,u}^{a^\star}, \mathcal{R}_E^{th^\star}\right), \tag{47}$$

onde $\mathcal{R}_{E,u}^{a^\star}$ é o valor ótimo sem restrições em $\mathcal{R}_E$, que é dado pela equação de ponto fixo

$$\begin{aligned}\mathcal{R}_{E,u}^{a^\star} = {} & (C_B - C_B 2^{R_{E,u}^{a^*}} + 2^{R_{E,u}^{a^*}} R_{E,u}^{a^*}) + \frac{4\sigma_s^2\left(2^{R_{E,u}^{a^*}}-1\right)^2}{\log(2)\omega_E^2 2^{R_{E,u}^{a^*}}} + \frac{A_0 N_E^r \theta_E^{AP}}{N_0 \log(2)\omega_E^2 2^{R_{E,u}^{a^*}} E_{\vartheta-1}\left(\frac{\chi_E^{fso}}{\theta_E^{AP}}\right)} \\ & \left(\frac{\left\{2^{R_{E,u}^{a^*}}\left[\log(2)\omega_E^2\left(C_B - R_{E,u}^{a^*}\right) - 4\sigma_s^2\right] + 4\sigma_s^2\right\}}{\exp\left(\frac{\chi_E^{fso}}{\theta_E^{AP}}\right)} \right. \\ & \left. - \frac{\left(\frac{\chi_E^{fso}}{\theta_E^{AP}}\right)^{-\kappa}\left(\omega_E^2 - 4\kappa_E^{AP}\sigma_s^2\right)\left[\Gamma\left(\kappa_E^{AP}\right) - \Gamma\left(\kappa_E^{AP}, \frac{\chi_E^{fso}}{\theta_E^{AP}}\right)\right]}{\left(2^{R_{E,u}^{a^*}}-1\right)^{-1}} \right),\end{aligned} \tag{48}$$

e $\mathcal{R}_E^{th^\star}$ *é o valor ótimo restringido de* $\mathcal{R}_E$ *para um dado máximo valor permitido de* S^{th}*, que é dado por*

$$\mathcal{R}_E^{th^\star} = \log_2\left(1 + \frac{A_0 N_E^r \theta_E^{AP}}{N_0}\left(\frac{\Gamma\left(\kappa_E^{AP}, \frac{x_E^{fso}}{\theta_E^{AP}}\right) - S^{th}\Gamma\left(\kappa_E^{AP}\right)}{E_\vartheta\left(\frac{x_E^{fso}}{\theta_E^{AP}}\right)}\right)^{\frac{1}{\kappa_E^{AP}}}\right). \tag{49}$$

Em (48) *e* (49), $E.(\cdot)$ *é a função integral exponencial,* $\vartheta = -\kappa_E^{AP} + \frac{\omega_E^2}{4\sigma_s^2} + 1$*, enquanto* θ_k^{AP} *e* κ_k^{AP} *são os parâmetros de escala e forma da variável gama aproximada, que são respectivamente dados como*

$$\kappa_k^{AP} = \left[\tfrac{(\beta+1)(\alpha+1)}{\beta\alpha} - (1+\epsilon)\right]^{-1}, \tag{50a}$$

$$\theta_k^{AP} = \left[\tfrac{(\beta+1)(\alpha+1)}{\beta\alpha} - (1+\epsilon)\right]\Omega, \tag{50b}$$

onde ϵ *e* Ω *são os parâmetros de ajuste (AL-AHMADI; YANIKOMEROGLU, 2009).*

Demonstração. Para se obter (47), primeiro recorre-se ao fato de que, de acordo com (AL-AHMADI; YANIKOMEROGLU, 2009), uma variável aleatória gama-gama pode ser aproximada por uma variável gama X_k^{AP} com os parâmetros de forma κ_k^{AP} e escala θ_k^{AP} dados, respectivamente, por (50a) e (50b). Assim, (45) pode ser aproximado como

$$\begin{aligned}\mathcal{S}_{fso}(\mathcal{R}_E) &\approx \Pr\left\{ZX_E^{\mathrm{AP}} > \frac{N_0\left(2^{\mathcal{R}_E}-1\right)}{N_E^r A_0}\right\}\\ &\approx 1 - F_{m,n,AP}^{\gamma\gamma p}\left(\frac{N_0\left(2^{\mathcal{R}_E}-1\right)}{N_E^r A_0}, 1, N_E^r\right),\end{aligned} \tag{51}$$

onde $F_{m,n,AP}^{\gamma\gamma p}(\cdot)$ pode ser facilmente obtido como

$$F_{m,n,AP}^{\gamma\gamma p}(x,\alpha_p,\beta_p) = \frac{\left(\frac{x}{\theta_E^{\mathrm{AP}}}\right)^{\kappa_E^{\mathrm{AP}}} E_{-\kappa_E^{\mathrm{AP}}+\frac{\omega_e^2}{4\sigma_s^2}+1}\left(\frac{x}{\theta_E^{\mathrm{AP}}}\right) - \Gamma\left(\kappa_E^{\mathrm{AP}}, \frac{x}{\theta_E^{\mathrm{AP}}}\right) + \Gamma\left(\kappa_E^{\mathrm{AP}}\right)}{\Gamma\left(\kappa_E^{\mathrm{AP}}\right)}. \tag{52}$$

Utilizando $\partial\Psi_{fso}^a(\mathcal{R}_E)/\partial\mathcal{R}_E = 0$ e resolvendo para $\mathcal{R}_E$, obtém-se o ponto estacionário de $\Psi_{fso}^a(\mathcal{R}_E)$, que é dado por (48). Tem-se que, de forma semelhante ao que foi apresentado em (YAN et al., 2015), uma análise da identificação de pontos estacionários via (48) e $\partial^2\Psi_{fso}^a(\mathcal{R}_E)/\partial\mathcal{R}_E^2$ não é tratável. Observando que a probabilidade de (51) é uma função monotônica decrescente de $\mathcal{R}_E$ (para $\mathcal{R}_E < C_B$) e seguindo uma abordagem similar ao que foi apresentado em (YAN et al., 2015), tem-se que (39) é côncava ou semi-côncava

com apenas um ponto estacionário para todas as situações testadas. Isso está de acordo com o comportamento de diminuição monotônica de (51). Assim, tem-se que os pontos estacionários dados por (48) sempre identificam o máximo local nas simulações.

Recorrendo ao fato de que $\mathcal{S}_{fso}(\mathcal{R}_E)$ é uma função monotônica decrescente de $\mathcal{R}_E$, pode-se ver que a taxa de redundância no limiar $\mathcal{S}^{\text{th}}$ é a taxa de redundância mínima permitida. Usando a equação (51), pode-se encontrar a função inversa em relação a $\mathcal{S}^{\text{th}}$, que é dada por (49). Observando que $\Psi^{a}_{fso}(\mathcal{R}_E)$ aumenta para $\mathcal{R}_E < \mathcal{R}^{a^\star}_{E,u}$ e diminui para $\mathcal{R}_E > \mathcal{R}^{a^\star}_{E,u}$, tem-se que, sem restrições, $\mathcal{R}^{a^\star}_{E,u}$ representa a taxa de redundância máxima, no sentido de que qualquer valor diferente de $\mathcal{R}^{a^\star}_{E,u}$ resultará em um valor menor de $\Psi^{a}_{fso}(\mathcal{R}_E)$. Observando que $\mathcal{R}^{a^\star}_{E}$ não pode ser menor do que (49) (devido à restrição de SOP), pode-se concluir que $\mathcal{R}^{a^\star}_{E,u}$ é o valor máximo entre (48) e (49), que é dado por (47). □

4.2.4 Esquema Com Taxa Fixa

No esquema de taxa fixa para comunicações em FSO, a EST apresentada em (9) pode ser reescrita como

$$\Psi^{\mathsf{f}}_{fso}(\mathcal{R}_E, \mathcal{R}_B) = (\mathcal{R}_B - \mathcal{R}_E)\left[1 - \mathcal{O}^{f}_{fso}(\mathcal{R}_B)\right]\left[1 - \mathcal{S}_{fso}(\mathcal{R}_E)\right], \tag{53}$$

onde $\mathcal{O}^{f}(\cdot)$ é a probabilidade de *outage* em termos de confiabilidade para o esquema de taxa fixa.

O SOP em (53) é obtida de (41). A probabilidade de confiabilidade, por sua vez, é dada como

$$\begin{aligned} 1 - \mathcal{O}^{f}_{fso}(\mathcal{R}_B) &= \Pr\{C_B \geq \mathcal{R}_B\} \\ &= \Pr\{\gamma_B > 2^{\mathcal{R}_B} - 1\} \\ &= \Pr\left\{\frac{I_{m,n}A_0}{N_0} > 2^{\mathcal{R}_B} - 1\right\}. \end{aligned} \tag{54}$$

Percebendo que a turbulência $I_{m,n}$ em (54) engloba os efeitos das técnicas TLS e MRC, tem-se que (54) é dado da seguinte maneira.

Lema 3. *A probabilidade de outage em termos de confiabilidade para o esquema de taxa fixa é dada por*

$$\mathcal{O}^{f}_{fso}(\mathcal{R}_B) = F^{\gamma\gamma}_{m,n}(\mathcal{X}^{fso}_B, 1, N^r_B)^{N^t_A}, \tag{55}$$

onde $\mathcal{X}^{fso}_B = \frac{N_0(2^{\mathcal{R}_B}-1)}{N^r_B A_0}$ *e* $F^{\gamma\gamma}_{m,n}(\cdot)$ *representa a cdf de uma única variável aleatória gama-gama para a SNR em Bob, e é dada por* (32).

Demonstração. Para obter (55), a mesma abordagem utilizada no Lema 2 foi adotada, com a diferença de que (55) não leva em consideração os erros de alinhamento, e apresenta o efeito do TLS, uma vez que (55) é relacionada ao canal legítimo. □

A EST do esquema de taxa fixa é finalmente obtida após a substituição de (41) e (55) em (53).

4.2.4.1 Taxa Alvo Ótima De Redundância

Diferente do esquema adaptativo, no esquema de taxa fixa a EST é uma função de $\mathcal{R}_E$ e $\mathcal{R}_B$. Assim, para obter os valores ótimos de tais parâmetros (ou seja, $\mathcal{R}_E^{f^\star}$ e $\mathcal{R}_B^{f^\star}$), primeiro é preciso identificar os valores ótimos de $\mathcal{R}_E$ e $\mathcal{R}_B$ sem restrições de sigilo, o que é apresentado no que se segue.

