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

JAMIL DE ARAUJO FARHAT

ESQUEMAS DE COMUNICAÇÃO COOPERATIVA SEGURA CONSIDERANDO REGIMES PARCIAIS DE SEGURANÇA, MÚLTIPLAS ANTENAS E BLOCOS DE TAMANHO FINITO

TESE

CURITIBA
2018

JAMIL DE ARAUJO FARHAT

ESQUEMAS DE COMUNICAÇÃO COOPERATIVA SEGURA CONSIDERANDO REGIMES PARCIAIS DE SEGURANÇA, MÚLTIPLAS ANTENAS E BLOCOS DE TAMANHO FINITO

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 Ciências" – Área de Concentração: Telecomunicações e Redes.

Orientador: Prof. Dr. Glauber Gomes de Oliveira Brante

Coorientador: Prof. Dr. Richard Demo Souza

CURITIBA
2018

Dados Internacionais de Catalogação na Publicação

F223e
2018

Farhat, Jamil de Araujo
Esquemas de comunicação cooperativa segura considerando regimes parciais de segurança, múltiplas antenas e blocos de tamanho finito / Jamil de Araujo Farhat.-- 2018.
96 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. 90-96.

1. Energia - Consumo. 2. Sistemas de comunicação sem fio - Medidas de segurança. 3. Sistemas de transmissão de dados - Medidas de segurança. 4. Sistemas MIMO. 5. Códigos corretores de erros (Teoria da informação). 6. Redes de computação - Protocolos. 7. Análise numérica. 8. Métodos de simulação. 9. Engenharia elétrica - Teses. I. Brante, Glauber Gomes de Oliveira, 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 171

A Tese de Doutorado intitulada **"Esquemas de Comunicação Cooperativa Segura Considerando Regimes Parciais de Segurança, Múltiplas Antenas e Blocos de Tamanho Finito",** defendida em sessão pública pelo(a) candidato(a) **Jamil de Araujo Farhat**, no dia 12 de junho 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). Glauber Gomes de Oliveira Brante – Presidente – (UTFPR)
Prof(a). Dr(a). Hirley Alves – (Universidade de Oulu)
Prof(a). Dr(a). Taufik Abrão – (UEL)
Prof(a). Dr(a). João Luiz Rebelatto – (UTFPR)
Prof(a). Dr(a). Bruno Sens Chang – (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, 12 de junho de 2018.

AGRADECIMENTOS

Agradeço primeiramente à Deus, que me deu o dom da vida e me permitiu ter força e sabedoria para realização deste trabalho. Também agradeço a todos, que das mais variadas formas contribuíram para realização deste trabalho, em especial:

Aos meus pais, Sami Jamil Farhat e Dayse Regina de Araujo Farhat, e ao meu irmão, Nader de Araujo Farhat, por todo amor e confiança.

À minha futura esposa, Rayta Paim Horta, por todo amor, paciência e apoio em todos os momentos desde o dia que nos conhecemos;

Aos meus amigos e orientadores, Glauber Brante e Richard Souza, que sempre estiveram dispostos a me motivar, e me permitiram evoluir profissionalmente com ideias e orientações extremamente valiosas;

Aos amigos do Laboratório de Sistemas de Comunicações Sem Fio que auxiliaram no meu aprendizado com as discussões cientificas e conversas corriqueiras;

Aos meus amigos por toda paciência, confiança e apoio.

RESUMO

FARHAT, Jamil de Araujo. Esquemas de Comunicação Cooperativa Segura considerando Regimes Parciais de Segurança, Múltiplas Antenas e Blocos de Tamanho Finito. 96 f. Tese – Programa de Pós-graduação em Engenharia Elétrica e Informática Industrial, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

A crescente demanda por sistemas de comunicação sem fio torna a segurança da informação transmitida um importante aspecto a ser considerado no desenvolvimento de novos sistemas. Desta forma, nesta tese abordamos diferentes estudos da segurança na camada física considerando cenários com regimes parciais de segurança, múltiplas antenas e blocos de tamanho finito. Com relação aos regimes parciais de segurança, investiga-se a eficiência energética segura (SEE, do inglês *Secure Energy Efficiency*) de uma rede cooperativa nos quais os requisitos parciais de segurança são implementados através de um parâmetro de equivocação fracionário, $\theta \in (0, 1]$, que permite segurança parcial quando $\theta < 1$. Assume-se que somente a informação do estado do canal (CSI, do inglês *Channel State Information*) do canal legítimo está disponível, enquanto a CSI da escuta é desconhecida. Desta forma, propomos um esquema denominado *CSI-Aided Decode-and-Forward* (DF), em que o transmissor utiliza da CSI disponível do canal legítimo para escolha entre o caminho direto ou cooperativo. Além do mais, considera-se que o *relay* emprega Codificação de Repetição (CSI-RC), em que fonte e *relay* utilizam a mesma palavra-código, ou Codificação Paralela (CSI-PC), em que diferentes palavras-código são utilizadas. Para maximização da SEE, uma alocação conjunta de potência é proposta, utilizando o algoritmo Dinkelbach para alocação de potência, que também otimiza θ. Os esquemas propostos são comparados com o DF tradicional, *Amplify-and-Forward* (AF) e *Cooperative Jamming* (CJ). Estendendo a análise anterior, estuda-se a SEE para cenários cooperativos em que todos os nós são equipados com múltiplas antenas. É proposta uma alocação conjunta da taxa de confidencialidade e da alocação de potência em Alice e no *relay* de modo a maximizar a SEE sujeita a um limite em termos da mínima probabilidade de *outage* de segurança necessária. Considerando este cenário MIMO (do inglês, *Multiple-Input Multiple-Output*) em que apenas a CSI do canal principal é conhecida por Alice, o esquema *Artificial-Noise* (AN) é comparado com o esquema *CSI-Aided Decode-and-Forward*. Por fim, considerando um cenário mais restritivo em relação à CSI, porém mais realista, em que a CSI de nenhum dos canais é conhecida, o *throughput* seguro é investigado em um cenário com atraso crítico, típico em comunicações *machine-to-machine*, no qual os usuários se comunicam com blocos de transmissão de tamanho finito. Nesta abordagem, o desempenho da comunicação direta é comparada com o protocolo cooperativo *Selective Decode-and-Forward* (SDF).

Palavras-chave: Segurança na camada física, Comunicação cooperativa, Eficiência energética, Múltiplas antenas, Blocos de tamanho finito

ABSTRACT

FARHAT, Jamil de Araujo. Cooperative Secure Communication Schemes considering Partial Secrecy Regimes, Multiple Antennas and Finite Blocklengths. 96 f. Tese – Programa de Pós-graduação em Engenharia Elétrica e Informática Industrial, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

The growing demand for wireless communications systems makes security an important and difficult design task. Therefore, in this thesis we approached different studies at physical layer security considering different scenarios of partial secrecy requirements, multiple antennas and finite blocklenghts. With respect to the partial secrecy regime, we evaluate the secure energy efficiency (SEE) of a cooperative network subject to partial secrecy requirements, implemented through a fractional equivocation parameter $\theta \in (0, 1]$ that allows partial secrecy when $\theta < 1$. We assume that only the channel state information (CSI) of the legitimate channel is available, while the CSI with respect to the eavesdropper is unknown. Then, we propose a CSI-Aided Decode-and-Forward (DF) scheme, in which the transmitter uses the available CSI in order to choose between direct and cooperative paths. Moreover, the relay employs either Repetition Coding (CSI-RC), *i.e.*, source and relay use the same codebook, or Parallel Coding (CSI-PC), when different codebooks are used. By resorting to the Dinkelbach algorithm, we propose a joint power allocation scheme, which also optimizes θ to maximize the SEE. Our schemes are compared with the traditional DF, Amplify-and-Forward (AF), and Cooperative Jamming (CJ). Extending the previous analysis, we also study the SEE in a cooperative scenario where all nodes are equipped with multiple antennas. Moreover, we employ secrecy rate and power allocation at Alice and at the relay in order to maximize the SEE, subjected to a constraint in terms of a minimal required secrecy outage probability. Considering this MIMO scenario in which only the CSI with respect to the legitimate nodes is available at Alice, we compare the Artificial-Noise (AN) scheme with CSI-Aided Decode-and-Forward (CSI-DF). Lastly, considering a more restrictive scenario with respect to the CSI, but more realistic, in which the legitimate transmitter has no knowledge of the instantaneous channel state information with respect to neither the legitimate receiver nor the eavesdropper, we investigate the secure throughput in a delay-critical scenario, such as in some applications of machine-to-machine communications, so that users communicate with a finite blocklength. In this approach, the performance of direct and selective decode-and-forward cooperative communication strategies are compared.

Keywords: Physical layer security, Cooperative communications, Energy Efficiency, MIMO, Finite blocklength

LISTA DE FIGURAS

LISTA DE SIGLAS

AF	*Amplify-and-Forward*
AN	*Artificial-Noise*
AWGN	*Additive White Gaussian Noise*
CDF	*Cumulative Distribution Function*
CDI	*Channel Direction Information*
CGI	*Channel Gain Information*
CJ	*Cooperative Jamming*
CSI-DF	*CSI-aided Decode-and-Forward*
CSI-PC	*CSI-Aided with Parallel Coding*
CSI-RC	*CSI-Aided with Repetition Coding*
CSI	*Channel State Information*
DF	*Decode-and-Forward*
HARQ	*Hybrid Automatic Retransmission Request*
IoT	*Internet of Things*
M2M	*Machine-to-Machine*
MIMO	*Multiple-Input Multiple-Output*
MISOSE	*Multiple-Input Single-Output Single-Antenna Eavesdropper*
mmWave	*Millimeter Wave*
MRC	*Maximal Ratio Combining*
NLOS	*Non Line-Of-Sight*
NOMA	*Non-Orthogonal Multiple Access*
PAR	*Peak-to-Average Ratio*
PDF	*Probability Density Function*
SC	*Selection Combining*
SDF	*Selective Decode-and-Forward*
SEE	*Secure Energy Efficiency*
SIR	*Signal-to-Interference Ratio*
SNR	*Signal-to-Noise Ratio*
SOP	*Secrecy Outage Probability*
TAS	*Transmit Antenna Selection*
VA	Variável Aleatória

LISTA DE SÍMBOLOS

θ	Parâmetro de equivocação fracionária
P_i	Potência de transmissão
$\mathbf{x}_i$	Vetor de dados transmitido
$\mathbf{w}_j$	Ruído aditivo Gaussiano branco
N_0	Densidade espectral de potência unilateral do ruído térmico
h_{ij}	Coeficiente de desvanecimento no enlace *i*-*j*
κ_{ij}	Perda de percurso entre os nós i e j
G	Ganho total das antenas de transmissão e recepção
f_c	Frequência de portadora
c	Velocidade da luz no vácuo
υ	Expoente de perda de percurso
M_l	Margem de enlace
N_f	Figura de ruído no receptor
d_{ij}	Distância entre os nós *i*-*j*
γ_{ij}	SNR instantânea
$\bar{\gamma}_{ij}$	SNR média
N	Potência de ruído
B	Largura de banda
C_s	Capacidade de confidencialidade
C_L	Capacidade do canal legítimo
C_E	Capacidade do canal de Eve
$\mathcal{R}$	Taxa de comunicação segura
$\mathcal{R}_\mathrm{E}$	Taxa de equívoco
$\mathcal{R}_\mathrm{B}$	Taxa de transmissão de palavras-código
Δ	Limite inferior da equivocação fracionária
$p_\mathrm{gso}^{(\mathrm{esq})}$	Probabilidade generalizada da *outage* de segurança
η_s	Eficiência energética segura
τ_s	*Throughput* seguro
P_total	Potência total
${}_2F_1\left(.,.;.;.\right)$	Função hipergeométrica de Gauss
P_TX	Potência gasta no circuito de transmissão
P_RX	Potência gasta no circuito de recepção
ω	Energia adicional do amplificador de potência
n_A	Número de antenas em Alice
n_B	Número de antenas em Bob
n_R	Número de antenas no *relay*
n_E	Número de antenas em Eve
$\Gamma(.)$	Função gamma completa
$\hat{\gamma}(.)$	Função gamma incompleta
$\Psi(.,.,.)$	Função hipergeométrica confluente de Tricomi
n	Tamanho da palavra-código

ϵ	Probabilidade de erro de pacote
C	Capacidade ergódica do canal
V	Dispersão do canal
k_{B}	Total de bits transmitidos por Alice em cada *frame*
k_{S}	Total de bits transmitidos de maneira segura em cada *frame*
k_{E}	Total de bits relacionados ao custo da transmissão segura

SUMÁRIO

1 INTRODUÇÃO

A crescente demanda por sistemas de comunicação sem fio torna a segurança da informação transmitida um importante aspecto a ser considerado no desenvolvimento de novos sistemas. A partir dos recentes avanços tecnológicos, a criptografia, baseada na capacidade computacional da escuta, pode necessitar de melhorias e complementos, sendo a segurança na camada física uma alternativa (SHANNON, 1949; BLOCH; BARROS, 2011; BLOCH et al., 2008). A segurança na camada física explora as flutuações do canal sem fio para permitir uma comunicação segura entre um par de usuários legítimos, denominados Alice e Bob, que se comunicam na presença de uma escuta, denominada Eve, que tenta obter algum tipo de informação da rede (WYNER, 1975). O princípio básico da segurança na camada física foi introduzido por (WYNER, 1975) com o modelo do canal de escuta (do inglês, *wiretap channel*). Neste modelo Eve recebe uma versão degradada da informação transmitida entre Alice e Bob, o que acaba tornando a comunicação segura possível. Além de necessitar de menor esforço computacional, a segurança na camada física também permite quantificar a confidencialidade do canal de uma maneira tangível (BLOCH; BARROS, 2011; BLOCH et al., 2008).

As grandezas utilizadas para determinação da confidencialidade destes sistemas estão usualmente relacionadas ao nível de informação do estado do canal (CSI, do inglês *Channel State Information*) disponível a Alice. Considerando conhecimento global da CSI disponível a Alice, a confidencialidade perfeita é obtida adaptando a taxa de comunicação segura, de modo que possamos ter uma comunicação confiável entre Alice e Bob com a informação não ficando disponível a Eve (BLOCH et al., 2008). O código responsável por garantir esta probabilidade mínima de erro para transmissão entre Alice e Bob, além de manter a confidencialidade da informação em relação à Eve é denominado código de escuta (do inglês, *wiretap code*). A medida de confidencialidade associada com este cenário é a capacidade de confidencialidade (do inglês, *secrecy capacity*), considerada, por exemplo, em (GOPALA et al., 2008; LI et al., 2011; DING et al., 2012). Contudo, esta suposição necessita que Alice tenha informação da CSI de Eve, o que normalmente não ocorre porque Eve é uma escuta passiva que apenas tenta interceptar as informações transmitidas entre os nós legítimos.

Desta forma, supondo uma abordagem mais realista em que apenas a CSI do canal legítimo está disponível a Alice, não é possível definir diretamente a capacidade de confidencialidade do sistema. Neste caso uma análise probabilística da

confidencialidade da informação deve ser realizada, definindo a probabilidade de que a taxa de confidencialidade escolhida seja maior que a capacidade de confidencialidade do sistema. Esta análise, denominada como probabilidade de *outage* de segurança (do inglês, *secrecy outage probability*) é considerada, por exemplo, em (GABRY et al., 2011b; VILELA et al., 2011; ZHENG et al., 2015). Por fim, outro possível cenário ocorre quando Alice não tem conhecimento algum da CSI. Desta forma, além da análise probabilística da informação estar disponível a Eve, também é necessário determinar a probabilidade de ocorrer uma transmissão confiável entre Alice e Bob. Portanto, a probabilidade de *outage* de segurança é definida pela união de dois eventos independentes: Bob não decodificar corretamente a mensagem transmitida por Alice e a capacidade instantânea do canal de Eve estar acima da taxa de equívoco do código de escuta em uso. Este cenário sem nenhuma CSI disponível à Alice é considerado em (TANG et al., 2009; BRANTE et al., 2015; LIU et al., 2015).

Uma forma de aprimorar a segurança do canal na presença de uma escuta está relacionada com a utilização da característica de radiodifusão do meio sem fio, que permite o uso da comunicação cooperativa (LANEMAN et al., 2004). O cenário cooperativo é baseado no modelo de canal chamado *relay*, proposto por (MEULEN, 1971). Este modelo é constituído por três nós: Alice, *relay* e Bob. Nesta estratégia, Alice e *relay* atuam como parceiros, com o *relay* auxiliando Alice a encaminhar a informação até Bob. Estudos iniciais sobre a capacidade de confidencialidade em esquemas cooperativos podem ser encontrados em (LAI; GAMAL, 2008; DONG et al., 2010), enquanto estudos mais recentes ainda demonstram os benefícios das técnicas cooperativas em aprimorar a segurança do sistema (WANG et al., 2014; ZOU et al., 2015), especialmente em cenários compostos de múltiplos nós, como rede de sensores sem fio e *multicasting*. Alguns esquemas cooperativos tradicionais empregados no contexto de segurança na camada física são o *Decode-and-Forward* (DF), o *Amplify-and-Forward* (AF) e o *Cooperative Jamming* (CJ). Em (GABRY et al., 2011b, 2011a; CHEN et al., 2015), os autores comparam estes protocolos para diferentes posições de Eve, concluindo que o esquema AF apresenta um melhor desempenho em grande parte dos casos, exceto quando Eve está bem próxima aos nós legítimos, quando o protocolo CJ é mais vantajoso. Já em (WANG et al., 2015b) os autores exploram a CSI disponível do canal legítimo para realizar cooperação via *beamforming* e *jamming* em um cenário com múltiplos *relays*. Similarmente, em (DENG et al., 2015), a CSI disponível é utilizada pelo *relay* para decisão sobre cooperar ou injetar ruído com o intuito de aumentar a segurança do sistema.