Lema 4. *Os valores ótimos sem restrições de $\mathcal{R}_E$ e $\mathcal{R}_B$ que alcançam em conjunto um EST máximo localmente são fornecidos, respectivamente, por*

$$\mathcal{R}_{E,u}^{f^\star} = \mathcal{R}_{B,u}^{f^\star} + \frac{1}{\log(2)N_A^t}\left[\left(1-2^{-\mathcal{R}_B}\right)e^{\frac{x_B^{fso}}{\theta_B^{AP}}}\Gamma\left(\kappa_B^{AP}\right)\left(\frac{x_B^{fso}}{\theta_B^{AP}}\right)^{-\kappa_B^{AP}}\left(C_1 - {C_1}^{1-N_A^t}\right)\right], \tag{56a}$$

$$\mathcal{R}_{B,u}^{f^\star} = \mathcal{R}_{E,u}^{f^\star} + \frac{\left(-1+2^{R_{E,u}^{f*}}\right)}{2^{R_{E,u}^{f*}}\omega_e^2\log(2)}\left(\frac{4\sigma_s^2}{2^{-R_{E,u}^{f*}}\omega_e^2\log(2)} + \frac{\left(\frac{X_{\mathcal{R}_E}}{\theta_E^{AP}}\right)^{-\kappa_E^{AP}}\left(\omega_e^2 - 4\kappa_E^{AP}\sigma_s^2\right)\left[\Gamma\left(\kappa_E^{AP}\right) - \Gamma\left(\kappa_E^{AP}, \frac{X_{\mathcal{R}_E}}{\theta_E^{AP}}\right)\right]}{-\frac{\left(-1+2^{R_{E,u}^{f*}}\right)E_{\vartheta-1}\left(\frac{X_{\mathcal{R}_E}}{\theta_E^{AP}}\right)N_0}{\theta_E^{AP}A_0N_E^r} + \exp\left(-\frac{X_{\mathcal{R}_E}}{\theta_E^{AP}}\right)}\right), \tag{56b}$$

onde $C_1 = Q\left(\kappa_B^{AP}, 0, \frac{x_B^{fso}}{\theta_B^{AP}}\right)$, *sendo* $Q(\cdot,0,\cdot)$ *a função gama incompleta regularizada generalizada.*

Demonstração. Usando (53), os valores de $(\mathcal{R}_E, \mathcal{R}_B)$ que maximizam conjuntamente a EST para o esquema de taxa fixa podem ser escritos como

$$(\mathcal{R}_E^{f^\star}, \mathcal{R}_B^{f^\star}) = \underset{\substack{0<\mathcal{R}_B \\ 0<\mathcal{R}_E<\mathcal{R}_B}}{\arg\max}\ \Psi_{fso}^f(\mathcal{R}_E, \mathcal{R}_B). \tag{57}$$

Substituindo (41) e (55) em (53) e usando a aproximação de uma variável gama-

gama por uma variável gama, (53) pode ser aproximada como

$$\Psi_{fso}^{f}(\mathcal{R}_E,\mathcal{R}_B) \approx (\mathcal{R}_B-\mathcal{R}_E)\left[1-Q\left(\kappa_B^{\mathrm{AP}},0,\frac{\mathcal{X}_B^{fso}}{\theta_B^{\mathrm{AP}}}\right)\right] F_{m,n,AP}^{\gamma\gamma p}\left(\mathcal{X}_E^{fso}\right), \tag{58}$$

e, definindo a derivada parcial de primeira ordem de (58) com respeito a $\mathcal{R}_B$ para zero, tem-se que

$$0 = C_2\left(1-C_1^{N_A^t}\right) - \frac{C_2 N_0 2^{\mathcal{R}_B}\log(2) N_A^t \mathcal{R}\, e^{-\frac{\mathcal{X}_B^{fso}}{\theta_B^{\mathrm{AP}}}}\left(\frac{\mathcal{X}_B^{fso}}{\theta_B^{\mathrm{AP}}}\right)^{\kappa_B^{\mathrm{AP}}-1} C_1^{N_A^t-1}}{\theta_B^{\mathrm{AP}} N_b A_0 \Gamma\left(\kappa_B^{\mathrm{AP}}\right)}, \tag{59}$$

onde $C_2 = Q\left(\kappa_E^{\mathrm{AP}},0,\frac{\mathcal{X}_E^{fso}}{\theta_E^{\mathrm{AP}}}\right)$ e $\mathcal{R} = \mathcal{R}_B - \mathcal{R}_E$. Resolvendo (59) para $\mathcal{R}_E$, obtém-se (56a). Definindo a derivada parcial de primeira ordem de (58) com respeito a $\mathcal{R}_E$ para zero e resolvendo para $\mathcal{R}_B$, obtém-se (56b).

Com base no teorema de Young (YOUNG, 1984) e de forma semelhante ao usado em (YAN et al., 2015), a matriz Hessiana de (58) é simétrica e pode ser expressa como

$$\mathrm{Hess} = \begin{bmatrix} \frac{\partial^2 \Psi_{fso}^{f}(\mathcal{R}_E,\mathcal{R}_B)}{\partial \mathcal{R}_B^2} & \frac{\partial^2 \Psi_{fso}^{f}(\mathcal{R}_E,\mathcal{R}_B)}{\partial \mathcal{R}_B \partial \mathcal{R}_E} \\ \frac{\partial^2 \Psi_{fso}^{f}(\mathcal{R}_E,\mathcal{R}_B)}{\partial \mathcal{R}_E \partial \mathcal{R}_B} & \frac{\partial^2 \Psi_{fso}^{f}(\mathcal{R}_E,\mathcal{R}_B)}{\partial \mathcal{R}_E^2} \end{bmatrix} = \begin{bmatrix} \mathcal{A} & \mathcal{B} \\ \mathcal{B} & \mathcal{C} \end{bmatrix}. \tag{60}$$

Para $\mathcal{A} < 0$ e $\mathcal{A}\cdot\mathcal{C} - \mathcal{B}^2 > 0$, $(\mathcal{R}_{E,u}^{f^\star},\mathcal{R}_{B,u}^{f^\star})$ pode ser usado para obter o máximo local de $\Psi_{fso}^{f}(\mathcal{R}_E,\mathcal{R}_B)$.

□

Os valores ótimos de $\mathcal{R}_E$ e $\mathcal{R}_B$ para a EST com restrições de sigilo são apresentados no que se segue.

Teorema 3. *Os valores restritos ótimos de $\mathcal{R}_E$ e $\mathcal{R}_B$ que maximizam a EST com restrições de sigilo para o esquema de taxa fixa são dados, respectivamente, por*

$$\mathcal{R}_E^{f^\star} = \max\left(\mathcal{R}_{E,u}^{f^\star},\mathcal{R}_E^{th^\star}\right), \tag{61a}$$

$$\mathcal{R}_B^{f^\star} = \begin{cases} \mathcal{R}_{B,u}^{f^\star}, & \textit{se } \mathcal{R}_{E,u} \geq \mathcal{R}_E^{th^\star}; \\ \mathcal{R}_{B,c}^{f^\star}, & \textit{caso contrário.} \end{cases} \tag{61b}$$

onde $\mathcal{R}_{B,c}^{f^\star}$ *é o valor ótimo restringido de* $\mathcal{R}_B$ *e é dado por*

$$\mathcal{R}_{B,c}^{f^\star} = \log_2\left(-\frac{A_0 N_B^r \theta_B^{AP}}{N_0} W\left(\frac{\left(C1 - C1^{1-N_A^t}\right)\Gamma\left(\kappa_B^{AP}\right)\left(\frac{X_{\mathcal{R}_B}}{\theta_B^{AP}}\right)^{1-\kappa_B^{AP}}}{\exp\left(\frac{N_0}{A_0 N_B^r \theta_B^{AP}}\right)\left(R_{B,c}^{f*} - \mathcal{R}_E^{f*}\right)\log(2) N_A^t}\right)\right), \tag{62}$$

onde $W(\cdot)$ *corresponde à função* W *de Lambert.*

Demonstração. Primeiro, deve-se notar que $\mathcal{S}_{fso}(\mathcal{R}_E)$ é uma função monotonicamente decrescente de $\mathcal{R}_E$, o que significa que, se $\mathcal{R}_{E,u}^{f^\star} < \mathcal{R}_E^{th^\star}$, então usar $\mathcal{R}_{E,u}^{f^\star}$ resultará em uma SOP maior que o máximo permitido $\mathcal{S}^{\text{th}}$. Seguindo uma abordagem semelhante à descrita no Teorema 2, pode-se concluir que o valor ótimo de $\mathcal{R}_E$ em um cenário restrito é dado pelo máximo entre $\mathcal{R}_{E,u}^{f^\star}$ e $\mathcal{R}_E^{th^\star}$, que resulta em (61a).

Observando que $\mathcal{R}_{B,u}^{f^\star}$ não representa o valor ótimo de $\mathcal{R}_B$ quando $\mathcal{R}_{E,u}^{f^\star} < \mathcal{R}_E^{th^\star}$, é preciso encontrar o valor ótimo de $\mathcal{R}_B$ para um valor fixo de $\mathcal{R}_E = \mathcal{R}_E^{th^\star}$. Semelhante ao apresentado em (YAN et al., 2015) e descrito no Teorema 2, tem-se que o valor de $\mathcal{R}_B$ que atinge o ponto estacionário de $\Psi_{fso}^{f}(\mathcal{R}_E,\mathcal{R}_B)$ é o ótimo $\mathcal{R}_B$ para um valor fixo de $\mathcal{R}_E$, que é obtido substituindo (41) e (55) em (53), equacionando a primeira derivada para zero e resolvendo para $\mathcal{R}_B$. Segue que a primeira derivada é dada por

$$0 = (1-\mathcal{S}^{\text{th}})\left(1 - C_1^{N_A^t}\right) - \frac{N_0 2^{\mathcal{R}_B}(1-\mathcal{S}^{\text{th}})\log(2) N_A^t \mathcal{R}\; C_1^{N_A^t - 1}\left(\frac{x_B^{fso}}{\theta_B^{\text{AP}}}\right)^{\kappa_B^{\text{AP}}-1}}{\exp\left(-\frac{x_B^{fso}}{\theta_B^{\text{AP}}}\right)\theta_B^{\text{AP}} N_b A_0 \Gamma\left(\kappa_B^{\text{AP}}\right)}, \tag{63}$$

resultando em (62) e concluindo a prova. □

4.2.5 Resultados Numéricos

Nesta seção, são apresentados resultados numéricos para avaliar a análise realizada na Seção 4.2, adotando o mesma SNR γ_0 livre de turbulência para Eve e Bob, com $d = d_{m,n} = 1$ km, $\lambda = 1550$ nm (ABOU-RJEILY, 2015), e usando os parâmetros de ajuste $\epsilon = 0$ e $\Omega = 0{,}97$ para a variável gama aproximada. Seguindo (FARID; HRANILOVIC, 2007), também é utilizado $\omega_b = 2.5$ e $\rho = 0.1$.

A Figura 11 apresenta a EST com restrições de sigilo em função da taxa de redundância para o esquema de transmissão adaptativa com $\sigma_s \in \{1,2,3\}$ e $N_A^t = N_E^r = 2$, e para diferentes valores de $\mathcal{S}^{\text{th}}$. Pode-se ver que, à medida que o desvio padrão do deslocamento do erro de alinhamento aumenta, a SOP máxima permitida

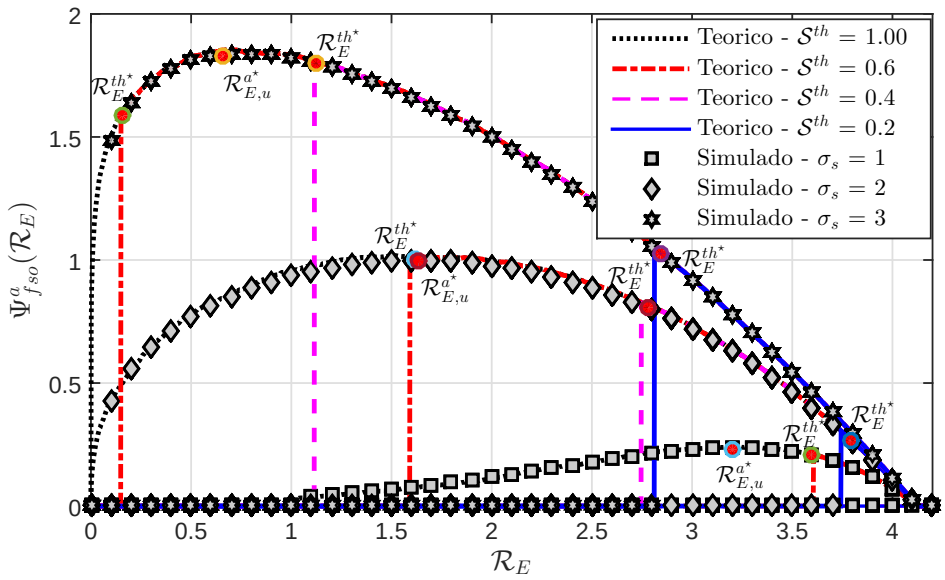


Figura 11 – $\Psi^a_{fso}(\mathcal{R}_E)$ em função de $\mathcal{R}_E$ para o esquema de transmissão adaptativa com $N_A^t = N_E^r = 2$, $N_B^r = 1$, $\mathcal{S}^{\text{th}} \in \{1,0.6,0.4,0.2\}$ e $\sigma_s \in \{1,2,3\}$.
Fonte: Autoria própria.

também é aumentada, o que significa que, dependendo de σ_s, o sistema pode ter que operar com um valor menor de $\Psi^a_{fso}(\mathcal{R}_E)$ para garantir que a SOP máxima permitida seja viável. Note que isso está de acordo com o modelo de sistema proposto, uma vez que o aumento de σ_s diminui a fração da potência recebida por Eve, uma vez que ele aumenta a probabilidade do espião estar fora do raio do feixe recebido ω_b. Da Figura 11, também pode-se ver que os valores teóricos aproximados (representados pelos círculos vermelhos) de $\mathcal{R}_{E,u}^{a\star}$ (sem restrições) e $\mathcal{R}_E^{th\star}$ (para $\mathcal{S}^{\text{th}} \in \{0.6,0.4,0.2\}$) de, respectivamente, (48) e (49), estão de acordo com os resultados numéricos ótimos para diferentes valores de σ_s, demonstrando um erro de aproximação abaixo de 2%. É importante notar também que, como indicado no Teorema 2 e semelhante ao observado em (YAN et al., 2014, 2015), os pontos estacionários obtidos de (48) representam o máximo local para todos os cenários avaliados neste trabalho.

Para validar as derivações analíticas dos Lemas 2 e 3, a Figura 12 apresenta a EST em função da taxa de redundância $\mathcal{R}_E$ e a taxa de palavras de código enviadas $\mathcal{R}_B$ para $N_A^t = N_E^r = 2$, $N_B^r = 1$ e $\sigma_s = 2$, em um cenário sem restrições ($\mathcal{S}^{\text{th}} = 1.0$). Pode-se ver que os resultados usando (41) e (55) são equivalentes aos resultados da simulação, confirmando a utilidade de tais equações. Além disso, note que a SOP em (41) é aplicada para esquemas adaptativo e de taxa fixa, de modo que a Figura 12 também valida a expressão SOP obtida para o esquema adaptativo.

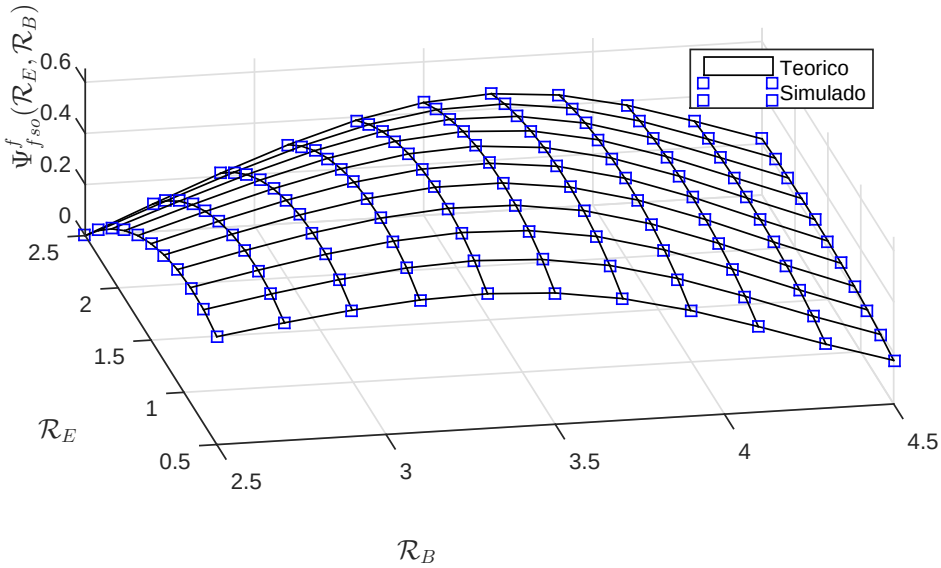
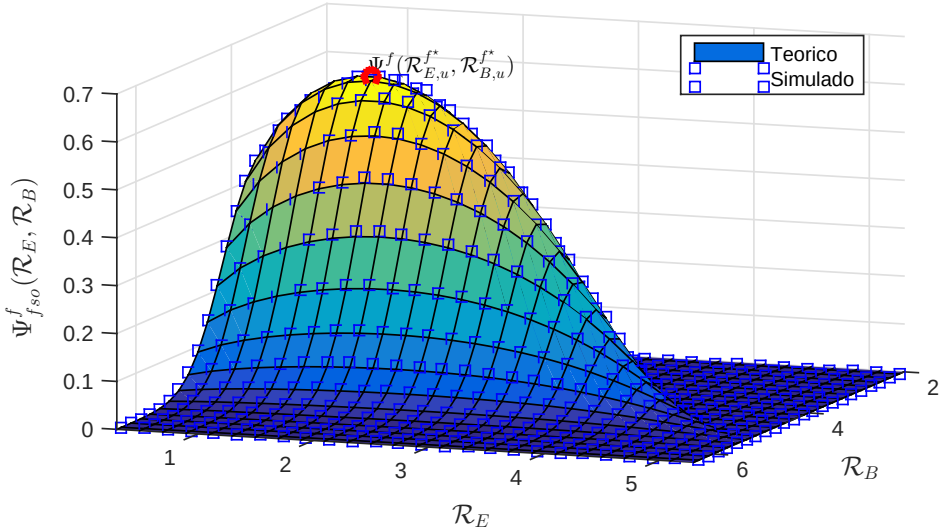


Figura 12 – $\Psi^f_{fso}(\mathcal{R}_E,\mathcal{R}_B)$ em função de $\mathcal{R}_E$, $\mathcal{R}_B$ para o esquema de transmissão de taxa fixa com $N^t_A = N^r_E = 2$, $N^r_B = 1$, $\sigma_s = 2$ e $\mathcal{S}^{\text{th}} = 1.0$.
Fonte: Autoria própria.

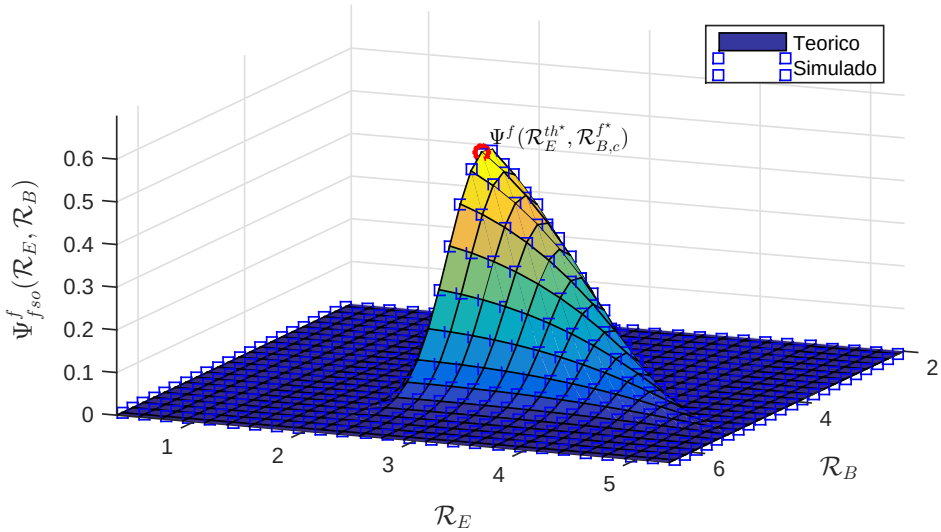
A Figura 13(a) apresenta o valor sem restrições ($\mathcal{S}^{\text{th}} = 1.0$) da EST em função da taxa de redundância $\mathcal{R}_E$ e a taxa de palavras de código $\mathcal{R}_B$, para o esquema de transmissão de taxa fixa com $N^t_A = N^r_E = 2$, $N^r_B = 1$ e $\sigma_s = 2$. Pode-se ver que existe um valor ótimo de $\mathcal{R}_B$ para cada valor de $\mathcal{R}_E$ (e vice-versa), e que existe um ponto estacionário de $\Psi^f_{fso}(\mathcal{R}_E,\mathcal{R}_B)$ que resulta na ótima EST, conforme indicado no Teorema 3. Pode-se também ver que os valores teóricos aproximados de $\mathcal{R}^{f^\star}_{E,u} = 1.250$ bpcu e $\mathcal{R}^{f^\star}_{B,u} = 3.401$ bpcu de, respectivamente, (56a) e (56b), estão de acordo com as taxas numéricas ótimas $\mathcal{R}_E = 1.257$ bpcu e $\mathcal{R}_B = 3.400$ bpcu, o que resulta em $\Psi^f_{fso}(\mathcal{R}_E,\mathcal{R}_B) = 0.62$ bpcu.