Outra estratégia para aumentar a confidencialidade do sistema está relacionada

à utilização de múltiplas antenas (MIMO, do inglês *Multiple-Input Multiple-Output*) nos nós do sistema (ALVES et al., 2012; YANG et al., 2013, 2013, 2015). Em (ALVES et al., 2012) os autores estudam o protocolo de seleção de antenas de transmissão (TAS, do inglês *Transmit Antenna Selection*) no transmissor legítimo, que possibilita melhorar o desempenho da probabilidade de *outage* de segurança com um baixo custo, complexidade e consumo de potência em comparação com outras estratégias MIMO. Com relação a outras estratégias, outras combinações, como por exemplo, TAS com combinação de razão máxima (MRC, do inglês *Maximal Ratio Combining*) ou combinação de seleção (SC, do inglês *Selection Combining*) no receptor legítimo e na escuta são investigados em (YANG et al., 2013, 2013, 2015). Com relação ao TAS, visto que apenas o índice da antena com melhor condição do canal é retroalimentada a Alice, os autores em (ALVES et al., 2012) demonstram que a diversidade é incrementada com respeito a Bob, mas não com relação a Eve, o que implica em um aumento da confidencialidade. Já em Bob, conforme (YANG et al., 2013), a estratégia ótima em termos de confidencialidade é o MRC.

Considerando a utilização conjunta da comunicação cooperativa e múltiplas antenas, dois métodos cooperativos tipicamente empregados são os esquemas DF e o *Artificial-Noise* (AN). O protocolo DF combinado com TAS foi analisado, por exemplo, em (LIN et al., 2016) considerando um cenário de informação de CSI desatualizada em Alice. Os autores mostram que um aumento no número de antenas nos nós legítimos reduz significativamente a probabilidade de *outage* de segurança, mesmo considerando o cenário de CSI desatualizada. Recentemente, a SOP (do inglês, *Secrecy Outage Probability*) do esquema AN foi investigada por (COSTA et al., 2016); já a métrica da SEE (do inglês, *Secure Energy Efficiency*) foi empregada em (HU et al., 2016c; FARHAT et al., 2016), nos quais o esquema AN demonstra uma possibilidade de aperfeiçoar a SEE e a SOP em comparação com esquemas não cooperativos (HU et al., 2016c). Adicionalmente, as estratégias de retransmissão e *jamming* por nós *relays*, utilizando o esquema AN, contra múltiplos *eavesdroppers* são estudados em (HUI et al., 2015).

Uma maneira usualmente empregada para aumentar o desempenho destes sistemas está relacionada à alocação de potência em Alice e no *relay*. A alocação de potência consiste na escolha da potência ótima que permita maximizar uma função de interesse. Sobre a alocação de potência, (CHORTI et al., 2015) propõe um esquema de alocação de potência para um cenário *block fading* não cooperativo, com diferentes considerações com relação ao *feedback* da CSI. Considerando cenários cooperativos, uma extensão de (GABRY et al., 2011b) é dada por (GABRY et al., 2011a), em que um esquema ótimo de alocação de potência é proposto para minimizar a probabilidade

de *outage* de segurança dos protocolos DF e CJ. Contudo, as abordagens propostas por (GABRY et al., 2011a; CHORTI et al., 2015) são complexas, já que uma busca exaustiva é empregada para obter as potências ótimas a serem alocadas.

Uma maneira iterativa e distribuída para realizar alocação de potência é obtida a partir do algoritmo Dinkelbach (DINKELBACH, 1967), o qual foi desenvolvido para otimizar a razão entre funções de mesma variável, tornando-se especialmente útil quando a eficiência energética é a métrica de interesse (ZAPPONE; JORSWIECK, 2014). Por exemplo, (BRANTE et al., 2013; WANG et al., 2015a; ZAPPONE et al., 2014; FARHAT et al., 2015) empregam algoritmos baseados no algoritmo Dinkelbach para maximizar métricas relacionadas à eficiência energética. Em (BRANTE et al., 2013) os autores maximizam a eficiência energética em sistemas MIMO, obtendo resultados similares em comparação com a abordagem de busca exaustiva, porém com uma complexidade reduzida. Recentemente, (WANG et al., 2015a) analisa a SEE em um cenário com múltiplos *relays* operando com o protocolo DF, em que um subconjunto de *relays* que decodificam corretamente a mensagem de Alice cooperam em um segundo *slot* de tempo. Adicionalmente, (ZAPPONE et al., 2014) estuda alocação de recursos para maximizar a SEE em um cenário com múltiplas antenas no transmissor legítimo com diferentes cenários de CSI. Finalmente, em (FARHAT et al., 2015) nós maximizamos a SEE de um esquema *CSI-Aided*, em que Alice explora a CSI disponível do canal legítimo para escolher o melhor caminho para se comunicar com Bob, diretamente ou com auxílio do *relay*.

Contudo, as métricas tradicionais de capacidade citadas anteriormente são caracterizadas em um regime assintótico em que o tamanho do bloco tende a infinito. A quinta geração (5G) de sistemas de comunicação sem fio deverá suportar novos tipos de tráfegos de comunicação, os quais podem empregar tamanhos de blocos relativamente curtos de forma a cumprir restrições severas de latência, como, por exemplo, em comunicações *machine-to-machine* (M2M) (DURISI et al., 2016). Nestes cenários as métricas tradicionais de capacidade não podem ser diretamente aplicados para análise e desenvolvimento de esquemas de segurança na camada física. Estudos tutoriais do impacto dos blocos de tamanho finito podem ser encontrados em (DURISI et al., 2016), enquanto em (YANG et al., 2012) a formulação da teoria da informação para limites de desempenho sob blocos finitos em canais *block-fading* Rayleigh é discutida. Nestes cenários, o sistema deve ser caracterizado em termos da máxima taxa atingível, representado por $R^{\star}(n,\epsilon)$, a qual depende do tamanho do bloco ou palavra-código (n) e da probabilidade de erro de pacote associada (ϵ). Adicionalmente, em (YANG et al., 2012), os autores demonstram que $R^{\star}(n,\epsilon)$ não é monotônica com relação ao tempo de coerência do canal, de forma que

existe um tempo de coerência que permite maximizar $R^{\star}(n,\epsilon)$ mantendo uma relação ótima entre diversidade e custo de estimativa do canal. Com relação aos cenários cooperativos, os autores em (HU et al., 2016a) analisam a probabilidade de erro de pacote para blocos de tamanhos finitos considerando o protocolo DF em um cenário *single-hop*, enquanto uma rede cooperativa *multi-hop* é considerada em (DU et al., 2016). Também em (DU et al., 2016), uma comparação entre sistemas com blocos de tamanhos finitos e infinitos é realizada, demonstrando que o número ótimo de saltos que maximizam o *throughput* são diferentes considerando estas duas suposições. Com relação às métricas de capacidade de confidencialidade, os limites para máxima taxa de confidencialidade em canais *block-fading* são obtidos em (YANG et al., 2013). Considerando canais *wiretap*, os autores em (CAO et al., 2015) analisam o *trade-off* entre confidencialidade e confiabilidade no cenário com blocos de tamanho finito, fornecendo expressões para o desempenho de segurança para diferentes canais. Em (YANG et al., 2016) os autores mostram que, similarmente à análise com blocos de tamanhos infinitos, a capacidade de segurança para blocos de tamanhos finitos também é formulada pela diferença entre a capacidade do canal legítimo e da escuta. Além disso, um limite superior para $R_s^{\star}(n,\epsilon,\delta)$ é desenvolvido, o qual determina a máxima taxa de confidencialidade, dada uma probabilidade de erro de vazamento, δ, com relação à Eve.

1.1 OBJETIVOS

Este trabalho tem como objetivo realizar uma investigação sobre diferentes aspectos da confidencialidade em sistemas cooperativos com a presença de dois usuários legítimos, Alice e Bob, comunicando-se com auxílio de um nó *relay*, na presença de um espião passivo. Nesta tese abordaremos diversos estudos recentes relacionados à probabilidade generalizada de *outage* de segurança, à utilização de múltiplas antenas e aos cenários em que a comunicação ocorre com blocos de tamanho finito.

Com relação à probabilidade generalizada de *outage* de segurança, estamos particularmente interessados no caso onde Alice tem CSI perfeita apenas do canal legítimo. A partir deste conhecimento, propomos um esquema denominado CSI-*Aided Decode-and-Forward* que utiliza da CSI disponível para escolha do melhor tipo de comunicação entre Alice e Bob (comunicação direta ou cooperativa). Além do mais, consideramos que o *relay* emprega Codificação de Repetição, em que fonte e *relay* utilizam a mesma palavra-código, ou Codificação Paralela, em que diferentes palavras-código são utilizadas. Desta forma, os esquemas propostos serão comparados com o DF tradicional, o AF e o CJ. Por fim,

visando a maximização da SEE, uma alocação conjunta de potência e θ será proposta.

Com relação à utilização de múltiplas antenas, é investigada a SEE para cenários cooperativos em que todos os nós são equipados com múltiplas antenas. Considerando o cenário de CSI em que apenas a informação do estado do canal principal é conhecida por Alice, o esquema AN é comparado com o esquema CSI-DF. Visando a maximização da SEE, uma alocação conjunta da taxa de confidencialidade e da alocação de potência em Alice e no *relay*, sujeita a um limite em termos da mínima probabilidade de *outage* de segurança necessária, é proposta.

Por fim, com relação aos blocos de tamanhos finitos, é analisado um cenário restritivo de CSI em que a informação tanto do canal legítimo quanto da escuta são desconhecidas. Desta forma, é realizada uma análise comparativa entre o desempenho da comunicação direta e do protocolo cooperativo SDF a partir do *throughput* seguro.

1.2 ESTRUTURA DO DOCUMENTO

O restante do documento está organizado da seguinte forma. O Capítulo 2 apresenta uma fundamentação teórica de diversos conceitos básicos relacionados à transmissão digital no canal sem fio, à comunicação cooperativa e à segurança na camada física.

Já no Capítulo 3 é apresentada uma formulação generalizada da probabilidade de *outage* de segurança, cuja representação é dada pela probabilidade da equivocação em Eve, Δ, não ser menor que um valor especificado de $\theta \in (0, 1]$, que representa um valor mínimo aceitável de equivocação. Considerando esta métrica generalizada, será estudado o comportamento de diferentes esquemas cooperativos a partir do relaxamento da segurança, por um ajuste adequado de θ. Além disto, a partir da métrica de eficiência energética segura, será demonstrado o método de alocação conjunta utilizada para otimização da potência, pelo algoritmo Dinkelbach, e otimização de θ.

Na sequência, estendendo o trabalho anterior, o Capítulo 4 considera cenários MIMO cooperativos em que Alice emprega TAS, enquanto Bob e Eve empregam MRC. Além do mais, o nó *relay* emprega *jamming*, a partir do projeto de um vetor *beamforming* que permite ao esquema AN interferir em Eve sem interferir em Bob, ou cooperação utilizando o protocolo CSI-*aided* DF (CSI-DF), no qual os nós legítimos utilizam da CSI disponível para escolha entre o melhor caminho: direto ou cooperativo. Para estes esquemas cooperativos, uma alocação de potência e taxa será empregada de forma a

maximizar a SEE, sujeita a requisitos mínimos com relação à máxima SOP.

Já no Capítulo 5, analisamos cenários cooperativos considerando blocos de tamanhos finitos. Em particular assumimos um cenário crítico com relação ao atraso, típico de aplicações M2M. Desta forma, comparamos as técnicas de transmissão direta e cooperativa, a partir do emprego do protocolo DF seletivo (SDF). Adicionalmente, assumimos nenhum conhecimento de CSI em Alice, tanto com relação a Bob quanto a Eve, de forma que a métrica do *throughput* seguro, neste caso, é dado pela união de dois eventos independentes: pela probabilidade de erro de pacote em Bob e probabilidade de vazamento de informação à Eve.

Por fim, o Capítulo 6 conclui o documento com comentários e considerações finais.

Listamos abaixo as publicações obtidas relacionadas com o tema desta tese:

1. J. Farhat, G. Brante, R. D. Souza and J. L. Rebelatto, "*Secure energy efficiency of selective decode and forward with distributed power allocation*,"**2015 International Symposium on Wireless Communication Systems (ISWCS)**, Bruxelas, pp. 701-705, 25-28 Agosto, 2015.

2. J. Farhat, G. Brante, R. D. Souza and J. L. Rebelatto, "*Energy Efficiency of Repetition Coding and Parallel Coding Relaying Under Partial Secrecy Regime*", **IEEE Access**, vol. 4, pp. 7275-7288, 2016.

3. J. Farhat, G. Brante and R. D. Souza, "*On the Secure Energy Efficiency of TAS/MRC With Relaying and Jamming Strategies*", **IEEE Signal Processing Letters**, vol. 24, no. 8, pp. 1228-1232, Agosto, 2017.

4. J. Farhat, G. Brante and R. D. Souza. "*Secure Throughput Optimization of Selective Decode-and-Forward with Finite Blocklength*", **IEEE 87th Vehicular Technology Conference (VTC)**, Porto, 3-6 Junho, 2018.

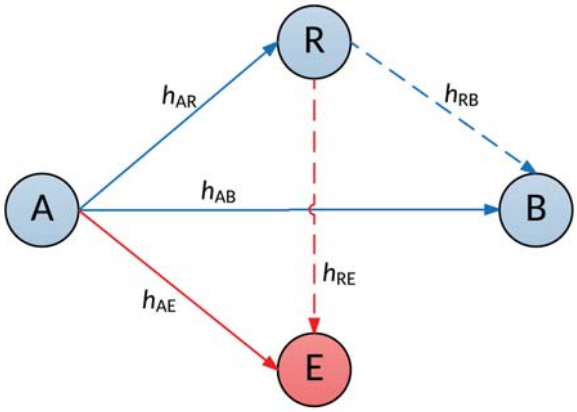
2 CONCEITOS BÁSICOS

Neste capítulo apresentamos os conceitos básicos relacionados ao modelo de sistema da transmissão segura no canal sem fio, à confidencialidade e aos protocolos de comunicação cooperativa. O objetivo é abordar de maneira sucinta os fundamentos que serão empregados nos estudos realizados a partir dos próximos capítulos.

2.1 MODELO DE SISTEMA DA COMUNICAÇÃO SEGURA

Consideraremos três usuários legítimos, Alice (A), *relay* (R) e Bob (B) se comunicando na presença de uma escuta, Eve (E), como mostrado na Figura 1.

Figura 1 – A comunicação ocorre na presença de uma escuta e os nós legítimos são auxiliados por um nó *relay*.



Fonte: Autoria própria.

O bloco de informação recebido por qualquer antena receptora do nó $j \in \{\mathrm{R}, \mathrm{B}, \mathrm{E}\}$ da transmissão de $i \in \{\mathrm{A}, \mathrm{R}\}$, com $i \neq j$, é representado por

$$\mathbf{y}_{ij} = \sqrt{\kappa_{ij} P_i}\, h_{ij}\, \mathbf{x}_i + \mathbf{w}_j, \tag{1}$$

onde P_i é a potência de transmissão e $\mathbf{x}_i$ é o bloco de dados transmitido com energia unitária. Além disto, $\mathbf{w}_j$ é o ruído aditivo Gaussiano branco (AWGN, do inglês *Additive White Gaussian Noise*) de média zero com variância $N_0/2$ por dimensão e h_{ij} representa a realização quase-estática do canal, com elementos Gaussianos complexos distribuídos com média nula e variância unitária. Desta forma, o desvanecimento do canal, representado por $|h_{ij}|$, é descrito estatisticamente por uma função densidade de probabilidade (PDF, do inglês *Probability Density Function*) Rayleigh.

Além do mais, κ_{ij} representa a perda de percurso entre i e j, e é dado por (GOLDSMITH, 2005)

$$\kappa_{ij} = \frac{G}{(4\pi f_c/c)^2 \, d_{ij}^{\upsilon} \, M_l \, N_f}, \tag{2}$$

onde G é o ganho total das antenas transmissoras e receptoras, f_c é a frequência de portadora, c é a velocidade da luz no vácuo, υ é o expoente de perda de percurso, M_l é a margem de enlace, N_f é a figura de ruído no receptor e d_{ij} é a distância entre os nós de transmissão e recepção. Além disto, assumimos comunicação *half-duplex* entre os nós com transmissões ortogonais no tempo.

A SNR instantânea no receptor, que representa a relação entre o nível do sinal recebido e o ruído, dada por γ_{ij}, em qualquer enlace entre i e j pode ser definida como

$$\gamma_{ij} = |h_{ij}|^2 \, \bar{\gamma}_{ij}, \tag{3}$$

onde $\bar{\gamma}_{ij} = (\kappa_{ij} P_i)/N$ é a SNR média, $N = N_0 B$ é a potência de ruído, com N_0 representando a densidade espectral de potência unilateral do ruído térmico e B a largura de banda do sistema.

Um dos modelos mais utilizados para descrever o comportamento de propagação de sinais em casos em que não há linha de visada (NLOS) entre o transmissor e o receptor, comum em grande parte das redes de transmissão sem fio, é a distribuição Rayleigh (GOLDSMITH, 2005). Considerando que o canal sem fio segue esta distribuição, a variável aleatória γ_{ij}, que é função de $|h_{ij}|^2$, apresenta distribuição exponencial com média $\overline{\gamma}_{ij}$ e PDF definida, conforme (PROAKIS; SALEHI, 2008), por:

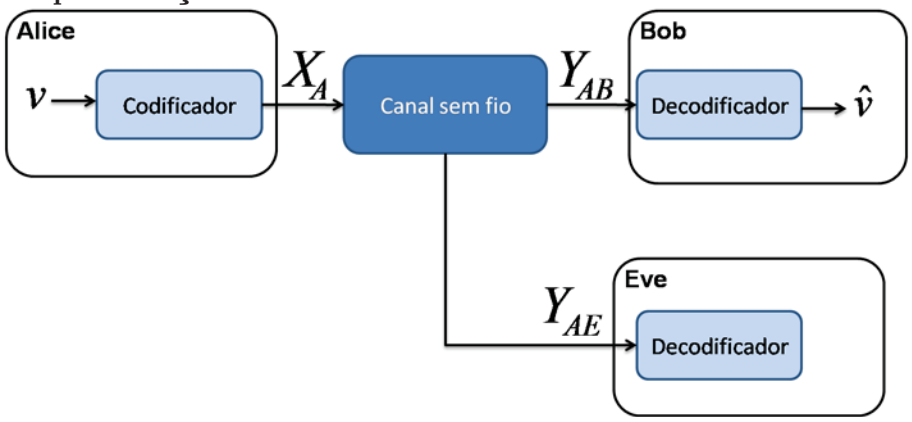
$$f_{\gamma}(\gamma_{ij}) = \begin{cases} \frac{1}{\overline{\gamma}_{ij}} \mathrm{e}^{-\frac{\gamma_{ij}}{\overline{\gamma}_{ij}}}, & \text{se } \gamma_{ij} \geq 0 \\ 0, & \text{se } \gamma_{ij} < 0 \end{cases} \tag{4}$$

2.2 SEGURANÇA NA CAMADA FÍSICA

A confidencialidade em um sistema de comunicação sem fio refere-se à capacidade de um canal permitir a transmissão de informações entre Alice até Bob sem que esta informação seja decodificada por Eve. A segurança da informação na camada física foi introduzida por (WYNER, 1975), a partir do modelo do canal de escuta, representado na Figura 2.

A partir da figura, vemos que Alice codifica a mensagem v em um bloco de

Figura 2 – Representação do modelo do canal de escuta.



Fonte: Autoria Própria

dados de transmissão X_{A}, que é enviado por um canal com ruído. Eve observa uma versão ruidosa, Y_{AE}, do sinal disponível a Bob, Y_{AB}. Neste modelo duas medidas podem ser caracterizadas: a confidencialidade e a confiabilidade. A confidencialidade está relacionada ao nível de confusão de Eve sobre a mensagem v, dada a observação do sinal Y_{AE}. Já a confiabilidade está relacionada à probabilidade da mensagem decodificada por Bob, $\hat{v}$, ser diferente da mensagem originalmente transmitida por Alice, v.

Além do modelo do canal de escuta, os autores em (WYNER, 1975) também definem o código de escuta, código responsável por possibilitar a transmissão de mensagens de maneira segura entre os nós legítimos do sistema, e o *trade-off* existente entre a taxa de informação pretendida por Alice e o nível de ignorância em Eve. Para o código de escuta, dois parâmetros de taxa devem ser definidos: a taxa de transmissão das palavras-códigos, $\mathcal{R}_{\mathrm{B}} = \mathrm{H}(X_{\mathrm{A}})/n$, e a taxa de informação confidencial, $\mathcal{R} = \mathrm{H}(v)/n$, onde H(.) representa a entropia da informação. A diferença positiva entre as taxas, $\mathcal{R}_{\mathrm{E}} = \mathcal{R}_{\mathrm{B}} - \mathcal{R}$, define o custo da segurança contra Eve. Conforme (HE, 2016), um código de escuta de tamanho n é construído gerando $2^{n\mathcal{R}_{\mathrm{B}}}$ palavras-códigos $x_{\mathrm{A}}^{n}(w,v)$ de tamanho n, onde $w = 1,2,\ldots,2^{n\mathcal{R}}$ e $v = 1,2,\ldots,2^{n(\mathcal{R}_{\mathrm{B}}-\mathcal{R})}$. Para cada mensagem com índice w, uma mensagem v com probabilidade uniforme é selecionada aleatoriamente, de modo que $x_{\mathrm{A}}^{n}(w,v)$ é transmitida.

Uma grandeza fundamental da confidencialidade de um canal é a capacidade de confidencialidade. Esta medida determina a máxima taxa com que Alice e Bob podem se comunicar de maneira confiável, sem que tal informação possa ser decodificada por Eve. Tal grandeza, C_{s}, é determinada pela diferença entre as capacidades do canal legítimo, C_{L}, e do canal da escuta, C_{E}. Portanto, a capacidade de confidencialidade

é dada por (BLOCH; BARROS, 2011; CSISZAR; KORNER, 1978)

$$C_{\mathrm{s}} = C_{\mathrm{L}} - C_{\mathrm{E}}. \tag{5}$$

Já as capacidades C_{L} e C_{E} podem ser definidas, considerando canais e entradas Gaussianas, por (SHANNON, 1949)

$$\begin{aligned} C_{\mathrm{L}} &= B \cdot \log_2(1+\gamma_{\mathrm{L}}) \\ C_{\mathrm{E}} &= B \cdot \log_2(1+\gamma_{\mathrm{E}}) \end{aligned} \tag{6}$$

onde γ_i, com $i \in \{\mathrm{L}, \mathrm{E}\}$ é a SNR instantânea do canal legítimo e de escuta, respectivamente. No restante do documento é considerado que a capacidade do sistema está normalizada em relação à largura de banda.

A medida da capacidade de confidencialidade está relacionada com o conhecimento global da CSI por Alice. Se assumimos que o comportamento de ambos os canais, legítimo e de escuta, são conhecidos, é possível desenvolver um código de escuta de modo que Eve nunca consiga decodificar a palavra-código. Desta forma, a taxa de comunicação segura é dada por $\mathcal{R}= C_{\mathrm{L}} - C_{\mathrm{E}}$ sendo que a confidencialidade perfeita é obtida apenas adaptando a taxa do código de escuta (BLOCH et al., 2008). Porém, considerando o caso em que apenas o comportamento do canal legítimo seja conhecido, a confidencialidade perfeita não pode ser garantida, já que o comportamento do canal de Eve é desconhecido. Neste caso, é necessário estabelecer um código de escuta de taxa $\mathcal{R} = C_{\mathrm{L}} - \mathcal{R}_{\mathrm{E}}$, na qual C_{L} é igual à capacidade do canal legítimo e $\mathcal{R}_{\mathrm{E}}$ representa uma taxa de equívoco estimada para Eve. Desta forma, um evento de falha é definido pelo evento da capacidade do canal de Eve, C_{E}, exceder a taxa de equívoco, $\mathcal{R}_{\mathrm{E}}$, sendo equivalente à situação da capacidade de confidencialidade do canal ser menor que a taxa $\mathcal{R}$. A probabilidade deste evento é denominada probabilidade de *outage* de segurança e é definida como (BLOCH; BARROS, 2011)

$$p_{\mathrm{out}} = \Pr\{C_{\mathrm{s}} < \mathcal{R}\}. \tag{7}$$

Outro caso possível, considerado em (TANG et al., 2007, 2009; BRANTE et al., 2015), é que não esteja disponível ao transmissor o conhecimento instantâneo de nenhum dos dois canais, tanto do legítimo como da escuta. Neste cenário, como C_L também não é conhecida, deve-se estabelecer uma taxa de comunicação segura fixa dada por $\mathcal{R} = \mathcal{R}_{\mathrm{B}} - \mathcal{R}_{\mathrm{E}}$, onde $\mathcal{R}_{\mathrm{B}}$ e $\mathcal{R}_{\mathrm{E}}$ são taxas escolhidas para o canal legítimo e de Eve, respectivamente. Para este cenário, uma falha ocorre quando $\mathcal{R}_{\mathrm{B}}$ supera C_L ou

quando C_E supera $\mathcal{R}_{\mathrm{E}}$. Neste caso, a probabilidade de *outage* de segurança é definida pela união de dois eventos independentes: a probabilidade do receptor legítimo não conseguir decodificar a mensagem transmitida, definida como evento de falha de confiabilidade, e a probabilidade da capacidade instantânea do canal de Eve superar a taxa de equívoco do código de escuta utilizado, definida como evento de falha de confidencialidade.

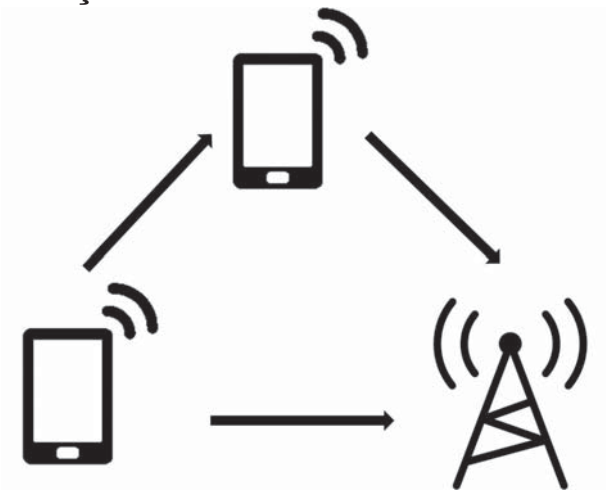
2.3 ESQUEMAS DE TRANSMISSÃO COOPERATIVOS

Uma maneira eficiente de combater os efeitos do desvanecimento no canal sem fio é a utilização de técnicas que proporcionem caminhos independentes para transmissão do sinal, ou seja, exploração da diversidade. A principal ideia nesta estratégia está relacionada ao fato de que existe uma probabilidade baixa que caminhos independentes apresentem desvanecimentos rigorosos no mesmo instante de tempo (GOLDSMITH, 2005). Um modo de se obter este ganho de diversidade espacial é a comunicação cooperativa, na qual o ganho ocorre a partir do compartilhamento de recursos entre nós distintos (LANEMAN et al., 2004).

Utilizando a estratégia de comunicação cooperativa, exemplificada na Figura 3, o *relay* auxilia Alice a encaminhar a informação até Bob. No decorrer deste documento alguns protocolos cooperativos clássicos serão considerados, os quais fazem uso consistente do *relay*, já que a informação oriunda de Alice deverá ser decodificada e o resultado deverá ser encaminhado a Bob. Alguns exemplos de protocolos cooperativos clássicos encontrados na literatura são o *Amplify-and-Forward* e o *Decode-and-Forward* Fixo, apresentados em (LANEMAN et al., 2004). No protocolo AF, o *relay* aplica um ganho de sinal na informação recebida por Alice e reencaminha a informação para Bob. Já no protocolo DF, o *relay* decodifica a informação recebida por Alice e reencaminha esta informação re-codificada a Bob. Além destes, apresentaremos protocolos que em que o *relay*, ao invés de auxiliar Bob, tem a função de confundir Eve a partir da injeção de ruído no sistema.

Nos próximos capítulos serão apresentados protocolos cooperativos sob o ponto de vista de segurança. Como dito anteriormente, a comunicação cooperativa permite a transmissão de uma maneira mais confiável entre os nós legítimos e também permite aumentar a confidencialidade do sistema. No capítulos 3 e 4, esquemas cooperativos que exploram completamente a CSI disponível em Alice são propostos para maximizar as métricas de confidencialidade do sistema. No capítulo 4, além da comunicação cooperativa, a utilização de múltiplas antenas nos nós do sistema é considerada de modo a explorar de maneira mais intensa a diversidade espacial do sistema. Cabe ressaltar que a

Figura 3 – Representação da comunicação cooperativa com o *relay* auxiliando Alice a reencaminhar a informação até Bob.



Fonte: Autoria Própria

diversidade espacial permite aumentar a taxa do sistema sem aumentar a largura de banda e diminuir a probabilidade de erro entre os receptores. Já no Capítulo 5 uma comparação entre transmissão direta e cooperativa é realizada em cenários típicos de comunicações M2M em que a transmissão ocorre com blocos de tamanho finito e limitado.

3 PROBABILIDADE GENERALIZADA DE OUTAGE DE SEGURANÇA

Neste capítulo consideramos um caso de conhecimento de CSI no qual apenas o comportamento do canal legítimo é conhecido. Como dito anteriormente, neste caso a confidencialidade perfeita não pode ser garantida, já que o comportamento do canal de Eve é desconhecido. Neste caso, a probabilidade de *outage* de segurança, dada pela capacidade do canal de Eve exceder a taxa de equívoco ou a capacidade de confidencialidade do canal ser menor que a taxa $\mathcal{R}$, é dada por (7).

Contudo, considerando que sistemas podem ter diferentes requisitos de confidencialidade, em (HE; ZHOU, 2014) os autores propõem um modelo de regime parcial em que as restrições de segurança podem ser relaxadas para otimizar outras medidas da confidencialidade, como a eficiência energética segura. De acordo com (HE; ZHOU, 2014), a probabilidade de erro de decodificação em Eve pode ser definida a partir de um limite inferior da equivocação fracionária, representada por Δ, que é uma variável aleatória (VA) descrita por

$$\Delta = \begin{cases} 1, & \text{se } C_{\mathrm{E}} \leq C_{\mathrm{L}} - \mathcal{R} \\ \frac{(C_{\mathrm{L}} - C_{\mathrm{E}})}{\mathcal{R}}, & \text{se } C_{\mathrm{L}} - \mathcal{R} < C_{\mathrm{E}} < C_{\mathrm{L}} \\ 0, & \text{se } C_{\mathrm{L}} \leq C_{\mathrm{E}} \end{cases}. \tag{8}$$

Cabe ressaltar que as condições de Δ representam diferentes níveis de confusão a Eve. Primeiramente, quando $C_{\mathrm{E}} \leq C_{\mathrm{L}} - \mathcal{R}$, a equivocação com $\Delta = 1$ indica que nenhuma informação está disponível a Eve e é possível a ela somente tentar adivinhar aleatoriamente a informação transmitida por Alice. Já o caso $\Delta = 0$, associado com $C_{\mathrm{L}} \leq C_{\mathrm{E}}$, implica que a comunicação segura não é possível. Adicionalmente, o caso intermediário com $\Delta = \frac{(C_{\mathrm{L}} - C_{\mathrm{E}})}{\mathcal{R}}$ representa o regime parcial de segurança, em que apenas uma fração da comunicação é transmitida de maneira segura.

Portanto, uma forma generalizada da probabilidade de *outage* de segurança, representada por $p_{\mathrm{gso}}^{(\mathrm{esq})}$, englobando diferentes níveis de segurança é dada por (HE; ZHOU, 2014)

$$p_{\mathrm{gso}}^{(\mathrm{esq})} = \Pr\{\Delta < \theta\}, \tag{9}$$

onde o sobrescrito $^{(\mathrm{esq})}$ representa o esquema cooperativo empregado, enquanto $\theta \in (0, 1]$ é o mínimo valor aceitável para a equivocação fracionária. Salienta-se que a formulação usual da probabilidade de *outage* de segurança considera somente o caso $C_{\mathrm{E}} \leq C_{\mathrm{L}} - \mathcal{R}$,

que corresponde ao caso em que $\theta = 1$.

Desta forma, substituindo (8) em (9), a probabilidade generalizada de *outage* de segurança pode ser reescrita como

$$p_{\text{gso}}^{(\text{esq})} = \Pr\left\{0 < \theta \bigcap C_{\text{L}} \leq C_{\text{E}}\right\} + \Pr\left\{\frac{C_{\text{L}} - C_{\text{E}}}{\mathcal{R}} < \theta \bigcap C_{\text{L}} - \mathcal{R} < C_{\text{E}} < C_{\text{L}}\right\} + \Pr\left\{1 < \theta \bigcap C_{\text{E}} \leq C_{\text{L}} - \mathcal{R}\right\}. \tag{10}$$

Contudo, já que $\theta \in (0, 1]$, temos que $\Pr\{0 < \theta\} = 1$ e $\Pr\{1 < \theta\} = 0$, de forma que (10) se torna

$$p_{\text{gso}}^{(\text{esq})} = \Pr\{C_{\text{L}} \leq C_{\text{E}}\} + \Pr\left\{C_{\text{L}} - C_{\text{E}} < \theta\mathcal{R} \bigcap C_{\text{L}} - \mathcal{R} < C_{\text{E}} < C_{\text{L}}\right\}. \tag{11}$$

Cabe ressaltar que em (11) consideramos que não existe perda de multiplexação na comunicação, ou seja, a comunicação ocorre em apenas um intervalo de tempo. Considerando comunicação cooperativa, assim como no decorrer deste capítulo, o termo $\mathcal{R}$ deve ser substituído por $2\mathcal{R}$.

3.1 PROTOCOLOS DE TRANSMISSÃO COOPERATIVA

Nesta seção apresentamos as equações da métrica da probabilidade generalizada da *outage* de segurança para cada esquema cooperativo. Esta formulação é necessária para definição das equações de eficiência energética segura para cada esquema. A SEE, representada por η_{s}, é definida pela razão entre a quantidade de bits transmitidos de maneira segura, denominada como *throughput* seguro, representado por τ_{s}, e a potência total utilizada para realizar tal transmissão, representada por P_{total}. O *throughput* seguro, assim como (BRANTE et al., 2015) com adição do parâmetro de equivocação θ, pode ser proposto como

$$\tau_{\text{s}}^{(\text{esq})} = \theta\mathcal{R}\left(1 - p_{\text{gso}}^{(\text{esq})}\right). \tag{12}$$

Desta forma, define-se a SEE por

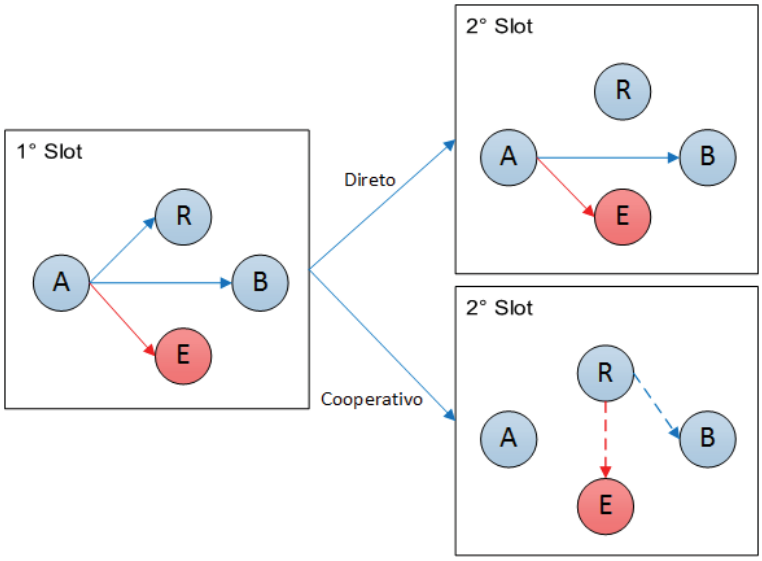
$$\eta_{\text{s}}^{(\text{esq})} = \frac{\tau_{\text{s}}^{(\text{esq})}}{P_{\text{total}}^{(\text{esq})}}, \tag{13}$$

onde $P_{\text{total}}^{(\text{esq})}$ representa o consumo total de potência do esquema cooperativo esq.

3.1.1 CSI-*Aided* DF com Codificação de Repetição (CSI-RC)

Considerando o cenário em que Alice tem CSI perfeita com respeito aos nós legítimos, observamos que os esquemas cooperativos tradicionais, como o *Decode-and-Forward* fixo empregado em (GABRY et al., 2011b, 2011a; CHEN et al., 2015) não exploram completamente a CSI disponível.