Na Figura 13(b) é apresentada uma análise semelhante, mas impondo uma restrição de sigilo com $\mathcal{S}^{\text{th}} = 0.5$. O valor do limiar $\mathcal{R}^{th^\star}_E$, para o qual qualquer valor menor resultará em uma SOP maior que o limite $\mathcal{S}^{th}$, pode ser obtido diretamente de (49). É importante notar que, de acordo com o Teorema 3, o valor ótimo de $\mathcal{R}^{f^\star}_E$ é o máximo entre $\mathcal{R}^{f^\star}_{E,u}$ e $\mathcal{R}^{th^\star}_E$, e que o valor ótimo $\mathcal{R}^{f^\star}_B$ pode ser obtido de (62). Finalmente, o valor ótimo de $\Psi^f_{fso}(\mathcal{R}^{th^\star}_E, \mathcal{R}^{f^\star}_{B,c})$ é apresentado usando (53), (49) e (62), confirmando a precisão das derivações matemáticas.

Na Figura 14 é apresentada a EST em função de $\mathcal{S}^{\text{th}}$ para os esquemas adaptativo e de taxa fixa para $N^r_E = 2$, $N^t_A = N^r_B \in \{1,2,4\}$ e $\sigma_s = 2$. Pode-se ver que, para diferentes valores de (N^t_A, N^r_B), os resultados usando (38), (39) e (53) estão de perfeito acordo com as simulações. Também pode-se ver que, à medida que a SOP máxima permitida aumenta,



(a) Cenário sem restrições com $\mathcal{S}^{\text{th}} = 1.0$.



(b) Cenário com restrições com $\mathcal{S}^{\text{th}} = 0.5$.

Figura 13 – $\Psi^f_{fso}(\mathcal{R}_E, \mathcal{R}_B)$ em função de $\mathcal{R}_E$, $\mathcal{R}_B$ para o esquema de taxa fixa com $N^t_A = N^r_E = 2$, $N^r_B = 1$ e $\sigma_s = 2$.
Fonte: Autoria própria.

a EST máxima obtida por ambos os esquemas também aumenta, e que um maior número de aberturas no canal legítimo permite que o sistema alcance uma SOP mais baixa mesmo no cenário sem restrições. Além disso, é mostrado que o esquema adaptativo é capaz de obter uma EST mais elevada do que o obtido usando o esquema de taxa fixa, o que é esperado porque, ao usar o esquema adaptativo, Alice possui o CSI instantâneo sobre o canal legítimo.

A Figura 15 apresenta a EST em função de $N^t_A = N^r_B = N^r_E$ para os esquemas adaptativo e de taxa fixa para $\mathcal{S}^{\text{th}} \in \{1, 0.3, 0.1\}$. Pode-se ver que, à medida que o número

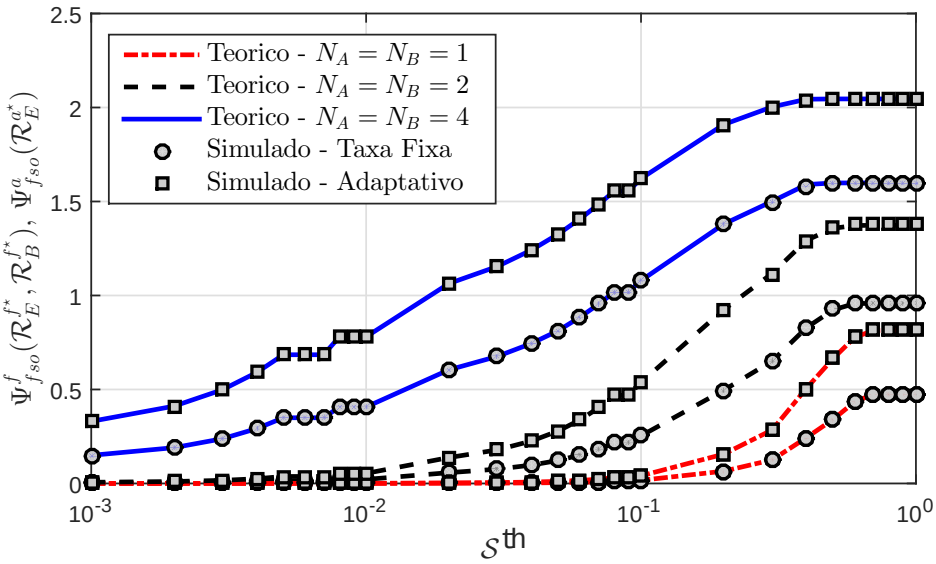


Figura 14 – $\Psi^f_{fso}(\mathcal{R}^{f^\star}_E, \mathcal{R}^{f^\star}_B)$, $\Psi^a_{fso}(\mathcal{R}^{a^\star}_E)$ em função de $\mathcal{S}^{\text{th}}$ para os esquemas de transmissão de taxa fixa e adaptativa com $N^r_E = 2$, $N^t_A = N^r_B \in \{1,2,4\}$ e $\sigma_s = 2$. Fonte: Autoria própria.

de aberturas aumenta para todos os nós, a EST máxima obtida também aumenta. Isso pode ser explicado pelo fato de que a ordem de diversidade no canal legítimo aumenta mais rapidamente do que a observada no canal de espionagem. Curiosamente, a EST é aproximadamente a mesma para o esquema adaptativo com $N^t_A = N^r_B = N^r_E = 5$ e $\mathcal{S}^{\text{th}} = 0.3$, e para o esquema de taxa fixa com $N^t_A = N^r_B = N^r_E = 10$ e $\mathcal{S}^{\text{th}} = 1.0$. Isso implica que, em um cenário com cinco aberturas por nó, o esquema adaptativo permite restringir a SOP de modo que ela seja tão baixa quanto 30%, enquanto atinge ainda o mesmo desempenho de EST que o esquema de taxa fixa sem restrições com dez aberturas por nó.

Finalmente, na Figura 16 é apresentada a EST em função de σ_s para os esquemas adaptativo e de taxa fixa, com $\mathcal{S}^{\text{th}} = 0.2$. Pode-se ver que, à medida que o desvio padrão do deslocamento do erro de alinhamento aumenta, a EST para ambos os regimes aumenta. Como se vê na Figura 11, isso se deve ao fato de que o aumento em σ_s diminui a capacidade do canal de espionagem.

4.3 MÚLTIPLOS SALTOS COM *RELAYS*

Para o cenário com múltiplos saltos, é considerado uma rede baseada em FSO onde um transmissor legítimo Alice, fornecido com N^t_A aberturas de transmissão por caminho, se comunica com um receptor legítimo, Bob, com N^r_B aberturas de recepção por

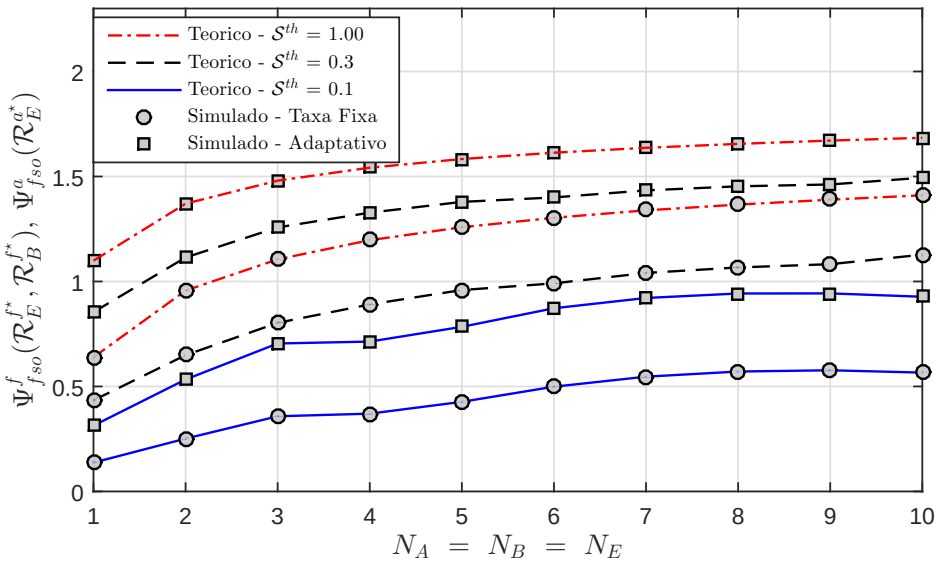


Figura 15 – $\Psi^f_{fso}(\mathcal{R}^{f^\star}_E,\mathcal{R}^{f^\star}_B)$, $\Psi^a_{fso}(\mathcal{R}^{a^\star}_E)$ em função de $N^t_A = N^r_B = N^r_E$ para os esquemas de transmissão de taxa fixa e adaptativa com $\mathcal{S}^{\text{th}} \in$ {1,0.3,0.1}.
Fonte: Autoria própria.

caminho, sendo assistido por vários *relays* (R) com N^t_R aberturas de transmissão e N^r_R aberturas de recepção, na presença de múltiplos espiões, cada Eve (E) com N^r_E aberturas de recepção. Esse modelo está ilustrado na Figura 17, onde d e $d_{m,n}$ representam a distância, respectivamente, para a comunicação direta e para o salto $n \in \{1,...,R_N+1\}$ no caminho $m \in \{1,...,N_P\}$. Observe que cada um dos N_P caminhos contém R_N *relays*, resultando em R_N+1 saltos por caminho. Assume-se que existem $R_{N,E}$ *relays* entre Alice e os espiões, e que existem $N_{P,E}$ Eves que cooperam entre si, onde cada Eve espia um caminho diferente. Assim, para $R_{N,E} = R_N$, todos os espiões estão perto de Bob. Também assume-se que as irradiações ópticas recebidas por diferentes nós são independentes e distribuídas de forma idêntica (i.i.d.). É considerada a detecção coerente de modo que a SNR no receptor para o canal $[m,n]$ é dada pela equação (29). Da mesma forma como considerado na Seção anterior, é assumido que os erros de alinhamento são insignificantes para os canais legítimos, de modo que $I^{i,j}_{p,m,n} = 1$ e a irradiância é dada por uma única variável aleatória gama-gama.