Figura 4 – Representação da escolha entre comunicação direta ou cooperativa dos esquemas CSI-*Aided* DF.



Fonte: Autoria Própria

Desta forma, de modo a explorar completamente a CSI disponível, é possível à Alice selecionar o caminho mais seguro até Bob, escolhendo entre a transmissão direta ou utilizando o *relay*, conforme Figura 4. Caso o caminho cooperativo seja escolhido por Alice, assumimos que o *relay* emprega o DF convencional utilizando o mesmo *codebook* de Alice, denominado por (KHORMUJI; LARSSON, 2009) como codificação de repetição. Portanto, a capacidade do canal legítimo do esquema CSI-RC proposto neste trabalho, representado pelo máximo entre os caminhos direto e cooperativo, é

$$C_{\mathrm{L}}^{(\text{CSI-RC})} = \frac{1}{2}\max\left\{\log_2\left(1+\gamma'_{\mathrm{AB}}\right), \min\left\{\log_2\left(1+\gamma_{\mathrm{AR}}\right), \log_2\left(1+\gamma_{\mathrm{B}}\right)\right\}\right\}, \tag{14}$$

onde $\gamma_{\mathrm{B}} = \gamma_{\mathrm{AB}} + \gamma_{\mathrm{RB}}$. Além do mais, $\gamma'_{\mathrm{AB}} = \gamma_{\mathrm{AB},1} + \gamma_{\mathrm{AB},2}$ representa que Alice transmite a mesma informação nos dois *slots* de tempo quando a comunicação direta é empregada, assim como (LANEMAN et al., 2004), com o intuito de se realizar uma comparação justa em termos de perdas de multiplexação com os outros esquemas cooperativos.

Já a capacidade do canal com relação à Eve depende da escolha do melhor

caminho para Alice, portanto

$$C_{\mathrm{E}}^{(\text{CSI-RC})} = \begin{cases} \dfrac{1}{2}\log_2(1+\gamma'_{\mathrm{AE}}), & \text{se Alice transmite diretamente,} \\ \dfrac{1}{2}\log_2(1+\gamma_{\mathrm{E}}), & \text{caso contrário,} \end{cases} \tag{15}$$

onde $\gamma'_{\mathrm{AE}} = \gamma_{\mathrm{AE},1} + \gamma_{\mathrm{AE},2}$ e $\gamma_{\mathrm{E}} = \gamma_{\mathrm{AE}} + \gamma_{\mathrm{RE}}$.

Contudo, obter uma equação fechada para a generalização da probabilidade de *outage* de segurança do CSI-RC é complexo, principalmente devido ao máximo entre $\log_2(1+\gamma'_{\mathrm{AB}})$ e $\min\{\log_2(1+\gamma_{\mathrm{AR}}), \log_2(1+\gamma_{\mathrm{B}})\}$ em (14). Portanto, recorremos a uma aproximação assumindo que o *relay* está em uma posição intermediária entre Alice e Bob, de forma que Alice escolhe pela transmissão direta sempre que $\gamma_{\mathrm{AB}} \geq \gamma_{\mathrm{AR}}$, enquanto a cooperação ocorre se $\gamma_{\mathrm{AR}} > \gamma_{\mathrm{AB}}$. Esta aproximação foi considerada em (FARHAT et al., 2015) para o caso em que $\theta = 1$, no qual foi demonstrado por resultados numéricos que o impacto na probabilidade de *outage* de segurança é mínimo independentemente da posição do *relay* entre Alice e Bob.

Teorema 1. *A probabilidade generalizada de outage de segurança para o esquema CSI-RC pode ser satisfatoriamente aproximada por*

$$\begin{aligned} p_{gso}^{(\textit{CSI-RC})} \approx{}& \frac{4^{2\mathcal{R}\theta} e^{\frac{1-4^{-\mathcal{R}\theta}}{(2\bar{\gamma}_{AE})}} \bar{\gamma}_{AB}\bar{\gamma}_{AE}^2}{(\bar{\gamma}_{AB}+4^{\mathcal{R}\theta}\bar{\gamma}_{AE})(\bar{\gamma}_{AB}\bar{\gamma}_{AR}+4^{\mathcal{R}\theta}\bar{\gamma}_{AE}(\bar{\gamma}_{AB}+\bar{\gamma}_{RE}))} + \frac{4^{\mathcal{R}\theta} e^{-\frac{4^{-\mathcal{R}\theta}(\bar{\gamma}_{RE}+\bar{\gamma}_{AE})}{(\bar{\gamma}_{RE}\bar{\gamma}_{AE})}}}{(\bar{\gamma}_{RE}-\bar{\gamma}_{AE})} \\ &\times \left[\frac{\overline{\gamma}_{AR}}{(\overline{\gamma}_{RB}-\overline{\gamma}_{AB})(\overline{\gamma}_{AB}+\overline{\gamma}_{AR})} \left(e^{\frac{1}{\bar{\gamma}_{RE}}+\frac{4^{-\mathcal{R}\theta}}{\bar{\gamma}_{AE}}} \bar{\gamma}_{RE}^2 \varsigma(\bar{\gamma}_{RE}) - e^{\frac{1}{\bar{\gamma}_{AE}}+\frac{4^{-\mathcal{R}\theta}}{\bar{\gamma}_{RE}}} \bar{\gamma}_{AE}^2 \varsigma(\bar{\gamma}_{AE}) \right) \right. \\ &\left. + \frac{e^{\frac{1}{\bar{\gamma}_{RE}}+\frac{4^{-\mathcal{R}\theta}}{\bar{\gamma}_{AE}}} \bar{\gamma}_{RE}^2 \chi(\bar{\gamma}_{RE}) - e^{\frac{1}{\bar{\gamma}_{AE}}+\frac{4^{-\mathcal{R}\theta}}{\bar{\gamma}_{RE}}} \bar{\gamma}_{AE}^2 \chi(\bar{\gamma}_{AE})}{(\bar{\gamma}_{AB}-\bar{\gamma}_{RB})} \right], \end{aligned} \tag{16}$$

onde

$$\begin{aligned} \varsigma(x) = {}& \frac{\bar{\gamma}_{RB}(\bar{\gamma}_{AB}+\bar{\gamma}_{AR})}{\bar{\gamma}_{RB}\bar{\gamma}_{AR}+4^{\mathcal{R}\theta}x(\bar{\gamma}_{RB}+\bar{\gamma}_{AR})} + \frac{\bar{\gamma}_{AB}(\bar{\gamma}_{AB}+\bar{\gamma}_{AR})}{\bar{\gamma}_{AB}\bar{\gamma}_{AR}+4^{\mathcal{R}\theta}x(\bar{\gamma}_{AB}+\bar{\gamma}_{AR})} \\ &+ \frac{\bar{\gamma}_{AB}^2}{\bar{\gamma}_{AB}\bar{\gamma}_{AR}+4^{\mathcal{R}\theta}x(\bar{\gamma}_{AB}+2\bar{\gamma}_{AR})} + \frac{\bar{\gamma}_{RB}\bar{\gamma}_{AB}^2}{\bar{\gamma}_{RB}\bar{\gamma}_{AB}\bar{\gamma}_{AR}+4^{\mathcal{R}\theta}x[\bar{\gamma}_{AB}\bar{\gamma}_{AR}+\bar{\gamma}_{RB}(\bar{\gamma}_{AB}+\bar{\gamma}_{AR})]} \end{aligned} \tag{17}$$

e

$$\chi(x) = \frac{\bar{\gamma}_{AB}^2}{\bar{\gamma}_{AB}\bar{\gamma}_{AR} + 4^{\mathcal{R}\theta}x(\bar{\gamma}_{AB} + 2\bar{\gamma}_{AR})} - \frac{\bar{\gamma}_{AB}^2}{\bar{\gamma}_{AB}\bar{\gamma}_{AR} + 4^{\mathcal{R}\theta}x(\bar{\gamma}_{AB} + \bar{\gamma}_{AR})} + \frac{\bar{\gamma}_{RB}^2}{\bar{\gamma}_{RB}\bar{\gamma}_{AR} + 4^{\mathcal{R}\theta}x(\bar{\gamma}_{RB} + \bar{\gamma}_{AR})} - \frac{\bar{\gamma}_{RB}^2}{\bar{\gamma}_{RB}\bar{\gamma}_{AB}\bar{\gamma}_{AR} + 4^{\mathcal{R}\theta}x[\bar{\gamma}_{AB}\bar{\gamma}_{AR} + \bar{\gamma}_{RB}(\bar{\gamma}_{AB} + \bar{\gamma}_{AR})]} \tag{18}$$

Demonstração. Disponível no Apêndice A. □

3.1.2 CSI-*Aided* DF com Codificação Paralela (CSI-PC)

Similarmente ao esquema CSI-RC e à Figura 4, neste esquema Alice explora completamente a CSI disponível para escolha do melhor caminho até Bob com o intuito de maximizar a SEE. Contudo, diferentemente do esquema CSI-RC, é proposto que a transmissão ocorre utilizando codificação paralela (KHORMUJI; LARSSON, 2009). Portanto, a informação enviada durante o segundo *slot* de tempo é codificada utilizando um *codebook* diferente, independente do *codebook* utilizado por Alice no primeiro *slot* de tempo. Em (KHORMUJI; LARSSON, 2009) os autores realizam a comparação dos esquemas RC e PC em um cenário sem restrições de segurança, no qual o PC apresenta um desempenho superior. Isto ocorre pelo fato da retransmissão ocorrer com novas informações sobre a mensagem, devido a utilização de um *codebook* diferente. Desta forma, a capacidade do canal legítimo, a partir de (KHORMUJI; LARSSON, 2009), é dada por

$$\begin{aligned} C_{\mathrm{L}}^{(\text{CSI-PC})} &= \frac{1}{2}\max\left\{\sum_{i=1}^{2}\log_2\left(1+\gamma_{\mathrm{AB},i}\right), \min\left\{\log_2\left(1+\gamma_{\mathrm{AR}}\right), \log_2\left(1+\gamma_{\mathrm{AB}}\right)+\log_2\left(1+\gamma_{\mathrm{RB}}\right)\right\}\right\} \\ &= \frac{1}{2}\max\left\{\sum_{i=1}^{2}\log_2\left(1+\gamma_{\mathrm{AB},i}\right), \min\left\{\log_2\left(1+\gamma_{\mathrm{AR}}\right), \log_2\left(1+\Phi_{\mathrm{B}}\right)\right\}\right\}, \end{aligned} \tag{19}$$

onde $\Phi_{\mathrm{B}} = \gamma_{\mathrm{AB}} + \gamma_{\mathrm{RB}} + \gamma_{\mathrm{AB}}\gamma_{\mathrm{RB}}$.

Similarmente ao esquema CSI-RC, a capacidade do canal de Eve também depende da escolha entre a transmissão direta ou cooperativa e, desta forma, é dada por

$$C_{\mathrm{E}}^{(\text{CSI-PC})} = \begin{cases} \dfrac{1}{2}\displaystyle\sum_{i=1}^{2}\log_2(1+\gamma_{\mathrm{AE},i}), & \text{se Alice transmite diretamente,} \\ \dfrac{1}{2}\log_2(1+\Phi_{\mathrm{E}}), & \text{caso contrário,} \end{cases} \tag{20}$$

onde $\Phi_{\mathrm{E}} = \gamma_{\mathrm{AE}} + \gamma_{\mathrm{RE}} + \gamma_{\mathrm{AE}}\gamma_{\mathrm{RE}}$.

Para obter a equação da probabilidade generalizada de *outage* de segurança para o esquema CSI-PC, precisamos obter primeiramente a PDF de Φ_{B} e Φ_{E}, as quais são difíceis de serem obtidas em uma forma exata devido à multiplicação e soma de duas VAs. Desta forma, no Lema 1, propomos uma aproximação para esta PDF.

Lema 1. *A VA* $\Phi_j = \gamma_{Aj} + \gamma_{Rj} + \gamma_{Aj}\gamma_{Rj}$*, com* $j \in \{B, E\}$*, pode ser satisfatoriamente aproximada por uma única VA com distribuição Gamma, cuja PDF é dada por*

$$f_{\Phi_j} \approx \frac{\Phi_j^{m_j-1} e^{-\frac{\Phi_j m_j}{\Omega_j}}}{\Gamma(m_j)\left(\frac{\Omega_j}{m_j}\right)^{m_j}}, \tag{21}$$

onde $m_j = \frac{{\Omega_j}^2}{\bar{\gamma}_{Rj}^2 + \bar{\gamma}_{Aj}^2 + \left(\sqrt{2}\bar{\gamma}_{Aj}\bar{\gamma}_{Rj}\right)^2}$ *e* $\Omega_j = \bar{\gamma}_{Rj} + \bar{\gamma}_{Aj} + \left(\sqrt{2}\bar{\gamma}_{Aj}\bar{\gamma}_{Rj}\right)$.

Demonstração. Disponível no Apêndice B. □

Baseado nos resultados do Lema 1, propomos a seguinte aproximação para a probabilidade generalizada de *outage* de segurança para o esquema CSI-PC.

Teorema 2. *A probabilidade generalizada da outage de segurança para o esquema CSI-PC pode ser aproximada por*

$$\begin{aligned} p_{gso}^{(CSI\text{-}PC)} \approx & \frac{2^{2\mathcal{R}\theta}\bar{\gamma}_{AB}\bar{\gamma}_{AE}^2 e^{-\frac{2^{-\mathcal{R}\theta}-1}{\bar{\gamma}_{AE}}}\left(\bar{\gamma}_{AB}+2^{\mathcal{R}\theta}\bar{\gamma}_{AE}\right)^{-1}}{\left(\bar{\gamma}_{AB}\bar{\gamma}_{AR}+2^{\mathcal{R}\theta}\bar{\gamma}_{AE}(\bar{\gamma}_{AB}+\bar{\gamma}_{AR})\right)} - \frac{\bar{\gamma}_{AR}^2}{(\bar{\gamma}_{AB}+\bar{\gamma}_{AR})^2} \\ & \times \left[\frac{\nu(\bar{\gamma}_{AB})(\bar{\gamma}_{AB}+\bar{\gamma}_{AR})+\nu(\bar{\gamma}_{AB}+\bar{\gamma}_{AR})\bar{\gamma}_{AB}}{\bar{\gamma}_{AR}} - 2^{2\mathcal{R}\theta m_B}\left(\frac{m_B}{m_E}\right)^{m_B}\right. \\ & \left. \times \left(\frac{\Omega_E}{\Omega_B}\right)^{m_B}\frac{\Gamma(m_B+m_E)}{\Gamma(m_E)}\,{}_2F_1\left(m_E, m_B+m_E; 1+m_B; -\frac{2^{2\mathcal{R}\theta}m_B\Omega_E}{m_E\Omega_B}\right) - 1\right], \end{aligned} \tag{22}$$

onde

$$\nu(x) = \left(1 + \frac{2^{2\mathcal{R}\theta}\Omega_E x}{\gamma_{AR} m_E}\right)^{-m_E} \tag{23}$$

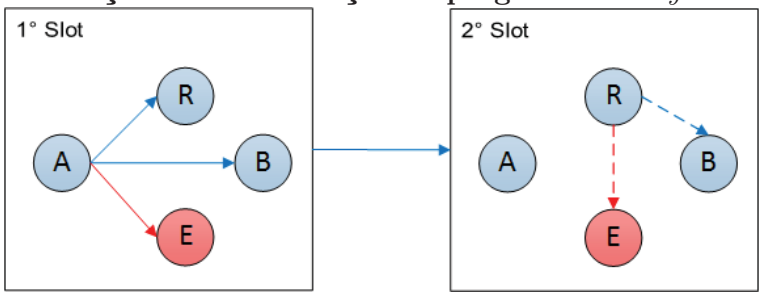
e ${}_2F_1(.,.;.;.)$ *é a função hipergeométrica de Gauss (GRADSHTEYN; RYZHIK, 2007, Eq. (9.111)).*

Demonstração. Disponível no Apêndice C. □

3.1.3 *Decode-and-Forward* (DF)

Para comparação, consideramos o DF assim como usualmente empregado na literatura como, por exemplo, em (GABRY et al., 2011b; DONG et al., 2010; GABRY et al., 2011a; CHEN et al., 2015). Neste esquema, conforme Figura 5, Alice transmite a informação no primeiro *slot* de tempo para o *relay* e Bob enquanto o *relay*, no segundo *slot* de tempo decodifica a mensagem recebida de Alice e então reencaminha para Bob.

Figura 5 – Representação da comunicação empregando o *relay* na retransmissão.



Fonte: Autoria Própria

Considerando que Bob emprega razão de combinação máxima (MRC), obtemos (DONG et al., 2010)

$$C_{\mathrm{L}}^{(\mathrm{DF})} = \frac{1}{2}\min\left\{\log_2\left(1+\gamma_{\mathrm{AR}}\right), \log_2\left(1+\gamma_{\mathrm{B}}\right)\right\} \tag{24}$$

e

$$C_{\mathrm{E}}^{(\mathrm{DF})} = \frac{1}{2}\log_2\left(1+\gamma_{\mathrm{E}}\right). \tag{25}$$

Proposição 1. *A probabilidade generalizada de outage de segurança do DF é dada por*

$$p_{gso}^{(DF)} \approx \frac{4^{\mathcal{R}\theta}\left[\mathcal{K}(\bar{\gamma}_{RE}) - \mathcal{K}(\bar{\gamma}_{AE})\right]}{\bar{\gamma}_{RE} - \bar{\gamma}_{AE}}, \tag{26}$$

onde

$$\mathcal{K}(x) = \frac{e^{\frac{(1-4^{\mathcal{R}\theta})}{x}} x^2 \left[\bar{\gamma}_{RB}\bar{\gamma}_{AB}\bar{\gamma}_{AR} + 4^{\mathcal{R}\theta}\, x\,(\bar{\gamma}_{RB}+\bar{\gamma}_{AR})(\bar{\gamma}_{AB}+\bar{\gamma}_{AR})\right]}{\left[\bar{\gamma}_{RB}\bar{\gamma}_{AR} + 4^{\mathcal{R}\theta}\, x\,(\bar{\gamma}_{RB}+\bar{\gamma}_{AR})\right]\left[\bar{\gamma}_{AB}\bar{\gamma}_{AR} + 4^{\mathcal{R}\theta}\, x\,(\bar{\gamma}_{AB}+\bar{\gamma}_{AR})\right]}. \tag{27}$$

Demonstração. Disponível no Apêndice D. □

Ressaltamos que (26) se torna a mesma expressão obtida em (GABRY et al., 2011a) quando $\theta = 1$.