4.3.1 Esquema Adaptativo

Observando que Alice possui o CSI instantâneo em relação aos canais entre Alice e Bob, seguindo (ABOU-RJEILY, 2015) é assumido que, primeiro, a solução SR com decodifica e encaminha seleciona o caminho ideal entre Alice e Bob. Então, para cada par de transmissor/receptor entre Alice e Bob, é empregada a técnica TLS e cada receptor

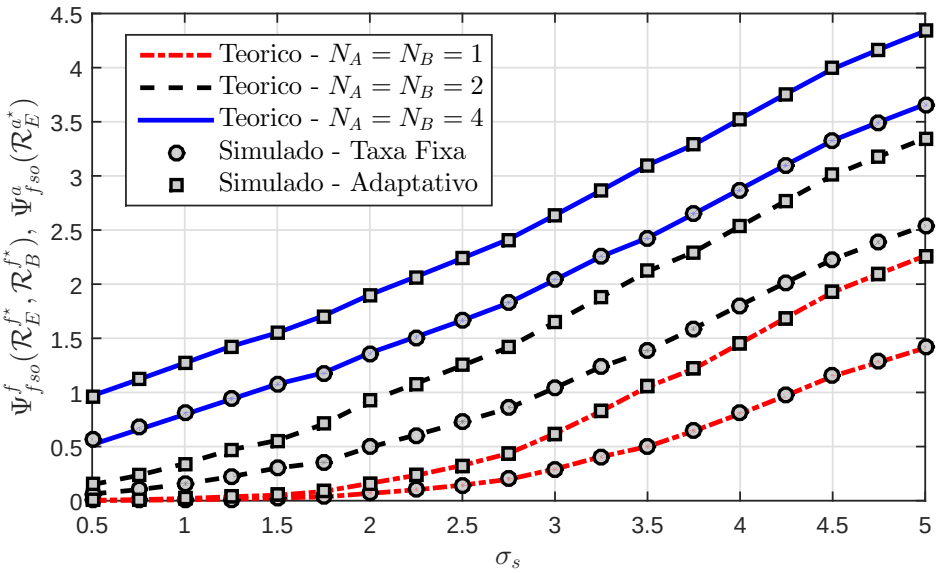


Figura 16 – $\Psi^f_{fso}(\mathcal{R}^{f^\star}_E, \mathcal{R}^{f^\star}_B)$, $\Psi^a_{fso}(\mathcal{R}^{a^\star}_E)$ em função de σ_s para os esquemas de transmissão adaptativa e de taxa fixa com $N^r_E = 2$ e $\mathcal{S}^{\text{th}} = 0.2$.
Fonte: Autoria própria.

opera utilizando MRC. Para um único salto, a irradiância pode ser escrita como (ABOU-RJEILY, 2015)

$$I^a_{m,n} = \begin{cases} I_{p,m,n} \sum_{j=1}^{N^r_E} I^{i,j}_{a,m,n}, & \text{Eve;} \\ \max\limits_{i=1,\ldots,N^t_{m,n}} I_{p,m,n} \sum_{j=1}^{N^r_{m,n}} I^{i,j}_{a,m,n}. & \text{Bob/Relay,} \end{cases} \tag{64}$$

onde $N^t_{m,n}$ e $N^r_{m,n}$ são, respectivamente, o número de aberturas transmissoras e receptoras do canal $[m,n]$. Para um único caminho, a SOP pode ser obtida como

$$\mathcal{S}_{fsor}(\mathcal{R}_E) = \Pr\left\{\frac{I_{m,n} r_{m,n} A_0 \mathcal{Z}_{m,n}}{N_0} > 2^{\mathcal{R}_E} - 1\right\}, \tag{65}$$

onde o índice m,E indica o canal específico no caminho m no qual Eve está presente e $I_{m,n}$ é obtido de (64) para o esquema adaptativo. Notando que a restrição de confiabilidade é sempre garantida, a EST de (38) pode ser representada por (39).

No que segue, é apresentada uma expressão para a SOP.

Teorema 4. *A SOP do esquema adaptativo é dada por*

$$\mathcal{S}^a_{fsor}(\mathcal{R}_E) = \frac{[1 - F^{\gamma\gamma p}_{m,n}(\mathcal{X}^{fsor}_E, 1, N^r_E)] N_{P,E}}{N_P}, \tag{66}$$

onde $\mathcal{X}^{fsor}_E = \frac{N_0(2^{\mathcal{R}_E}-1)}{N^r_E r_{m,n} A_0 \mathcal{Z}_{m,n}}$ *e* $F^{\gamma\gamma p}_{m,n}(\cdot)$ *é obtido de* (37).

Demonstração. Usando TLS e MRC, tem-se que (65) para a comunicação direta é dada

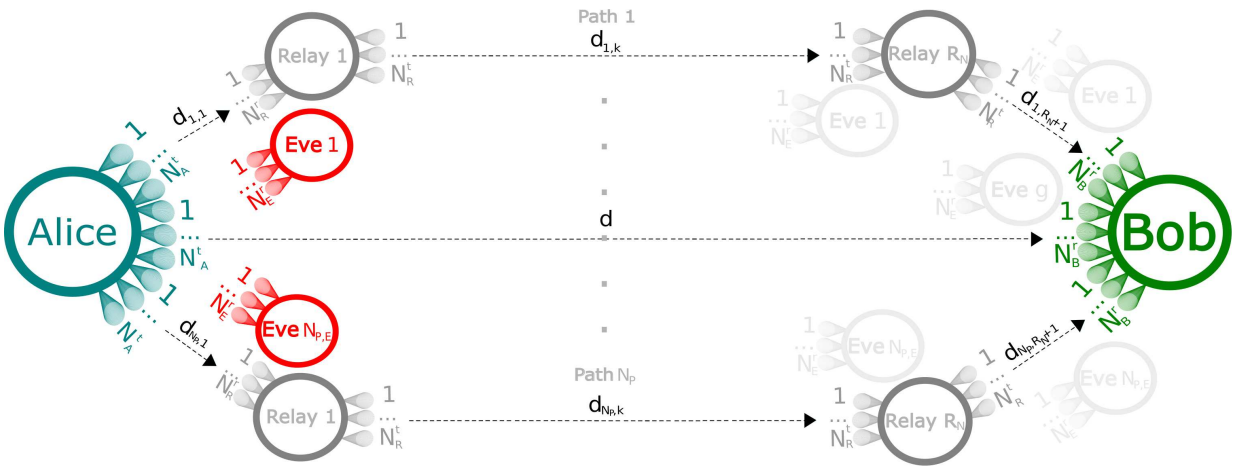


Figura 17 – Comunicação MIMOME FSO com múltiplos saltos.
Fonte: Autoria própria.

de maneira semelhante à (45) como

$$\mathcal{S}^{a}_{fsor}(\mathcal{R}_E) = \Pr\left\{ Z X_\alpha Y_{\beta_E} > \frac{N_0\left(2^{\mathcal{R}_E}-1\right)}{N_E^r r_{m,n} A_0 \mathcal{Z}_{m,n}} \right\}. \tag{67}$$

Para SR, pode-se ver que a SOP é igual ao produto entre (67), usando a cdf em (37), e a probabilidade de uma Eve estar no caminho transmissor, que é dada por $\frac{N_{P,E}}{N_P}$. □

A EST é então obtida substituindo (66) em (39).

4.3.2 Esquema com Taxa Fixa

Para o esquema de taxa fixa, é assumido que a técnica decodifica e encaminha com todos os *relays* ativos e retransmitindo é utilizada, o que implica que todos os *relays* que são capazes de decodificar a mensagem retransmitem com todas as suas respectivas aberturas. Para um único salto, a irradiância $I^f_{m,n}$ é igual para todos os nós e é dada como (ABOU-RJEILY, 2011)

$$I^f_{m,n} = I_{p,m,n} \frac{1}{N^t_{m,n}} \sum_{i=1}^{N^t_{m,n}} \sum_{j=1}^{N^r_{m,n}} I^{i,j}_{a,m,n}. \tag{68}$$

Note que tanto as restrições de sigilo quanto as restrições de confiabilidade não podem ser garantidas *a priori*, de maneira que a EST é dada pela equação (9).

Para obter uma forma fechada para a probabilidade de transmissão confiável e para a SOP, primeiro é necessário obter a probabilidade de transmissão confiável para um

único salto, que pode ser expressa como

$$1-O^{f}_{m,n}(\mathcal{R}_B,T_N)=\Pr\left\{\frac{I^{f}_{m,n}r_{m,n}A_0\mathcal{Z}_{m,n}}{N_0}>2^{\mathcal{R}_B}-1\right\}, \tag{69}$$

onde T_N representa o número de nós legítimos transmitindo para o receptor (que é maior que um apenas para Bob) e é obtido de maneira fechada no que segue.

Lema 5. *A probabilidade de transmissão confiável para um único salto $O^{f}_{m,n}(\cdot)$ é dada por*

$$1-O^{f}_{m,n}(\mathcal{R}_B,T_N)=1-F^{\gamma\gamma}_{m,n}(\mathcal{X}^{fsor}_B,T_N,T_N N^{r}_{m,n}N^{t}_{m,n}), \tag{70}$$

onde $\mathcal{X}^{fsor}_B=\frac{N_0\left(2^{\mathcal{R}_B}-1\right)}{T_N N^{r}_{m,n}r_{m,n}A_0\mathcal{Z}_{m,n}}$ *e* $F^{\gamma\gamma}_B(\cdot)$ *é obtido de* (37).

Demonstração. De maneira similar ao Teorema 4 e com a diferença que, para o esquema de taxa fixa o método de repetição é utilizando ao invés do TLS, tem-se que a irradiância é dada por (68), o que significa que existirão $N^{t}_{m,n}$ aberturas de recepção por nó. Notando que os efeitos em larga escala são assumidos como totalmente correlacionados entre as aberturas de recepção, o termo $\frac{1}{N^{t}_{m,n}}\sum_{i=1}^{N^{t}_{m,n}}$ pode ser visto como uma alteração no parâmetro β da variável aleatória gama-gama. Finalmente, usando a aproximação de (ZHANG et al., 2016) para a soma de variáveis gama-gama, o número de nós transmissores pode ser equacionado através da multiplicação de ambos os parâmetros α e β por T_N, resultando em (70) e concluindo a prova. □

Teorema 5. *A TP para o regime de taxa fixa é dada por*

$$\begin{aligned}1-\mathcal{O}^{f}_{fsor}(\mathcal{R}_B)=&\sum_{g=1}^{N_P}\binom{N_P}{g}\left(1-O^{f}_{m,n}(\mathcal{R}_B,1)\right)^{gR_N}\\&\left(1-\left(1-O^{f}_{m,n}(\mathcal{R}_B,1)\right)^{R_N}\right)^{N_P-g}(1-O^{f}_{m,n}(\mathcal{R}_B,g)).\end{aligned} \tag{71}$$

Demonstração. Para obter (71), recorre-se ao fato de que a probabilidade de *outage* pode ser reescrita como

$$\mathcal{O}^{f}_{fsor}(\mathcal{R}_B)=\sum_{c=1}^{2^{N_P}}O^{f}(S_c)\Pr\{S_c\}, \tag{72}$$

onde 2^{N_P} representa, para N_P caminhos, o número de grupos S_c únicos de *relays* transmissores na vizinhança de Bob, $O^{f}(S_c)$ é a probabilidade de *outage* para Bob quando todos os *relays* em S_c transmitem a mensagem e $\Pr\{S_c\}$ é a probabilidade de se ter o grupo S_c. Assumindo que cada caminho experimenta a mesma probabilidade de *outage*, que pode ser obtido através da distribuição correta da fração da potência $r_{m,n}$

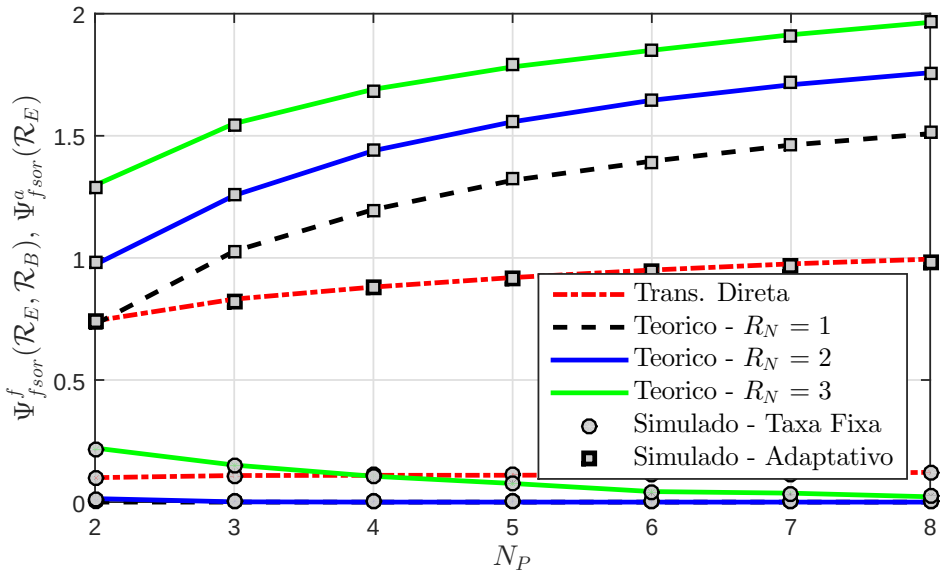


Figura 18 – $\Psi^a_{fsor}(\cdot)$, $\Psi^f_{fsor}(\cdot)$ em função de N_P para $\mathcal{S}^{\text{th}} = 0.6$ e $\gamma_0 = 30$ dB.
Fonte: Autoria própria.

utilizada por cada canal quando apenas a SNR média é conhecida, e que os parâmetros α e β são os mesmo para todos os *relays* transmissores na vizinhança de Bob, (72) pode ser expressa utilizando a TP usando a distribuição binomial apresentada em (71), no qual $(1-O^f_{m,n}(\mathcal{R}_B,1))^{R_N}$ representa a probabilidade de um *relay* próximo à Bob ser capaz de receber a mensagem e $(1-O^f_{m,n}(\mathcal{R}_B,g))$ representa a probabilidade de Bob ser capaz de decodificar a mensagem. □

Similar ao Teorema 5 e assumindo que os espiões cooperam entre si, a SOP em (38) é dada por

$$\mathcal{S}^f_{fsor}(\mathcal{R}_E) = \sum_{g=1}^{N_{P,E}} \binom{N_{P,E}}{g} \left(1-O^f_{m,n}(\mathcal{R}_B,1)\right)^{gR_{N,E}} \frac{(1-F^{\gamma\gamma p}_{m,n}(\mathcal{X}_E^{fsor} g^{-1}, g, gN_E^r N_{g,E}^t))}{\left(1-\left(1-O^f_{m,n}(\mathcal{R}_B,1)\right)^{R_{N,E}}\right)^{g-N_{P,E}}}, \tag{73}$$

onde $N^t_{g,E}$ indica o número de aberturas do nó transmissor no qual o g-ésimo Eve obtém a mensagem.

4.3.3 Resultados Numéricos

Nesta seção, são apresentados resultados numéricos para avaliar a análise anterior, adotando a mesma SNR γ_0 livre de turbulência para Eve e para o receptor legítimo (Bob ou Relay), com $d = 3$ km, $N^t_A = N^r_R = N^t_R = N^r_B = 2$, $\lambda = 1550$ nm (ABOU-

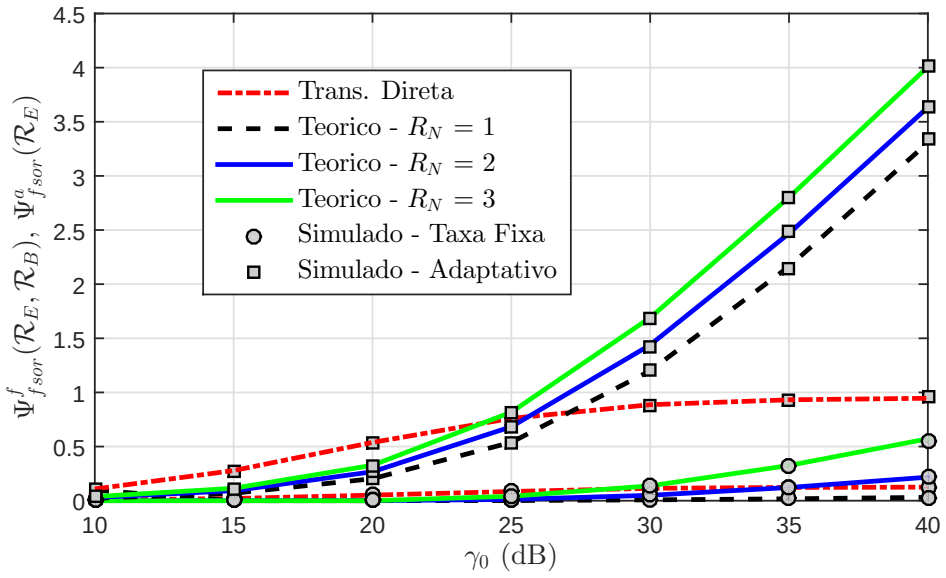


Figura 19 – $\Psi^a_{fsor}(\cdot)$, $\Psi^f_{fsor}(\cdot)$ em função de γ_0 para $\mathcal{S}^{\text{th}} = 1$ e $N_P = 4$.
Fonte: Autoria própria.

RJEILY, 2015) e $\sigma_s = 2$. No cenário com vários *relays*, salvo indicado o contrário, é assumido que a distância entre cada nó para um determinado caminho é $d_{m,n} = d/N_P$ e que $N_{P,E} = 1$ com Eve perto do primeiro *relay* de um dado caminho entre Alice e Bob. É considerado também que Eve tem o mesmo número total de aberturas de recepção por caminho que aquele usado no canal legítimo, ou seja, $N^r_E = N_P\ R_N\ N^r_B/N_{P,E}$, onde o termo $N_P R_N N^r_B$ representa o número de aberturas de transmissão e recepção para o canal legítimo em um cenário de comunicação direta.

Na Figura 18 é apresentado um importante resultado deste trabalho, apresentando a EST em função do número de caminhos para $\mathcal{S}^{\text{th}} = 0.6$ e $\gamma_0 = 30$ dB. Pode-se ver que as equações apresentadas estão muito próximas aos resultados numéricos e que, para o esquema adaptativo, a EST aumenta com o número de *relays* e caminhos, o que é explicado pelo fato que, para SR, o aumento no número de caminhos diminui a probabilidade de Eve estar no caminho certo, e o uso de *relays* adicionais diminui a turbulência de cada salto. Por outro lado, para o esquema de taxa fixa, a EST diminui ligeiramente com o aumento do número de caminhos, enquanto ainda aumenta com R_N.

A Figura 19 apresenta a EST em função de γ_0 sem restrições de sigilo. Para $N_P = 4$ e $\mathcal{S}^{\text{th}} = 1$, tem-se que o aumento na SNR aumenta significativamente a EST para o esquema adaptativo, enquanto apresenta apenas um ligeiro aumento para o regime de taxa fixa. Isso é justificado porque o esquema adaptativo usa SR, o que significa que Eve só pode se beneficiar por uma fração de γ_0, o que é demonstrado pela diferença entre a comunicação direta (ou seja, $N_P = 1$) e a comunicação utilizando *relays* com $R_N = 1$

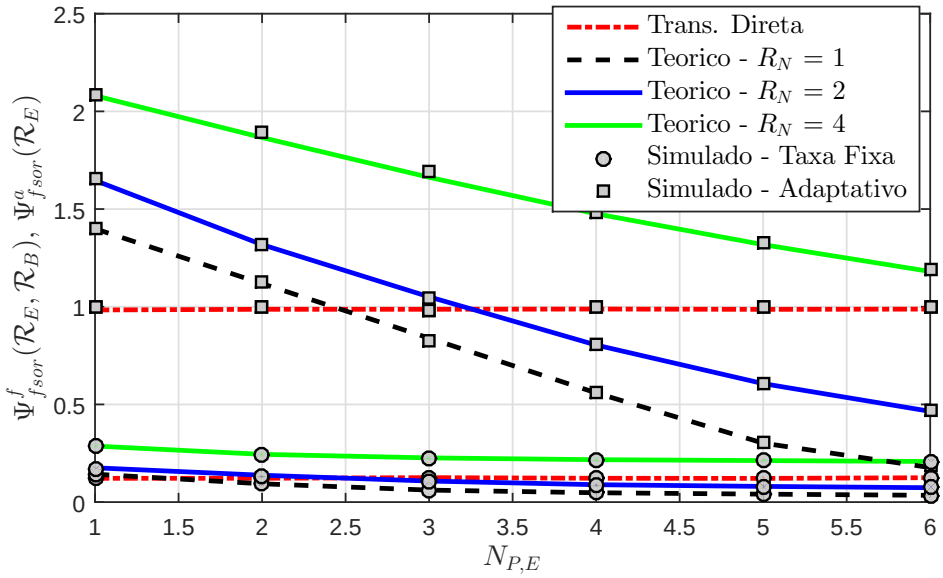


Figura 20 – $\Psi^a_{fsor}(\cdot)$, $\Psi^f_{fsor}(\cdot)$ em função de $N_{P,E}$ para $\mathcal{S}^{\text{th}} = 1$, $N_P = 6$ e $R_{N,E} = R_N$. Fonte: Autoria própria.