3.1.4 *Amplify-and-Forward* (AF)

No esquema AF, conforme esquema demonstrado na Figura 5, Alice transmite as informações por radiodifusão no primeiro *slot* de tempo enquanto o *relay* aplica um ganho de potência no sinal recebido por Alice e reencaminha a informação para Bob. Considerando que Bob aplica MRC nas transmissões recebidas por Alice e pelo *relay*, as capacidades dos canais legítimos e de Eve são dadas por (GABRY et al., 2011b)

$$C_{\mathrm{L}}^{(\mathrm{AF})} = \frac{1}{2}\log_2\left(1+\gamma_{\mathrm{AB}}+\frac{\gamma_{\mathrm{AR}}\,\gamma_{\mathrm{RB}}}{1+\gamma_{\mathrm{AR}}+\gamma_{\mathrm{RB}}}\right) \tag{28}$$

e

$$C_{\mathrm{E}}^{(\mathrm{AF})} = \frac{1}{2}\log_2\left(1+\gamma_{\mathrm{AE}}+\frac{\gamma_{\mathrm{AR}}\,\gamma_{\mathrm{RE}}}{1+\gamma_{\mathrm{AR}}+\gamma_{\mathrm{RE}}}\right). \tag{29}$$

Proposição 2. *A probabilidade generalizada de outage de segurança para o AF pode ser aproximada por*

$$p_{gso}^{(AF)} \approx \frac{\bar{\gamma}_B''\left[\mathcal{B}(\bar{\gamma}_B'',\bar{\gamma}_E'')-\mathcal{B}(\bar{\gamma}_B'',\bar{\gamma}_{AE})\right]}{(\bar{\gamma}_E''-\bar{\gamma}_{AE})(\bar{\gamma}_B''-\bar{\gamma}_{AB})} - \frac{\bar{\gamma}_{AB}\left[\mathcal{B}(\bar{\gamma}_{AB},\bar{\gamma}_E'')-\mathcal{B}(\bar{\gamma}_{AB},\bar{\gamma}_{AE})\right]}{(\bar{\gamma}_E''-\bar{\gamma}_{AE})(\bar{\gamma}_B''-\bar{\gamma}_{AB})}, \tag{30}$$

onde

$$\mathcal{B}(x,y) = \frac{y^2}{2^{-2\theta\mathcal{R}}x+y}e^{-\frac{(2^{-2\theta\mathcal{R}}-1)}{y}} \tag{31}$$

e

$$\bar{\gamma}_j'' = \frac{\bar{\gamma}_{AR}\bar{\gamma}_{Rj}}{\bar{\gamma}_{AR}+\bar{\gamma}_{Rj}} \tag{32}$$

com $j \in \{B,E\}$.

Demonstração. Disponível no Apêndice E. □

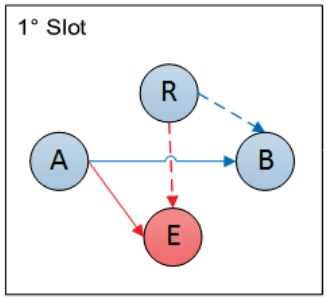
Note que (30) é similar à expressão dada em (GABRY et al., 2013), porém com a diferença que consideramos $\theta\mathcal{R}$ em vez de $\mathcal{R}$.

3.1.5 *Cooperative Jamming* (CJ)

No esquema CJ, o *relay* não auxilia a comunicação entre os nós legítimos. Diferentemente dos esquemas propostos anteriormente, o *relay* injeta ruído Gaussiano com a intenção de confundir Eve.

Desta forma, assim como mostrado na Figura 6, Alice e o *relay* transmitem ao mesmo tempo, de forma que as capacidades dos canais legítimos e de escuta são (VILELA

Figura 6 – Representação da comunicação na qual Alice e *relay* transmitem informação e ruído, respectivamente, ao mesmo tempo.



Fonte: Autoria Própria

et al., 2011)

$$C_{\mathrm{L}}^{(\mathrm{CJ})} = \log_2\left(1+\frac{\gamma_{\mathrm{AB}}}{1+\gamma_{\mathrm{RB}}}\right) \tag{33}$$

e

$$C_{\mathrm{E}}^{(\mathrm{CJ})} = \log_2\left(1+\frac{\gamma_{\mathrm{AE}}}{1+\gamma_{\mathrm{RE}}}\right). \tag{34}$$

Salientamos que o ruído injetado pelo *relay* também interfere em Bob, uma vez que esta SNR aparece no denominador de (33).

Proposição 3. *A probabilidade generalizada da outage de segurança do esquema CJ é*

$$p_{gso}^{(CJ)} = 1+\frac{e^{-b}}{\bar{\gamma}_{RE}\bar{\gamma}_{RB}\varepsilon\alpha}\left[\left(1-\frac{1}{\alpha l\varepsilon}\right)\mathcal{F}(\varepsilon+\varepsilon\alpha)+\left(\frac{1}{\alpha l\varepsilon}+\frac{1}{\alpha}\right)\mathcal{F}\left(\frac{1+\alpha}{\alpha\bar{\gamma}_{RE}}\right)-\bar{\gamma}_{RE}\right], \tag{35}$$

onde

$$b = \frac{2^{\theta\mathcal{R}}-1}{\bar{\gamma}_{AB}}, \tag{36}$$

$$\varepsilon = \frac{1+\bar{\gamma}_{RB}b}{\bar{\gamma}_{RB}}, \tag{37}$$

$$\alpha = \frac{\bar{\gamma}_{AB}}{\bar{\gamma}_{AE}(1+\bar{\gamma}_{AB}b)}, \tag{38}$$

$$l = 1-\frac{1}{\bar{\gamma}_{RE}\varepsilon\alpha}, \tag{39}$$

$$\mathcal{F}(x) = e^x E_1(x) \tag{40}$$

e $E_1(x) = \int_x^\infty \frac{e^{-t}}{t}\mathrm{d}t$ *é a integral exponencial.*

Demonstração. Disponível no Apêndice F. □

Salientamos que (35) é muito similar à expressão obtida em (GABRY et al., 2011a). Contudo o termo b depende de $\theta\mathcal{R}$, em vez de somente $\mathcal{R}$ como em (GABRY et al., 2011a).

3.2 ALGORITMO PARA OTIMIZAÇÃO DA SEE

Nesta seção abordaremos o algoritmo proposto para maximização da SEE a partir da alocação conjunta de potência em Alice e no *relay*, além do θ ótimo para economia de energia. O problema de otimização proposto pode ser matematicamente definido como

$$\begin{aligned} \underset{(P_{\mathrm{A}},P_{\mathrm{R}},\theta)}{\text{maximize}} \quad & \eta^{(\mathrm{esq})} = \frac{\theta\mathcal{R}\left(1-p_{\mathrm{gso}}^{(\mathrm{esq})}\right)}{P_{\mathrm{total}}^{(\mathrm{esq})}} \quad \left[\frac{\text{bits seguros}}{\mathrm{J}\times\mathrm{Hz}}\right] \\ \text{sujeito a} \quad & 0 < P_i \leq P_{\max}, \text{ com } i \in \{\mathrm{A},\mathrm{R}\}, \\ & 0 < \theta \leq 1, \end{aligned} \tag{41}$$

onde $P_{\max}$ representa a máxima potência de transmissão, a qual assumimos ser a mesma tanto para Alice quanto para o *relay*.

3.2.1 Consumo Total de Potência

Nesta subseção apresentamos o consumo total de potência de cada esquema cooperativo seguindo o mesmo modelo adotado em (CUI et al., 2004), o qual considera as potências empregadas em Alice e no *relay*, P_{A} e P_{R}, além da potência consumida nos circuitos de transmissão e recepção, P_{TX} e P_{RX}. Consideramos ainda ω, que representa o gasto adicional de energia associado ao amplificador de potência. Para um determinado nó i, conforme (CUI et al., 2004), o consumo de potência é dado por $(1+\omega)P_i$, onde $\omega = \left(\frac{\mathcal{E}}{\mathcal{N}} - 1\right)$ com $\mathcal{E} = 3\left(\frac{\sqrt{M}-1}{\sqrt{M}+1}\right)$ representa a relação pico-média (PAR, do inglês *Peak-to-Average Ratio*) para a modulação M-QAM e $\mathcal{N}$ a eficiência de dreno do amplificador.

Desta forma, o consumo de potência para os esquemas CSI-RC e CSI-PC é dado por

$$\begin{aligned} P_{\mathrm{total}}^{(\text{CSI-RC})} = P_{\mathrm{total}}^{(\text{CSI-PC})} = {} & 2\Big[(1+\omega)P_{\mathrm{A}} + P_{\mathrm{TX}} + P_{\mathrm{RX}}\Big]\ \Pr\{\gamma_{\mathrm{AB}} \geq \gamma_{\mathrm{AR}}\} \\ & + \Big[(1+\omega)(P_{\mathrm{A}}+P_{\mathrm{R}}) + 2P_{\mathrm{TX}} + 3P_{\mathrm{RX}}\Big]\ \Pr\{\gamma_{\mathrm{AR}} > \gamma_{\mathrm{AB}}\}, \end{aligned} \tag{42}$$

onde $\Pr\{\gamma_{\mathrm{AR}} > \gamma_{\mathrm{AB}}\} = \frac{\bar{\gamma}_{\mathrm{AR}}}{\bar{\gamma}_{\mathrm{AR}}+\bar{\gamma}_{\mathrm{AB}}}$. Salientamos que (42) depende da escolha de Alice entre a transmissão direta ou cooperativa. Caso $\gamma_{\mathrm{AB}} \geq \gamma_{\mathrm{AR}}$, a transmissão escolhida por Alice será a direta, de forma que o consumo de potência é dado pela potência utilizada por Alice nos dois *slots* de tempo, assim como a potência associada ao circuito de transmissão em Alice e ao circuito de recepção em Bob. Ao contrário, quando $\gamma_{\mathrm{AR}} > \gamma_{\mathrm{AB}}$, a cooperação

é empregada, de forma que o consumo de potência é dado pela potência empregada em Alice e no *relay*, além do consumo associado ao circuito de transmissão e o circuito de recepção do *relay* no primeiro *slot* de tempo e de Bob nos dois *slots* de tempo.

Para os esquemas cooperativos AF e DF têm-se

$$P_{\text{total}}^{(\text{AF})} = P_{\text{total}}^{(\text{DF})} = (1+\omega)\,(P_{\text{A}} + P_{\text{R}}) + 2P_{\text{TX}} + 3P_{\text{RX}}. \tag{43}$$

Salientamos que este consumo de potência é muito similar à (42) quando o *relay* coopera. Cabe ressaltar também que, apesar da mesma expressão do consumo total de potência para todos estes esquemas, a potência alocada por cada transmissor pode ser diferente entre cada esquema cooperativo.

Finalmente, o consumo do esquema CJ é

$$P_{\text{total}}^{(\text{CJ})} = (1+\omega)\,(P_{\text{A}} + P_{\text{R}}) + 2\,P_{\text{TX}} + P_{\text{RX}}, \tag{44}$$

o qual considera a potência empregada por Alice para transmissão da informação e pelo *relay* para injetar ruído Gaussiano. Além disto, $P_{\text{total}}^{(\text{CJ})}$ inclui o circuito de transmissão, em Alice e no *relay*, e o circuito de recepção, em Bob.

3.2.2 Algoritmo Proposto

O algoritmo proposto para maximização de SEE otimiza a potência e θ a partir de uma abordagem baseada no algoritmo Dinkelbach combinada com o algoritmo *golden section search* (PRESS et al., 2007). Para otimizar cada parâmetro, nós propomos um algoritmo composto de um laço externo e três laços internos. O laço externo está relacionado ao critério de parada do algoritmo e é iterado até o aumento de SEE, devido à alocação de P_{A}, P_{R} e θ, ser menor que um limiar predefinido ϵ. Já os laços internos estão associados à alocação de potências e θ. Portanto, dois laços internos utilizam uma abordagem baseada no algoritmo Dinkelbach para alocação de potência em Alice e no *relay* enquanto um terceiro laço interno encontra o melhor valor para θ, para um dado valor de P_{A} e P_{R}, utilizando o algoritmo de *golden section search* com interpolação parabólica. Os primeiros dois laços internos tem o critério de parada quando ϵ_{P} é atingido, enquanto ϵ_θ define o critério de parada do terceiro laço interno. O algoritmo proposto para resolver (41) é apresentado no Algoritmo 1 e discutido detalhadamente nas próximas subseções.

3.2.2.1 Otimização da Alocação de Potência

Devido à complexidade das expressões de $p_{\text{gso}}^{(\text{esq})}$, o problema de otimização formulado em (41) é difícil de ser resolvido de uma forma fechada. Uma alternativa iterativa e distribuída para otimização de razões entre funções de uma mesma variável, que difere de uma busca exaustiva, é dada pela algoritmo Dinkelbach (DINKELBACH, 1967; ZAPPONE; JORSWIECK, 2014).

Um programa fracionário é definido, de uma maneira geral, por

$$\underset{\mathbf{x}\in\mathbf{S}}{\text{maximize}}\ q(x) = \frac{f_1(x)}{f_2(x)}, \tag{45}$$

onde $\mathbf{S} \subseteq \mathbb{R}^n$ é um conjunto convexo, $f_1,\ f_2 : \mathbf{S} \to \mathbb{R}$, sendo $f_1(x)$ côncavo e $f_2(x) > 0$ convexo.

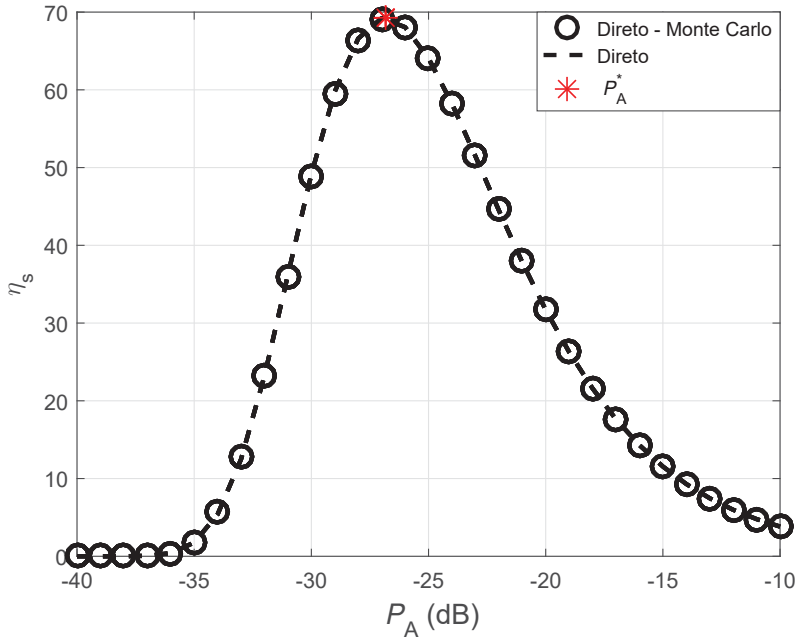
Conforme (ZAPPONE; JORSWIECK, 2014), mesmo que a função (45) seja pseudo-côncava, ou seja, mesmo que a função não seja estritamente côncava, existe um ponto de inflexão m. Desta forma, para qualquer ponto $t \leq m$ a função é não decrescente enquanto para $t \geq m$ a função é não crescente, de forma que é possível resolver o programa fracionário reescrevendo (45) como (DINKELBACH, 1967; ZAPPONE; JORSWIECK, 2014)

$$\begin{aligned} &\underset{\mathbf{x}\in\mathbf{S},\lambda\in\mathbb{R}}{\text{maximize}}\ \lambda \\ &\text{sujeito a}\ \ f_1(x) - \lambda f_2(x) \geq 0. \end{aligned} \tag{46}$$

A função objetivo que se deseja maximizar neste caso, conforme (41), é a eficiência energética segura. Tal medida, $\eta_s^{(\text{esq})}$, é dada pela razão entre o *throughput* seguro, $\tau_s^{(\text{esq})}$, e o gasto total de potência, $P_{\text{total}}^{(\text{esq})}$. Conforme (ZAPPONE et al., 2018), visto que *throughput* seguro é não negativo, diferenciável e côncavo, enquanto o gasto total de potência é diferenciável e convexo, temos que a eficiência energética segura é pseudo-côncava. Tal definição implica que qualquer ponto estacionário da função é um ótimo global.

A fim de realizar uma análise gráfica do comportamento da SEE com relação à variação da potência, a Figura 7 demonstra a SEE para o esquema de transmissão direto a partir da variação de potência alocada em Alice em dB. Adicionalmente, é traçado o valor de potência ótima que permite maximizar a SEE, $P_{\text{A}}^{\star}$, obtido igualando a derivada da eficiência energética segura com relação à potência a zero. Cabe ressaltar que apesar de ser considerada apenas a transmissão direta, tal análise pode ser estendida para os esquemas cooperativos considerados neste capítulo, visto que o uso da cooperação implica

Figura 7 – SEE em função de P_A considerando o esquema de transmissão direto. Além do mais, o valor da potência que maximiza a curva da SEE é obtido a partir da derivada primeira da eficiência energética segura com relação a potência e igualando tal equação a zero.



Fonte: Autoria própria.

apenas em uma variação de largura, altura ou deslocamento lateral da curva da eficiência energética segura, de modo que as características com relação à concavidade e convexidade permanecem as mesmas. A partir da análise dos resultados é possível verificar que pelo fato da equação ser diferenciável, não negativa para $P_\mathrm{A} \geq 0$ e igual a zero para $P_\mathrm{A} = 0$ e $P_\mathrm{A} \to \infty$, conforme (ZAPPONE et al., 2018), um valor ótimo finito deve existir para o sistema sobre o intervalo $\mathbb{R}_0^+$, de modo que a função objetivo aumenta no intervalo $0 \leq P_\mathrm{A} \leq P_\mathrm{A}^\star$, antes do ponto de inflexão $P_\mathrm{A}^\star$, e diminui no intervalo $P_\mathrm{A} > P_\mathrm{A}^\star$, após o ponto de inflexão. Desta forma, pode-se resolver o problema de otimização definido em (41) por (46).