(ou seja, $N_P = 4$).

Figura 20 apresenta a EST em função de $N_{P,E}$ para $\mathcal{S}^{\text{th}} = 1$, $R_{N,E} = R_N$ (ou seja, todos os Eves estão perto de Bob), $N_P = 6$ e $\gamma_0 = 30$ dB. Pode-se ver que a transmissão com vários saltos é útil para aumentar a EST mesmo quando múltiplos Eves estão espiando todos os caminhos entre Alice e Bob (ou seja, $N_{P,E} = N_P$), podendo superar a comunicação direta através do aumento de R_N.

4.4 COMENTÁRIOS

Neste Capítulo, foi caracterizada a performance do MIMOME para transmissões de FSO coerentes. Um cenário de ameaça em que Eve está perto de Bob foi investigado, o que significa que a diferença de SNR observada em Bob e Eve é afetada não só por N_A^t, N_B^r e N_E^r, mas também pelos erros de alinhamento devido à distância entre Bob e Eve. Ao adotar a EST com restrições de sigilo como a métrica de desempenho, obtiveram-se as taxas ótimas para os esquemas adaptativo e de taxa fixa. Os resultados numéricos confirmaram a precisão das derivações matemáticas. Além disso, os resultados analíticos e de simulação demonstraram que, independentemente da SOP máxima permitida, a EST para o esquema adaptativo supera os resultados obtidos usando o esquema de transmissão de taxa fixa para comunicações FSO coerentes. Em seguida, também foi demonstrado que um ganho significativo é alcançado ao adicionar múltiplas aberturas e que a EST também depende da distância entre Eve e Bob. Por fim, foi demonstrado que, diferente

de (ABOU-RJEILY, 2015), em um cenário com restrições de sigilo a utilização de *relays* pode ser benéfica para comunicações FSO quando comparado com comunicação direta, mesmo na presença de múltiplos espiões.

5 COMENTÁRIOS FINAIS

Neste trabalho, foi determinada a taxa de transmissão segura com restrições de sigilo para um canal MIMOME em RF e em FSO. Os resultados foram apresentados utilizando os esquemas adaptativo e de taxa fixa, que foram propostos em (YAN et al., 2014, 2015). Para comunicações em RF verificou-se que, sem a restrição de *outage* de sigilo, um espião poderia ser capaz de obter uma quantidade de informações sigilosas acima do máximo aceitável para um determinado sistema, evidenciando a importância da métrica proposta neste trabalho. Para comunicações em FSO, verificou-se a importância do uso de múltiplas aberturas de transmissão e recepção, além das vantagens em uso de *relays* em tais sistemas.

No Capítulo 2 foram apresentadas as técnicas de diversidade utilizadas neste trabalho. Para o cenário em RF, foram apresentadas as técnicas TAS, MRT, SC e MRC. Para os cenários em FSO, foram apresentadas as técnicas TLS, RC, SR e AR. Foi então apresentada a métrica de desempenho taxa efetiva de transmissão segura. No Capítulo 3, o modelo proposto em (YAN et al., 2014) foi então estendido para um esquema MIMOME, onde todos os nós contêm múltiplas antenas. Assim, considerando o cenário em RF, foram obtidas equações analíticas para descrever o modelo proposto, determinando uma equação de ponto fixo para a taxa de sigilo alvo que maximiza a taxa de transmissão segura com restrições de sigilo. Em seguida, resultados numéricos foram apresentados para confirmar as análises descritas neste trabalho. No Capítulo 4, considerando redes de comunicação sem fio em FSO, foram apresentadas equações determinando a taxa alvo ótima para os esquemas adaptativo e com taxa fixa, seguido pelos resultados numéricos. Por fim, foram apresentadas equações da EST para ambos os esquemas em um cenário com o uso de *relays*, seguido de simulações para demonstrar a precisão das equações obtidas.

Foi demonstrado que o esquema MIMOME utilizando TAS é muito mais eficiente que o esquema SISOME em termos da taxa de sigilo, sendo ainda menos susceptível ao aumento do número de antenas no espião. Foi também investigado como a imposição de uma máxima SOP afeta a taxa de transmissão segura para os esquemas SISOME e MIMOME. Quando existe uma máxima SOP permitida, o esquema SISOME pode falhar em prover uma taxa de transferência ótima, enquanto é possível se obter uma grande ou mesmo ótima taxa utilizando o esquema MIMOME.

Para comunicações em FSO, demonstrou-se um ganho significativo ao se adicionar múltiplas aberturas nos nós legítimos, e que a EST depende da distância entre Eve e Bob.

Com o uso de *relays*, mostrou-se que ambos os esquemas podem ser beneficiados pelo aumento no número de saltos entre Alice e Bob, e que apenas o esquema adaptativo com retransmissão seletiva beneficia-se do aumento do número de caminhos.

Trabalhos futuros incluem a utilização da taxa efetiva de transmissão segura com restrições de sigilo em outros cenários. Por exemplo, para transmissões em RF com o auxílio de nós retransmissores, dada a natureza difusora do canal sem fio, pode-se analisar como a presença de Eve em diversos pontos da rede afetam o desempenho do canal. Pode-se ainda considerar cenários utilizando outras formas de comunicação, como a comunicação molecular (FARSAD et al., 2013), e analisar como possíveis nós espiões podem comprometer tais redes. A codificação de rede, onde os nós são aptos a processar as informações recebidas de diferentes origens e transmitir combinações das informações disponíveis (AHLSWEDE et al., 2000; KOETTER; MéDARD, 2003), também pode ser levada em consideração no modelo do sistema em conjunto com a métrica proposta.

REFERÊNCIAS

ABOU-RJEILY, C. On the optimality of the selection transmit diversity for MIMO-FSO links with feedback. **IEEE Communications Letters**, v. 15, n. 6, p. 641–643, June 2011. ISSN 1089-7798.

ABOU-RJEILY, C. Performance analysis of FSO communications with diversity methods: Add more relays or more apertures? **IEEE Journal on Selected Areas in Communications**, v. 33, n. 9, p. 1890–1902, Sept 2015. ISSN 0733-8716.

AGHAJANZADEH, S.; UYSAL, M. Diversity multiplexing trade-off in coherent free-space optical systems with multiple receivers. **IEEE/OSA Journal of Optical Communications and Networking**, v. 2, n. 12, p. 1087–1094, Dec 2010. ISSN 1943-0620.

AHLSWEDE, R.; CAI, N.; LI, S.-Y.; YEUNG, R. Network information flow. v. 46, n. 4, p. 1204 – 1216, 2000.

AL-AHMADI, S.; YANIKOMEROGLU, H. On the approximation of the generalized-k PDF by a gamma PDF using the moment matching method. In: **Proceedings of the IEEE Wireless Communications and Networking Conference**. 2009. p. 1–6. ISSN 1525-3511.

AL-HABASH, M. A.; ANDREWS, L. C.; PHILLIPS, R. L. Mathematical model for the irradiance probability density function of a laser beam propagating through turbulent media. **Optical Engineering**, v. 40, n. 8, p. 1554–1562, 2001.

ALVES, H.; SOUZA, R. D.; DEBBAH, M.; BENNIS, M. Performance of transmit antenna selection physical layer security schemes. **IEEE Signal Processing Letters**, v. 19, n. 6, p. 372–375, June 2012.

ANDREWS, L. C.; PHILLIPS, R. L.; HOPEN, C. Y.; AL-HABASH, M. A. Theory of optical scintillation. **Journal of the Optical Society of America A**, OSA, v. 16, n. 6, p. 1417–1429, Jun 1999.

BARATA, J. A. **Notas para um Curso de Física-Matemática**. Prentice Hall, 2016.

BARROS, J.; RODRIGUES, M. R. D. Secrecy capacity of wireless channels. In: **Proceedings of the IEEE International Symposium on Information Theory (ISIT'06)**. 2006.

BELMONTE, A.; KAHN, J. M. Performance of synchronous optical receivers using atmospheric compensation techniques. **OSA Optics Express**, OSA, v. 16, n. 18, p. 14151–14162, Sep 2008.

BELMONTE, A.; KAHN, J. M. Capacity of coherent free-space optical links using atmospheric compensation techniques. **OSA Optics Express**, OSA, v. 17, n. 4, p. 2763–2773, Feb 2009.

BLOCH, M.; BARROS, J. **Physical-Layer Security: From Information Theory to Security Engineering**. Cambridge University Press, 2011.

BLOCH, M.; BARROS, J.; RODRIGUES, M.; MCLAUGHLIN, S. Wireless information-theoretic security. **IEEE Transactions on Information Theory**, v. 54, n. 6, p. 2515–2534, June 2008. ISSN 0018-9448.

EDELSON, B.; HYDE, G.; ELECTRICAL, I. of; COMMITTEE, E. E. A. P. **A Report of the IEEE-USA Aerospace Policy Committee on Laser Satellite Communications, Programs, Technology and Applications**. IEEE, 1996.

FARID, A. A.; HRANILOVIC, S. Outage capacity optimization for free-space optical links with pointing errors. **The Journal of Lightwave Technology**, v. 25, n. 7, p. 1702–1710, July 2007. ISSN 0733-8724.

FARSAD, N.; GUO, W.; ECKFORD, A. W. Tabletop molecular communication: Text messages through chemical signals. **PLOS ONE**, Public Library of Science, v. 8, n. 12, p. 1–13, 12 2013. Disponível em: <https://doi.org/10.1371/journal.pone.0082935>.

FRIED, D. L. Optical heterodyne detection of an atmospherically distorted signal wave front. **Proceedings of the IEEE**, v. 55, n. 1, p. 57–77, Jan 1967. ISSN 0018-9219.