Além do mais, podemos modificar (46) para reescrevê-la como (ZAPPONE; JORSWIECK, 2014)

$$F(\lambda) = \underset{\mathbf{x}\in\mathbf{S}}{\text{maximize}} \;\; f_1(x) - \lambda f_2(x), \tag{47}$$

na qual $f_1(x)$ é maximizada enquanto $f_2(x)$ é minimizada, com o parâmetro λ determinando o peso associado ao denominador.

Desta forma, o valor ótimo da função é encontrado com

$$F(\lambda) = 0 \iff \lambda = q^{\star}, \tag{48}$$

onde $q^{\star}$ é o valor ótimo para (45). Portanto, resolver (45) é equivalente a encontrar a raiz de

$$F(\lambda^{\star}) = \underset{\mathbf{x}\in\mathbf{S}}{\text{maximize}}\ f_1(x) - \lambda f_2(x) = 0. \tag{49}$$

Deste modo, o algoritmo Dinkelbach (DINKELBACH, 1967; ZAPPONE; JORSWIECK, 2014) é uma forma eficiente de encontrar $F(\lambda) = 0$, a partir de uma abordagem baseada no método de Newton para calcular λ para cada $(n+1)$-ésima iteração, conforme

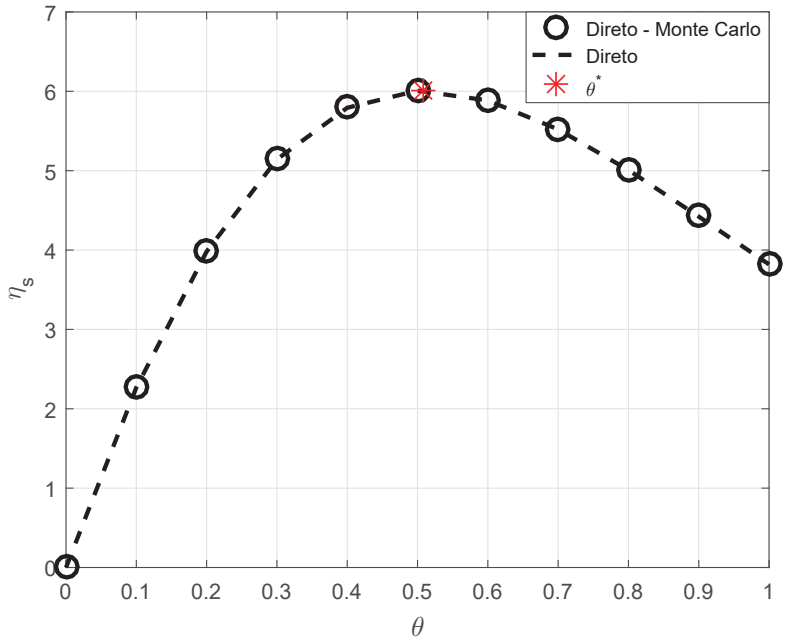
$$\lambda_{n+1} = \lambda_n - \frac{F(\lambda_n)}{F'(\lambda_n)} = \frac{f_1(x_n^{\star})}{f_2(x_n^{\star})}. \tag{50}$$

3.2.2.2 Otimização do parâmetro de equivocação fracionária θ

Similarmente à otimização da potência, inicialmente realizamos uma análise gráfica do comportamento da SEE a partir da variação de θ na Figura 8. Tal figura demonstra a SEE para o esquema de transmissão direta a partir da variação de θ. O valor de θ que maximiza a SEE, $\theta^{\star}$, é obtido igualando a derivada da eficiência energética segura com relação à θ a zero. Cabe ressaltar que, diferentemente da otimização de potências, o valor ótimo de θ, a partir da derivada, apenas é possível de ser obtido de forma numérica pelo fato de ser uma equação transcendental.

Desta forma, para encontrar o parâmetro de equivocação fracionária, θ, que otimiza $\eta_{\mathrm{s}}^{(\mathrm{esq})}$, a interpolação parabólica, que encontra o máximo de uma função unimodal a partir do estreitamento da faixa de valores dentro de um intervalo (PRESS et al., 2007), é realizada a partir do algoritmo *golden section search*. Considerando uma faixa inicial dada por $\theta \in (0,1]$, primeiramente escolhemos um tripleto inicial $\vartheta_0 = (\theta_1, \theta_3, \theta_2)$, onde $\theta_1 < \theta_3 < \theta_2$, e interpolamos ϑ_0 por uma parábola, cujo máximo é dado por θ_4. Então calculamos a eficiência energética utilizando θ_4, e, caso $\eta_{\mathrm{s}}^{(\mathrm{esq})}(\theta_4) > \eta_{\mathrm{s}}^{(\mathrm{esq})}(\theta_3)$ um novo tripleto é definido por $\vartheta_1 = (\theta_3, \theta_4, \theta_2)$, caso contrário, $\vartheta_1 = (\theta_1, \theta_3, \theta_4)$. A Figura 9 ilustra a ideia em que a função da SEE é representada pela linha sólida azul enquanto a interpolação parabólica é destacada na linha tracejada vermelha. Uma vez que a SEE, neste exemplo, é maior adotando θ_4 do que θ_3, o algoritmo estreita o intervalo escolhendo o novo tripleto como $\vartheta_1 = (\theta_3, \theta_4, \theta_2)$. Desta forma, a cada iteração o intervalo torna-se menor até que o algoritmo seja finalizado quando a tolerância predefinida para o tamanho do intervalo é

Figura 8 – SEE em função de θ considerando o esquema de transmissão direto. Já o valor de θ que maximiza a curva da SEE é obtido a partir da derivada primeira da SEE com relação a θ e igualando tal equação a zero.



Fonte: Autoria própria.

atingida.

3.3 RESULTADOS NUMÉRICOS

Nesta seção é realizada uma comparação da SEE entre os métodos cooperativos mencionados anteriormente. Consideramos $\mathcal{R} = 3$ bps/Hz, $\upsilon = 3$ e, por questões de simplicidade, consideramos que Alice, *relay* e Bob são dispostos ao longo de uma linha, com $d_{\mathrm{AB}} = 100$ m enquanto o *relay* varia entre Alice e Bob ao longo desta mesma linha. Além do mais, assim como em (CUI et al., 2004), empregamos os seguintes parâmetros de uma rede de sensores sem fio: $P_{\mathrm{TX}} = 112{,}2$ mW, $P_{\mathrm{RX}} = 97{,}9$ mW, $\omega = 1{,}86$, $B = 10$ kHz e $N_0 = -174$ dBm/Hz. Consideramos também uma margem de enlace de $M_l = 20$ dB, ganho total de antenas igual a $G = 5$ dBi, figura de ruído com $N_f = 10$ dB e frequência de portadora igual a $f_c = 2{,}5$ GHz.

Algoritmo 1 Algoritmo de Alocação Proposto

Entrada: $\eta_{\mathrm{s}}^{(\mathrm{esq})}$ e tolerâncias ϵ, ϵ_{P}, ϵ_{θ}

Inicialização: $m = 1$, $\eta_{\mathrm{s},0}^{(\mathrm{esq})} = 0$ e $\eta_{\mathrm{s},1}^{(\mathrm{esq})} = \eta_{\mathrm{s}}^{(\mathrm{esq})}$

Enquanto $\eta_{\mathrm{s},m}^{(\mathrm{esq})} - \eta_{\mathrm{s},m-1}^{(\mathrm{esq})} \geq \epsilon$ **faça**

; Alocação de potência de P_{A};

Inicialização: $\lambda_0 = 0$, $n = 0$

Enquanto $|F(\lambda_n)| \geq \epsilon_{\mathrm{P}}$ **faça**

Use $\lambda = \lambda_n$ em (49) para obter P_{A_n};

$\lambda_{n+1} = \frac{f_1(P_{\mathrm{A}_n})}{f_2(P_{\mathrm{A}_n})}$;

$n++$;

fim

$P_{\mathrm{A}_m}^{\star} = P_{\mathrm{A}_n}$;

; Alocação de potência de P_{R};

Inicialização: $n = 0$

Enquanto $|F(\lambda_n)| \geq \epsilon_{\mathrm{P}}$ **faça**

Use $\lambda = \lambda_n$ em (49) para obter P_{R_n};

$\lambda_{n+1} = \frac{f_1(P_{\mathrm{R}_n})}{f_2(P_{\mathrm{R}_n})}$;

$n++$;

fim

$P_{\mathrm{R}_m}^{\star} = P_{\mathrm{R}_n}$;

; Alocação de θ;

Inicialização: $\vartheta_0 = (\theta_1, \theta_3, \theta_2)$, $n = 1$

Enquanto $|\theta_1 - \theta_2| \geq \epsilon_{\theta}$ **faça**

Encontre θ_4 pela interpolação parabólica;

Se $\eta_{\mathrm{s}}^{(\mathrm{esq})}(\theta_4) > \eta_{\mathrm{s}}^{(\mathrm{esq})}(\theta_3)$: $\theta_1 = \theta_3$ e $\theta_3 = \theta_4$;

Senão: $\theta_2 = \theta_4$;

Calcule o tripleto ϑ_n utilizando os novos $(\theta_1, \theta_3, \theta_2)$;

$n++$

fim

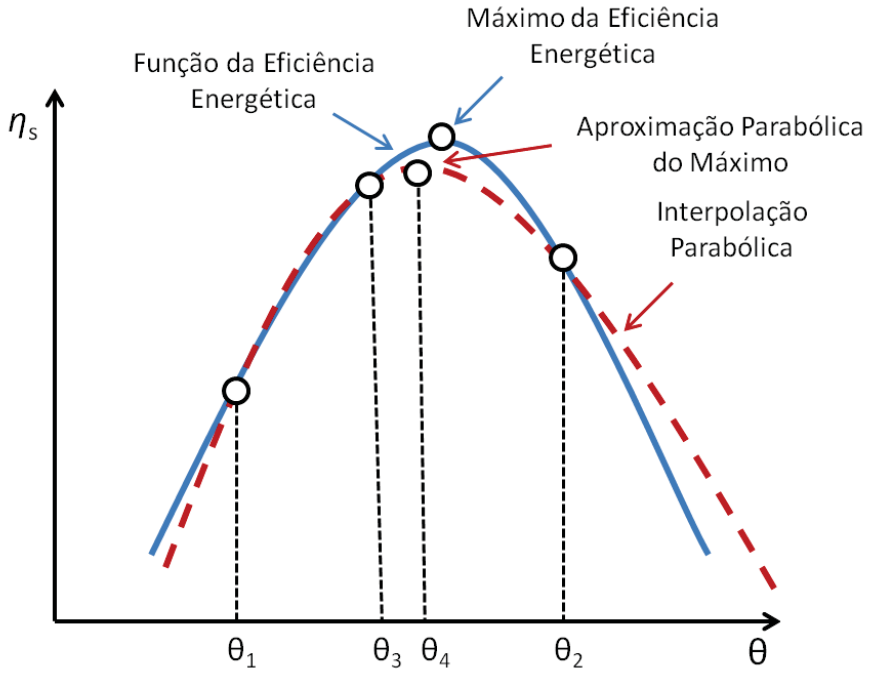
$\theta_m^{\star} = \theta_4$;

$m++$;

Calcule $\eta_{\mathrm{s},m}^{(\mathrm{esq})}$ utilizando $P_{\mathrm{A}_{m-1}}^{\star}$, $P_{\mathrm{R}_{m-1}}^{\star}$ e $\theta_{m-1}^{\star}$;

fim

Figura 9 – Alocação de θ utilizando o algoritmo de *golden section search* com interpolação parabólica.



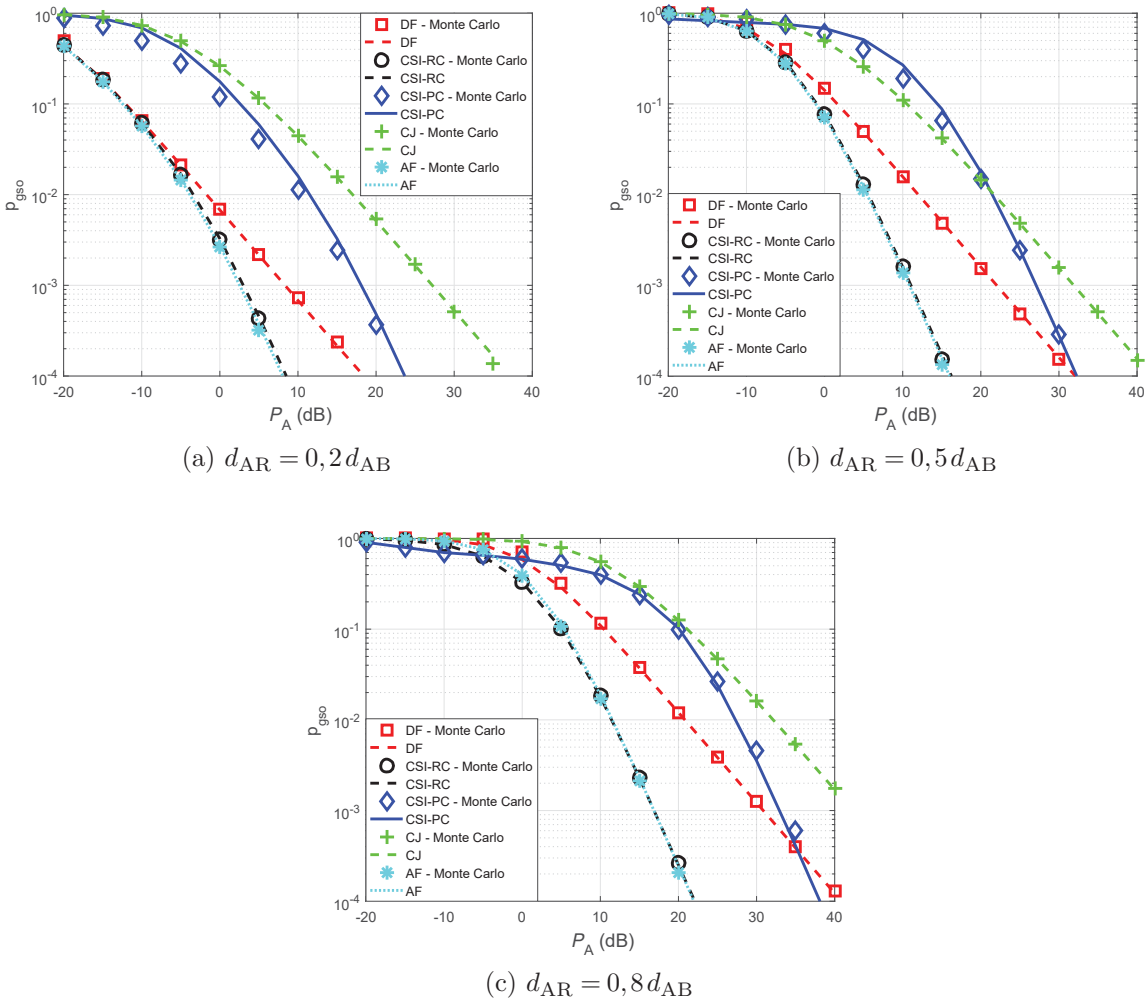
Fonte: Autoria própria.

3.3.1 Validação Numérica

Primeiramente na Figura 10 comparamos as expressões derivadas das probabilidades generalizadas de *outage* de segurança com as simulações por Monte Carlo para $d_{\mathrm{AR}} = 0,2\,d_{\mathrm{AB}}$ na Figura 10a, para $d_{\mathrm{AR}} = 0,5\,d_{\mathrm{AB}}$ na Figura 10b e para $d_{\mathrm{AR}} = 0,8\,d_{\mathrm{AB}}$ na Figura 10c. Como é possível observar, uma ótima concordância entre cada par de curvas é obtida. Além disto, a Figura 10 demonstra que a aproximação considerada no Lema 1, para o esquema CSI-PC, é muito próxima ao caso exato independentemente do posicionamento do *relay*.

Na Figura 11 comparamos a SEE para o esquema CSI-RC considerando valores fixos de $\theta \in \{0,3; 0,7; 1,0\}$. Consideramos o *relay* posicionado no ponto médio entre Alice e Bob, enquanto variamos a SNR do canal Alice-Bob ($\bar{\gamma}_{\mathrm{AB}}$) para uma SNR fixa em Eve, com $\bar{\gamma}_{\mathrm{AE}} = 9$ dB e $\bar{\gamma}_{\mathrm{RE}} = 13$ dB. Desta forma, para cada $\bar{\gamma}_{\mathrm{AB}}$ realizamos a alocação de potência no *relay* utilizando o algoritmo Dinkelbach e uma abordagem com busca exaustiva. Como podemos observar o algoritmo Dinkelbach apresenta resultados muito semelhantes à solução com busca exaustiva, porém com a vantagem de ser implementado com uma baixa complexidade e convergindo com uma taxa super-linear, como mostrado em (ZAPPONE; JORSWIECK, 2014). Além do mais, é interessante observar que η_{s} varia

Figura 10 – Comparação entre as expressões obtidas para probabilidade generalizada de *outage* de segurança com as simulações por Monte Carlo considerando $\theta = 1$ para diferentes posições do *relay* entre Alice e Bob.



(a) $d_{\mathrm{AR}} = 0,2\,d_{\mathrm{AB}}$ (b) $d_{\mathrm{AR}} = 0,5\,d_{\mathrm{AB}}$

(c) $d_{\mathrm{AR}} = 0,8\,d_{\mathrm{AB}}$

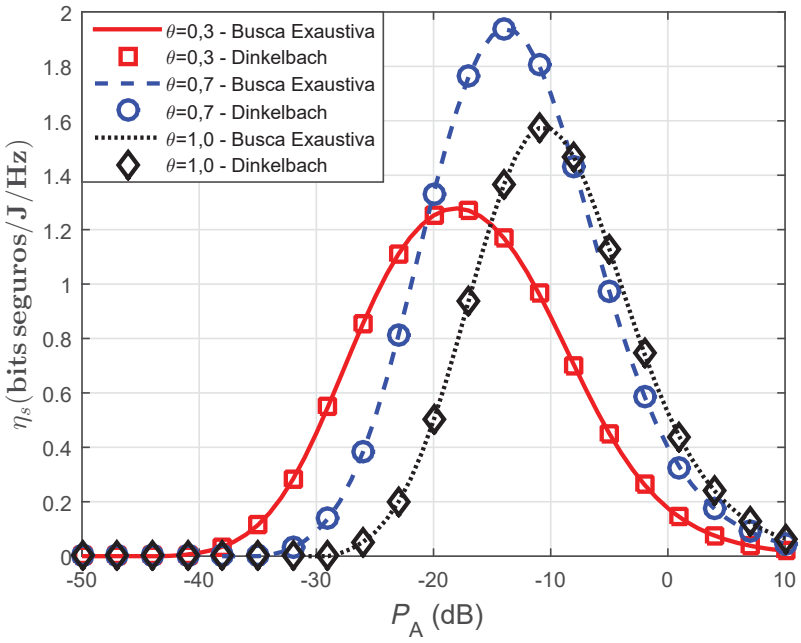
Fonte: Autoria própria.

consideravelmente com θ. Ressaltamos também que diferentes valores de θ implicam na maximização da SEE para diferentes $\bar{\gamma}_{\mathrm{AB}}$, indicando que uma otimização conjunta de θ e potência permite otimizar consideravelmente os valores de SEE para os esquemas cooperativos.

3.3.2 Otimização de Potência

Estendendo a análise para diferentes esquemas cooperativos, considerando otimizações de potências em Alice e no *relay*, na Figura 12 comparamos a SEE dos esquemas cooperativos CSI-RC, CSI-PC, DF, AF e CJ em função de θ. Nota-se que os esquemas AF e DF são sempre superados pelos esquemas CSI-RC e CSI-PC, devido ao

Figura 11 – SEE do esquema cooperativo CSI-RC para valores fixos de θ, enquanto a alocação de potência no *relay* é realizada utilizando o algoritmo Dinkelbach e uma abordagem por busca exaustiva.

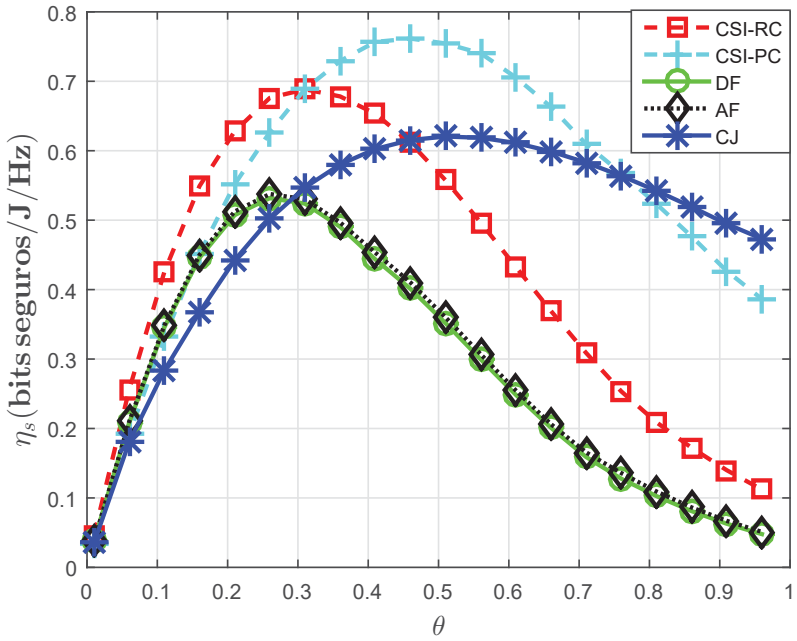


Fonte: Autoria própria.

fato que estes esquemas exploram completamente a CSI disponível em Alice para escolha entre a transmissão direta ou pelo *relay*. Adicionalmente, a Figura 12 demonstra que o esquema CSI-PC não é a melhor estratégia para todos os cenários. Diferentemente de (KHORMUJI; LARSSON, 2009), em que o esquema de codificação paralela supera o esquema com codificação de repetição quando a confidencialidade não é considerada, a Figura 12 demonstra que existem regiões em que o esquema CSI-RC apresenta um melhor desempenho. Isto ocorre devido ao fato das capacidades com relação a Bob e a Eve aumentarem em diferentes proporções de acordo com o incremento de θ. Portanto, quando uma métrica de confidencialidade que depende de θ é considerada, o esquema CSI-PC pode ser mais benéfico a Eve do que a Bob, tornando o esquema CSI-RC mais vantajoso. Com relação ao esquema CJ, é interessante ressaltar que pelo fato do ruído injetado pelo *relay* afetar tanto Eve quanto Bob, a alocação de potência tem um papel importante no estabelecimento da potência ótima que permite interferir em Eve porém não demasiadamente de modo a tornar a comunicação entre Alice e Bob inviável. Pelo fato do esquema CJ também ter um melhor desempenho em algumas situações, abordaremos os esquemas CSI-RC, CSI-PC e CJ para as próximas análises.

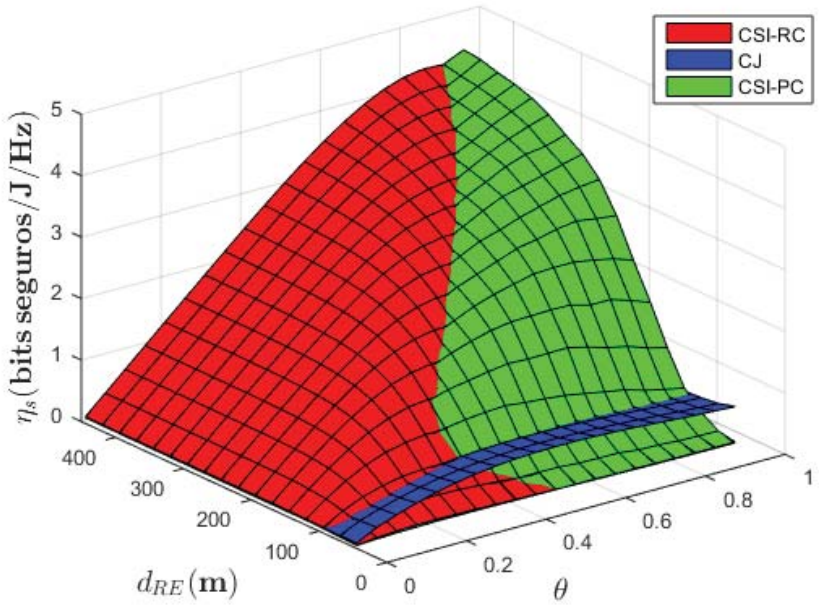
As Figuras 13 e 14 comparam η_s para os três esquemas cooperativos em função de

Figura 12 – SEE do CJ, AF, DF, CSI-RC e CSI-PC em função de θ para $d_{\mathrm{RE}} = 1,3\,d_{\mathrm{AB}}$ e $d_{\mathrm{AR}} = 0,2\,d_{\mathrm{AB}}$.



Fonte: Autoria própria.

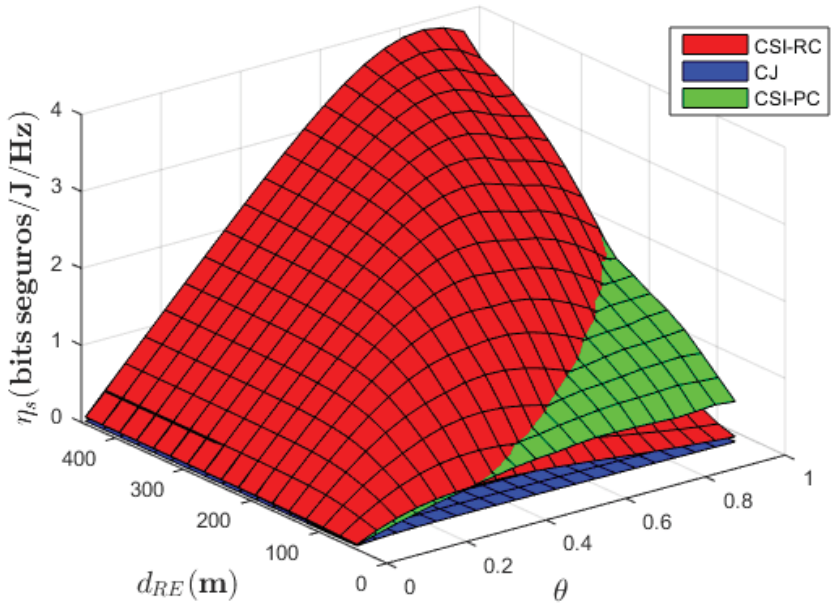
Figura 13 – $\eta_{\mathrm{s}}^{(\mathrm{CSI\text{-}RC})}$, $\eta_{\mathrm{s}}^{(\mathrm{CSI\text{-}PC})}$ e $\eta_{\mathrm{s}}^{(\mathrm{CJ})}$ em função de d_{RE} e θ para $d_{\mathrm{AR}} = 0,2\,d_{\mathrm{AB}}$.



Fonte: Autoria própria.

d_{RE} e θ enquanto $d_{\mathrm{AR}} = 0,2d_{\mathrm{AB}}$ (Figura 13) e $d_{\mathrm{AR}} = 0,8d_{\mathrm{AB}}$ (Figura 14). Como podemos observar, o desempenho de cada esquema cooperativo depende consideravelmente do

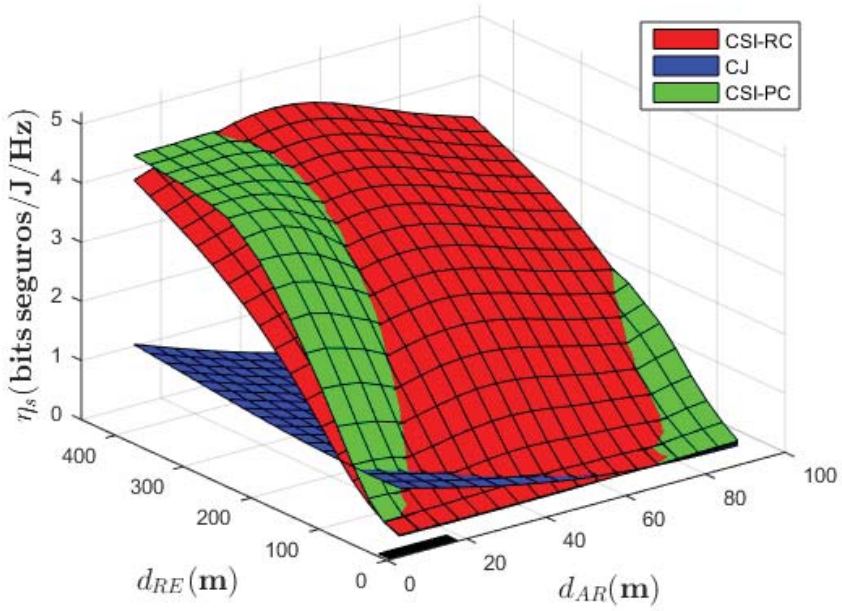
Figura 14 – $\eta_s^{(\text{CSI-RC})}$, $\eta_s^{(\text{CSI-PC})}$ e $\eta_s^{(\text{CJ})}$ em função de d_{RE} e θ para $d_{\text{AR}} = 0,8\,d_{\text{AB}}$.



Fonte: Autoria própria.

posicionamento do *relay* e de Eve. Considerando o *relay* próximo à Alice, os esquemas CSI-RC, CSI-PC e CJ apresentam diferentes regiões nas quais cada esquema apresenta um melhor desempenho. Por exemplo, quando Eve está próxima aos nós legítimos, é mais benéfico para o *relay* atacar Eve através de *jamming* do que auxiliar Alice pela cooperação. Desta forma, o esquema CJ apresenta uma melhor desempenho, como a Figura 13 demonstra em uma região com baixos valores de d_{RE}. Contudo, se o *relay* está próximo à Bob, o ruído Gaussiano injetado pelo esquema CJ também afeta o desempenho de Bob, de forma que, como mostrado na Figura 14, a SEE do esquema CJ decai consideravelmente. Já o esquema CSI-PC permite aumentar a SEE do sistema quando $\theta \to 1$ e o *relay* está em uma das seguintes situações: *i)* está próximo à Alice (Figura 13); *ii)* está próximo à Bob, e Eve está próxima ao *relay* (Figura 14); contudo, quando θ pode ser relaxado e de maneira mais expressiva quando o *relay* está mais próximo a Bob, o CSI-RC permite importantes ganhos em comparação com o CSI-PC. Tal comportamento dos esquemas a partir da variação da posição do *relay*, com o esquema CSI-RC apresentando importantes ganhos na Figura 14, ocorre pelo fato de que, quando o *relay* está mais próximo a Bob, o aumento da capacidade de confidencialidade do esquema CSI-PC é limitado pelo canal de Eve, visto que as novas informações sobre a mensagem auxiliam Eve mais intensamente do que no caso com o *relay* mais próximo a Alice.

Figura 15 – SEE em função de d_{RE} e d_{AR} a partir de uma otimização conjunta de θ e potência através do algoritmo proposto.

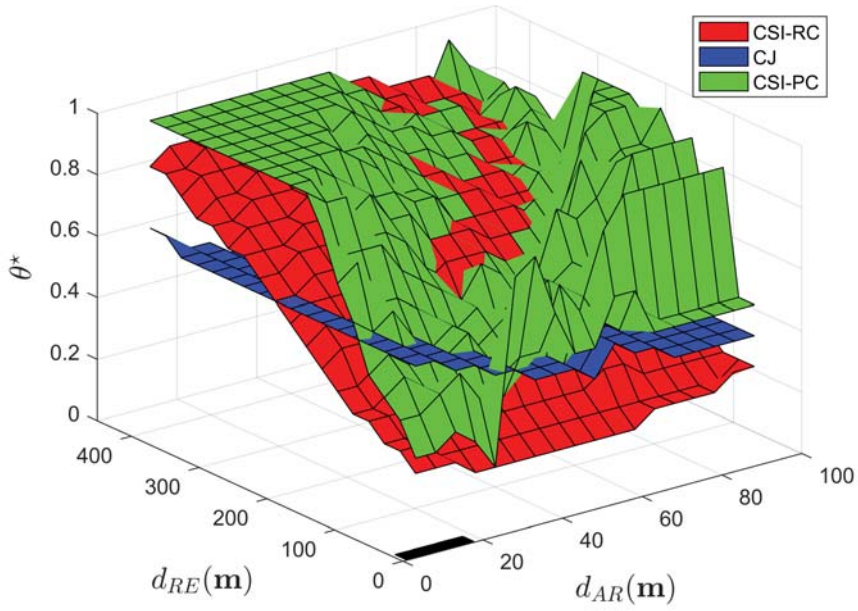


Fonte: Autoria própria.

3.3.3 Otimização Conjunta de Potência e θ

Para melhor visualização dos cruzamentos entre os esquemas CSI-RC, CSI-PC e CJ, na Figura 15 comparamos $\eta_{\mathrm{s}}^{(\mathrm{CSI\text{-}RC})}$, $\eta_{\mathrm{s}}^{(\mathrm{CSI\text{-}PC})}$ e $\eta_{\mathrm{s}}^{(\mathrm{CJ})}$ utilizando uma alocação conjunta de potência e θ, empregando o Algoritmo 1 proposto na Seção 3.2, enquanto variamos d_{RE} e d_{AR}. Como podemos observar, o esquema CSI-PC supera o esquema CSI-RC somente quando o *relay* está em um extremo, muito próximo à Alice ou a Bob. Apesar disto, uma melhoria significativa é observada nestas regiões. Adicionalmente, o esquema CJ supera outros esquemas quando Eve está próxima aos nós legítimos. Já a Figura 16 demonstra o comportamento do θ ótimo para cada esquema cooperativo a partir da alocação conjunta considerada no Algoritmo 1. Como é possível observar, os esquemas CSI-RC e CSI-PC apresentam um valor de θ próximo a um quando a distância de Eve com relação ao *relay* aumenta. Tal comportamento ocorre pelo fato que, com o aumento da distância de Eve com relação aos nós legítimos, as condições de segurança do sistema podem ser restringidas de modo a maximizar o *throughput* seguro e, consequentemente, a eficiência energética segura. Adicionalmente é possível observar que, com a proximidade do *relay* a Bob, conforme é possível observar também pela Figura 14, o esquema CSI-PC apresenta importantes ganhos de desempenho quando $\theta \to 1$.

Figura 16 – $\theta^\star$ em função de d_{RE} e d_{AR} a partir de uma otimização conjunta de θ e potência através do algoritmo proposto.

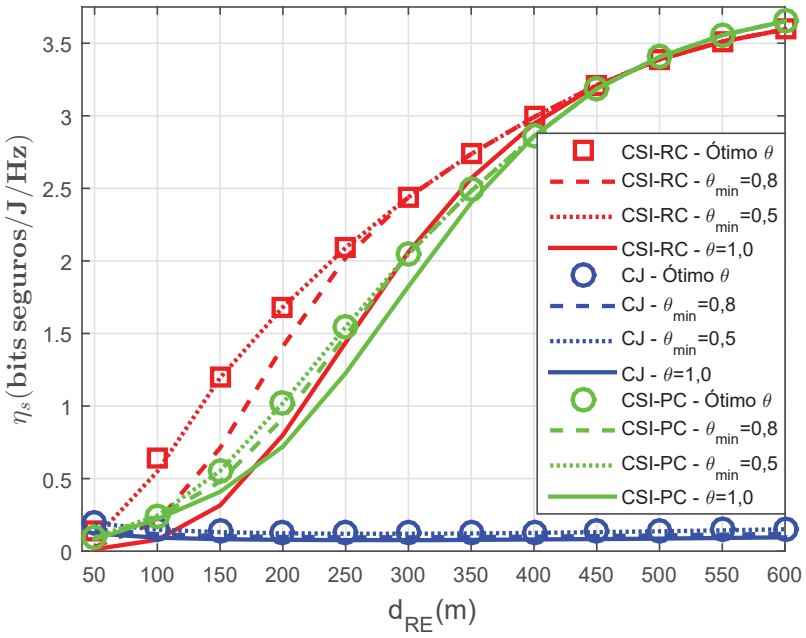


Fonte: Autoria própria.