GAPPMAIR, W. Further results on the capacity of free-space optical channels in turbulent atmosphere. **IET Communications**, v. 5, n. 9, p. 1262–1267, June 2011. ISSN 1751-8628.

GARCIA-ZAMBRANA, A.; CASTILLO-VAZQUEZ, C.; CASTILLO-VAZQUEZ, B.; HINIESTA-GOMEZ, A. Selection transmit diversity for FSO links over strong atmospheric turbulence channels. **IEEE Photonics Technology Letters**, v. 21, n. 14, p. 1017–1019, July 2009. ISSN 1041-1135.

GARRIDO-BALSELLS, J. M.; JURADO-NAVAS, A.; PARIS, J. F.; CASTILLO-VAZQUEZ, M.; PUERTA-NOTARIO, A. Spatially correlated gamma-gamma scintillation in atmospheric optical channels. **OSA Optics Express**, OSA, v. 22, n. 18, p. 21820–21833, Sep 2014.

GOLDSMITH, A. **Wireless Communications**. Cambridge University Press, 2005.

GRABNER, M.; KVICERA, V. Multiple scattering in rain and fog on free-space optical links. **Journal of Lightwave Technology**, v. 32, n. 3, p. 513–520, Feb 2014. ISSN 0733-8724.

JAKEMAN, E.; PUSEY, P. N. A model for non-Rayleigh sea echo. **IEEE Transactions on Antennas and Propagation**, v. 24, n. 6, p. 806–814, nov. 1976.

KARIMI, M.; NASIRI-KENARI, M. BER analysis of cooperative systems in free-space optical networks. **Journal of Lightwave Technology**, v. 27, n. 24, p. 5639–5647, Dec 2009. ISSN 0733-8724.

KAUR, P.; JAIN, V. K.; KAR, S. Capacity of free space optical links with spatial diversity and aperture averaging. In: **27th Queen's Biennial Symposium on Communications**. 2014. p. 14–18.

KAZEMLOU, S.; HRANILOVIC, S.; KUMAR, S. All-optical multihop free-space optical communication systems. **Journal of Lightwave Technology**, v. 29, n. 18, p. 2663–2669, Sept 2011. ISSN 0733-8724.

KHALIGHI, M. A.; SCHWARTZ, N.; AITAMER, N.; BOURENNANE, S. Fading reduction by aperture averaging and spatial diversity in optical wireless systems. **IEEE/OSA Journal of Optical Communications and Networking**, v. 1, n. 6, p. 580–593, November 2009. ISSN 1943-0620.

KHISTI, A.; WORNELL, G. W. Secure transmission with multiple antennas part ii: The MIMOME wiretap channel. **IEEE Transactions on Information Theory**, v. 56, n. 11, p. 5515–5532, Nov 2010. ISSN 0018-9448.

KOETTER, R.; MéDARD, M. An algebraic approach to network coding. **IEEE/ACM Transactions on Networking**, v. 11, n. 5, p. 782– 795, October 2003.

LAI, L.; GAMAL, H. E. The relay-eavesdropper channel: Cooperation for secrecy. **IEEE Transactions on Information Theory**, v. 54, n. 9, p. 4005–4019, September 2008.

LAMBERT, S. G.; CASEY, W. L. **Laser Communications in Space**. Artech House, 1995.

LOPEZ-MARTINEZ, F. J.; GOMEZ, G.; GARRIDO-BALSELLS, J. M. Physical-layer security in free-space optical communications. **IEEE Photonics Journal**, v. 7, n. 2, p. 1–14, April 2015. ISSN 1943-0655.

MAJUMDAR, A.; RICKLIN, J. **Free-Space Laser Communications: Principles and Advances**. Springer New York, 2010. (Optical and Fiber Communications Reports). ISBN 9780387286778.

MOSCHOPOULOS, P. G. The distribution of the sum of independent gamma random variables. **Annals of the Institute of Statistical Mathematics**, v. 37, n. 1, p. 541–544, Dec 1985. ISSN 1572-9052.

NAVIDPOUR, S. M.; UYSAL, M.; KAVEHRAD, M. BER performance of free-space optical transmission with spatial diversity. **IEEE Transactions on Wireless Communications**, v. 6, n. 8, p. 2813–2819, Aug 2007. ISSN 1536-1276.

NISTAZAKIS, H. E.; KARAGIANNI, E.; TSIGOPOULOS, A.; FAFALIOS, M.; TOMBRAS, G. Average capacity of optical wireless communication systems over atmospheric turbulence channels. **Journal of Lightwave Technology**, v. 27, n. 8, p. 974–979, April 2009. ISSN 0733-8724.

NIU, M.; CHENG, J.; HOLZMAN, J. F. **Optical Communication**. InTech, 2012. ISBN 978-953-51-0784-2.

NIU, M.; CHENG, J.; HOLZMAN, J. F. Space-time coded MPSK coherent MIMO FSO systems in gamma-gamma turbulence. In: **IEEE Wireless Communications and Networking Conference**. 2013. p. 4266–4271. ISSN 1525-3511.

NOLL, R. J. Zernike polynomials and atmospheric turbulence∗. **Journal of the Optical Society of America**, OSA, v. 66, n. 3, p. 207–211, Mar 1976.

OGGIER, F.; HASSIBI, B. The secrecy capacity of the MIMO wiretap channel. In: **Proceedings of the IEEE International Symposium on Information Theory, (ISIT'08)**. 2008.

PRIYADARSHANI, R.; BHATNAGAR, M. R.; GHASSEMLOOY, Z.; ZVANOVEC, S. Outage analysis of a SIMO FSO system over an arbitrarily correlated m-distributed channel. **IEEE Photonics Technology Letters**, 2017. ISSN 1041-1135.

SAFARI, M.; UYSAL, M. Do we really need OSTBCs for free-space optical communication with direct detection? **IEEE Transactions on Wireless Communications**, v. 7, n. 11, p. 4445–4448, November 2008. ISSN 1536-1276.

SANAYEI, S.; NOSRATINIA, A. Antenna selection in mimo systems. **IEEE Communications Magazine**, v. 42, n. 10, p. 68–73, Oct 2004. ISSN 0163-6804.

SANDALIDIS, H. G.; TSIFTSIS, T. A.; KARAGIANNIDIS, G. K. Optical wireless communications with heterodyne detection over turbulence channels with pointing errors. **The Journal of Lightwave Technology**, v. 27, n. 20, p. 4440–4445, Oct 2009. ISSN 0733-8724.

SHANNON, C. A mathematical theory of communications. **Bell System Technical Journal**, v. 27, p. 379–423 e 623–656, 1948.

SHANNON, C. E. Communication theory of secrecy systems. **Bell System Technical Journal**, v. 28, p. 656–715, 1949.

SHAULOV, G.; PATEL, J.; WHITLOCK, B.; MENA, P.; SCARMOZZINO, R. Simulation-assisted design of free space optical transmission systems. In: **Military Communications Conference, 2005. MILCOM 2005. IEEE**. 2005. p. 918–922 Vol. 2.

TAN, B. S.; LI, K. H.; TEH, K. C. Transmit antenna selection systems: A performance comparison of different types of receiver schemes. **IEEE Vehicular Technology Magazine**, v. 8, n. 3, p. 104–112, Sept 2013. ISSN 1556-6072.

THANGARAJ, A.; DIHIDAR, S.; CALDERBANK, A. R.; MCLAUGHLIN, S. W.; MEROLLA, J. M. Applications of LDPC codes to the wiretap channel. **IEEE Transactions on Information Theory**, v. 53, n. 8, p. 2933–2945, Aug 2007. ISSN 0018-9448.

TSIFTSIS, T. A. Performance of heterodyne wireless optical communication systems over gamma-gamma atmospheric turbulence channels. **IEEE Electronics Letters**, v. 44, n. 5, p. 372–373, Feb 2008. ISSN 0013-5194.

VAVOULAS, A.; SANDALIDIS, H.; VAROUTAS, D. Weather effects on FSO network connectivity. **Optical Communications and Networking, IEEE/OSA Journal of**, v. 4, n. 10, p. 734–740, Oct 2012. ISSN 1943-0620.

WANG, Z.; GIANNAKIS, G. A simple and general parameterization quantifying performance in fading channels. **IEEE Transactions on Communications**, v. 51, n. 8, p. 1389–1398, August 2003.

WILLEBRAND, H.; GHUMAN, B. Fiber optics without fiber. **IEEE Spectrum**, v. 38, n. 8, p. 40–45, Aug 2001. ISSN 0018-9235.

WYNER, A. D. The wire-tap channel. **Bell System Technical Journal**, v. 54, n. 8, p. 1355–1387, 1975.

YAN, S.; GERACI, G.; YANG, N.; MALANEY, R.; YUAN, J. On the target secrecy rate for SISOME wiretap channels. In: **Proceedings of the IEEE International Conference on Communications (ICC'14)**. 2014. p. 987–992.

YAN, S.; YANG, N.; GERACI, G.; MALANEY, R.; YUAN, J. Optimization of code rates in sisome wiretap channels. **IEEE Transactions on Wireless Communications**, v. 14, n. 11, p. 6377–6388, Nov 2015. ISSN 1536-1276.

YANG, N.; ELKASHLAN, M.; DUONG, T. Q.; YUAN, J.; MALANEY, R. Optimal transmission with artificial noise in MISOME wiretap channels. **to appear in the IEEE Transactions Vehicular Technology**, 2015.

YANG, N.; YEOH, P. L.; ELKASHLAN, M.; SCHOBER, R.; COLLINGS, I. B. Transmit antenna selection for security enhancement in MIMO wiretap channels. **IEEE Transactions on Communications**, v. 61, n. 1, p. 144–154, January 2013.

YOUNG, N. J. Orbits of the unit sphere of l(h, k) under symplectic transformations. **Journal of Operator Theory**, Theta Foundation, v. 11, n. 1, p. 171–191, 1984. ISSN 03794024, 18417744.

ZHANG, J.; MATTHAIOU, M.; KARAGIANNIDIS, G.; DAI, L. On the multivariate gamma-gamma ($\gamma\gamma$) distribution with arbitrary correlation and applications in wireless communications. **IEEE Transactions Vehicular Technology**, v. 65, n. 5, p. 3834–3840, 2016. ISSN 0018-9545.

ZHANG, X.; ZHOU, X.; MCKAY, M. R.; HEATH, R. W. Artificial-noise-aided secure multi-antenna transmission in slow fading channels with limited feedback. In: **2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)**. 2014. p. 3968–3972. ISSN 1520-6149.