A Figura 15 demonstra que uma alocação conjunta de θ e potência permite otimizar a SEE do sistema. Porém, dependendo da aplicação, o ótimo θ não pode ser aplicado, devido a um mínimo requisito de segurança que deve ser cumprido. Desta forma, na Figura 17 comparamos $\eta_{\mathrm{s}}^{(\mathrm{CSI\text{-}RC})}$, $\eta_{\mathrm{s}}^{(\mathrm{CSI\text{-}PC})}$ e $\eta_{\mathrm{s}}^{(\mathrm{CJ})}$ realizando uma otimização conjunta de θ e potência, considerando diferentes requisitos mínimos de confidencialidade. Consideramos o caso de otimização de potência com um valor fixo de $\theta = 1$, representando um cenário em que a segurança não pode ser relaxada, e dois cenários nos quais os requisitos mínimos são $\theta \in \{0,5; 0,8\}$, além do caso sem restrição nos valores de θ. Como podemos verificar pelos resultados numéricos, as conclusões gerais em termos de SEE são mantidas. Contudo, é interessante notar que, para os esquemas CSI-RC e CSI-PC, um valor aceitável de $\theta = 0,8$ permite obter valores de SEE consideravelmente maiores do que no caso com $\theta = 1$. Adicionalmente, um valor mínimo aceitável de $\theta = 0,5$ garante valores de SEE próximos ao caso sem restrições. Com relação ao esquema CJ, notamos que os resultados obtidos apresentam pequenas mudanças com relação a cada cenário de θ.

Finalmente, o comportamento de $\theta^\star$, o θ que maximiza a SEE, é mostrado na Figura 18 em função de d_{RE}. Como podemos observar, $\theta^\star$ para os esquemas CSI-RC e CSI-PC aumenta quando Eve está distante dos nós legítimos, uma vez que $p_{\mathrm{gso}}^{(\mathrm{CSI\text{-}RC})}$ e $p_{\mathrm{gso}}^{(\mathrm{CSI\text{-}PC})}$ diminuem enquanto d_{RE} aumenta, o que ocasiona em um aumento da SEE

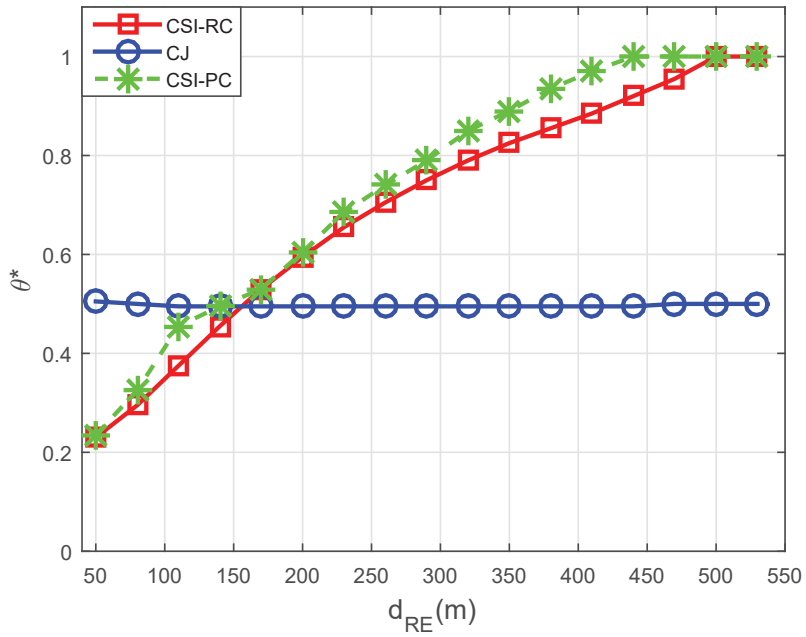
Figura 17 – SEE em função de d_{RE} a partir de uma otimização conjunta de θ e potência, com diferentes requisitos mínimos de confidencialidade para o sistema. O *relay* está posicionado em $d_{\mathrm{AR}} = 0,5 d_{\mathrm{AB}}$.



Fonte: Autoria própria.

com o aumento de θ. Por outro lado, $\theta^{\star}$ é praticamente constante para o esquema CJ, independentemente da posição de Eve. Isto ocorre pelo fato do desempenho relacionado à *outage* do CJ ser limitado pela interferência causado pelo *relay* em Bob, e, desta forma, a distância com respeito a Eve tem um impacto limitado na SEE. Cabe ressaltar que a mesma tendência para o comportamento de $\theta^{\star}$ é obtido para o *relay* mais próximo a Bob.

Figura 18 – Ótimo $\theta^{\star}$ que maximiza a eficiência energética segura para o CSI-RC, CSI-PC e CJ em função de d_{RE}. O *relay* está localizado em $d_{\mathrm{AR}} = 0,2d_{\mathrm{AB}}$.



Fonte: Autoria própria.

4 CONFIDENCIALIDADE EM CENÁRIOS MIMO

Neste capítulo estudamos a confidencialidade em cenários com múltiplas antenas nos nós legítimos e na escuta. Com relação ao cenário de CSI, similarmente ao Capítulo 3, consideramos o caso no qual apenas o comportamento do canal legítimo é conhecido. Desta forma, realizamos comparação entre dois protocolos cooperativos denominados CSI-DF e AN. No protocolo AN um vetor *beamforming* é desenvolvido a fim de que o *relay* injete um sinal de ruído no sistema que interfira somente em Eve, ou seja, sem prejudicar a comunicação entre os nós legítimos. Já no protocolo CSI-DF, os nós legítimos utilizam da CSI disponível para escolha entre o melhor caminho: direto ou cooperativo. Cabe ressaltar que o protocolo cooperativo CSI-DF considerado neste capítulo é uma extensão do protocolo CSI-RC da Subseção 3.1.1, a partir da utilização de múltiplas antenas em todos os nós. É importante destacar ainda que o protocolo CSI-RC é considerado, ao invés do CSI-PC, devido ao desempenho superior em grande parte dos cenários, conforme análise realizada na Subseção 3.3.

Nestes protocolos consideramos que Alice, Bob, *relay* e Eve apresentam, respectivamente, n_{A}, n_{B}, n_{R} e n_{E} antenas. Consideramos ainda que o protocolo TAS é empregado na transmissão enquanto o MRC é utilizado na recepção. Desta forma, Bob, ao receber a transmissão de Alice, informa o índice da melhor antena transmissora por um canal de retorno. A antena selecionada em Alice é um evento aleatório do ponto de vista do *relay* e Eve, de modo que não existe ganho de diversidade nestes nós. Desta forma, conforme (YANG et al., 2013), a razão sinal-ruído nos nós receptores seguem as seguintes funções densidade de probabilidade:

$$f_{i\mathrm{B}}^{\mathrm{TAS/MRC}}(\gamma) = \frac{n_i\,\gamma^{n_{\mathrm{B}}-1}\,e^{-\frac{\gamma}{\bar{\gamma}}}}{\Gamma(n_{\mathrm{B}})\,\bar{\gamma}^{n_{\mathrm{B}}}}\left(1-e^{-\frac{\gamma}{\bar{\gamma}}}\sum_{k=0}^{n_{\mathrm{B}}-1}\frac{\gamma^k}{k!\bar{\gamma}^k}\right)^{n_i-1} \tag{51}$$

em Bob, devido a combinação do TAS e MRC, e

$$f_{ij}^{\mathrm{MRC}}(\gamma) = \frac{\gamma^{n_j-1}\,e^{-\frac{\gamma}{\bar{\gamma}}}}{\Gamma(n_j)\,\bar{\gamma}^{n_j}} \tag{52}$$

no *relay* e em Eve devido a utilização do MRC, onde $\Gamma(.)$ é a função gamma completa (GRADSHTEYN; RYZHIK, 2007, §8.339.1), $i \in \{\mathrm{A},\mathrm{R}\}$ e $j \in \{\mathrm{R},\mathrm{E}\}$, com $i \neq j$. Para o caso em que consideramos apenas o MRC, a função distribuição acumulada (CDF,

do inglês *Cumulative Distribution Function*) pode ser definida como (LIN et al., 2016)

$$F_{ij}^{\mathrm{MRC}}(\gamma) = 1 - e^{-\frac{\gamma}{\bar{\gamma}}} \sum_{w=0}^{n_j-1} \left(\frac{1}{w!}\right) \left(\frac{\gamma}{\bar{\gamma}}\right)^{w}. \tag{53}$$

4.1 PROTOCOLOS MIMO DE TRANSMISSÃO COOPERATIVA

Nesta seção derivamos as equações das probabilidades de *outage* de segurança para os esquemas cooperativos CSI-DF e AN considerando múltiplas antenas nos nós legítimos e em Eve.

4.1.1 CSI-Aided Decode-and-Forward (CSI-DF)

Usualmente, uma dada realização do canal é estimada a partir de uma sequência de símbolos de treinamento enviado pelo transmissor. A partir desta sequência, o receptor decompõe a informação do canal obtida, $\mathbf{h}$, em uma informação da direção do canal CDI (do inglês, *Channel Direction Information*) e uma informação do ganho do canal CGI (do inglês, *Channel Gain Information*) , denotado por $||\mathbf{h}||$ (ZHANG et al., 2014, 2015). A CGI é real e positiva, de modo que pode ser eficientemente quantizada em um pequeno número de bits (YOO et al., 2007), enquanto a CDI é um vetor complexo com o mesmo número de dimensões do que o número de antenas receptoras (ZHANG et al., 2014, 2015), portanto, complexo de ser quantificado. Visto que empregamos o protocolo TAS nos transmissores, somente a CGI é necessária, o que permite reduzir o uso do *feedback*, permitindo uma implementação mais prática. Desta forma, com a disponibilidade da CGI, o esquema CSI-DF proposto permite realizar escolha entre o caminho mais vantajoso: direto ou cooperativo. Se a cooperação é escolhida, o *relay* emprega o esquema DF para reencaminhar a informação para Bob no segundo intervalo de tempo. Caso contrário, se o caminho direto é mais vantajoso, consideramos que Alice transmite a informação novamente no segundo intervalo de tempo a fim de realizar uma comparação justa com o protocolo cooperativo. Desta forma, a capacidade do canal legítimo é dada por

$$C_{\mathrm{L}}^{(\text{CSI-DF})} = \frac{1}{2} \max\{\log_2\left(1+\gamma'_{\mathrm{AB}}\right), \min\left\{\log_2\left(1+\gamma_{\mathrm{AR}}\right), \log_2\left(1+\gamma_{\mathrm{B}}\right)\right\}\}, \tag{54}$$

onde $\gamma_{\mathrm{B}} = \gamma_{\mathrm{AB}} + \gamma_{\mathrm{RB}}$ é a SNR equivalente em Bob quando a cooperação ocorre e $\gamma'_{\mathrm{AB}} = \gamma_{\mathrm{AB},1} + \gamma_{\mathrm{AB},2}$ é a SNR equivalente quando Alice transmite em dois intervalos de tempo consecutivos.

Em Eve, consideramos uma suposição otimista com relação a capacidade do canal (pessimista em termos da capacidade de confidencialidade), de forma que

$$C_{\mathrm{E}}^{(\text{CSI-DF})} = \frac{1}{2}\log_2(1+\gamma_{\mathrm{AE}}+\gamma_{\mathrm{RE}}), \tag{55}$$

o qual assume que o *relay* sempre participa da transmissão legítima. Cabe ressaltar que esta suposição é realizada para permitir obtermos uma expressão fechada para SOP utilizando o máximo entre variáveis aleatórias idênticas e independentemente distribuídas.

Considerando duas variáveis aleatórias idênticas e independentemente distribuídas, X_1 e X_2, o máximo e mínimo entre elas podem ser escritas, seguindo (Papoulis; Pillai, 2002), por

$$\Pr\{\max(X_1,X_2)\leq x\} = \Pr\{X_1\leq x\}\Pr\{X_2\leq x\} \tag{56}$$

$$\Pr\{\min(X_1,X_2)\leq x\} = \Pr\{X_1\leq x\}+\Pr\{X_1> x\}\Pr\{X_2\leq x\} \tag{57}$$

de forma que com uma abordagem similar a (LANEMAN et al., 2004), a partir de (56) e (57), e considerando que a correlação entre γ'_{AB} e γ_{B} é tratada como em (LANEMAN et al., 2004), a expressão de SOP pode ser escrita como

$$p_{\mathrm{out}}^{(\text{CSI-DF})} = \mathcal{O}_{\mathrm{ABE}}\left[\mathcal{O}_{\mathrm{ARE}}+(1-\mathcal{O}_{\mathrm{ARE}})\,\mathcal{O}_{\mathrm{BE}}\right], \tag{58}$$

onde

$$\mathcal{O}_{\mathrm{ABE}} = \Pr\left\{\left(\frac{1+\gamma'_{\mathrm{AB}}}{1+\gamma_{\mathrm{E}}}\right) < 2^{2\mathcal{R}}\right\}, \tag{59}$$

$$\mathcal{O}_{\mathrm{ARE}} = \Pr\left\{\left(\frac{1+\gamma_{\mathrm{AR}}}{1+\gamma_{\mathrm{E}}}\right) < 2^{2\mathcal{R}}\right\} \tag{60}$$

e

$$\mathcal{O}_{\mathrm{BE}} = \Pr\left\{\left(\frac{1+\gamma_{\mathrm{B}}}{1+\gamma_{\mathrm{E}}}\right) < 2^{2\mathcal{R}}\right\} \tag{61}$$

com $\gamma_{\mathrm{E}} = \gamma_{\mathrm{AE}}+\gamma_{\mathrm{RE}}$.

Em seguida, isolando γ_{E} para cada variável em (58) obtém-se

$$\begin{aligned} p_{\mathrm{out}}^{(\text{CSI-DF})} = &\Pr\{\gamma_{\mathrm{E}} > 2^{-2\mathcal{R}}\left(1+\gamma'_{\mathrm{AB}}\right)-1\}\Big[\Pr\{\gamma_{\mathrm{E}} > 2^{-2\mathcal{R}}(1+\gamma_{\mathrm{AR}})-1\} \\ &+\Pr\{\gamma_{\mathrm{E}} \leq 2^{-2\mathcal{R}}(1+\gamma_{\mathrm{AR}})-1\}\Pr\{\gamma_{\mathrm{E}} > 2^{-2\mathcal{R}}(1+\gamma_{\mathrm{B}})-1\}\Big], \end{aligned} \tag{62}$$

a qual requer a PDF relacionada a γ_{B} e a CDF relacionada a γ_{E} para ser resolvida de forma fechada.

Considerando as convoluções definidas por (LIN et al., 2016), a PDF relacionada a γ_{B} e a CDF relacionada a γ_{E} podem ser obtidas a partir de

$$f_{\mathrm{B}}(x) = \int_0^x f_{\mathrm{RB}}^{\mathrm{TAS/MRC}}(x-y)\, f_{\mathrm{AB}}^{\mathrm{TAS/MRC}}(y)\,\mathrm{d}y, \tag{63}$$

$$F_{\mathrm{E}}(x) = \int_0^x F_{\mathrm{RE}}^{\mathrm{MRC}}(x-y)\, f_{\mathrm{AE}}^{\mathrm{MRC}}(y)\,\mathrm{d}y, \tag{64}$$

as quais podem ser resolvidas a partir de (CHOI et al., 2005, eq. (8)), (GRADSHTEYN; RYZHIK, 2007, §1.111), (GRADSHTEYN; RYZHIK, 2007, §3.351.1) e (GRADSHTEYN; RYZHIK, 2007, §3.381.1), resultando em

$$\begin{aligned} f_{\mathrm{B}}(x) = {} & \frac{n_{\mathrm{R}} n_{\mathrm{A}} \Gamma(n_{\mathrm{B}})^{-2}}{(\bar{\gamma}_{\mathrm{RB}}\bar{\gamma}_{\mathrm{AB}})^{n_{\mathrm{B}}}} \sum_{k=0}^{n_{\mathrm{A}}-1} \sum_{m=0}^{n_{\mathrm{R}}-1} \binom{n_{\mathrm{A}}-1}{k} \binom{n_{\mathrm{R}}-1}{m} (-1)^{m+k} \prod_{\bar{\gamma}_{\mathrm{AB}}} \prod_{\bar{\gamma}_{\mathrm{AR}}} e^{-x\left(\frac{k+1}{\bar{\gamma}_{\mathrm{AB}}}\right)} \\ & \times x^{n_{\mathrm{B}}+\beta_1-1-l} \sum_{l=0}^{n_{\mathrm{B}}+\beta_1-1} \binom{n_{\mathrm{B}}+\beta_1-1}{l} (-1)^{l} \left[\left(\frac{m+1}{\bar{\gamma}_{\mathrm{RB}}} - \frac{k+1}{\bar{\gamma}_{\mathrm{AB}}} \right)^{-(n_{\mathrm{B}}+\beta_2+l)} \right] \\ & \times \hat{\gamma}\left(n_{\mathrm{B}}+\beta_2+l; \left[\frac{m+1}{\bar{\gamma}_{\mathrm{RB}}} - \frac{k+1}{\bar{\gamma}_{\mathrm{AB}}} \right] x \right), \end{aligned} \tag{65}$$

onde $\hat{\gamma}(.)$ é a função gamma incompleta,

$$\prod_{\bar{\gamma}_{\mathrm{AB}}} = \prod_{i=1}^{n_{\mathrm{B}}-1} \left[\sum_{u_i=0}^{u_{i-1}} \binom{u_{i-1}}{u_i} \left(\frac{1}{i!}\right)^{u_i-u_{i+1}} \left(\frac{1}{\bar{\gamma}_{\mathrm{AB}}} \right)^{u_i} \right] \tag{66}$$

com $\beta_1 = \sum_{i=1}^{n_{\mathrm{B}}-1} u_i$, $u_0 = k$ e $u_{n_{\mathrm{B}}} = 0$,

$$\prod_{\bar{\gamma}_{\mathrm{AR}}} = \prod_{i=1}^{n_{\mathrm{R}}-1} \left[\sum_{v_i=0}^{v_{i-1}} \binom{v_{i-1}}{v_i} \left(\frac{1}{i!}\right)^{v_i-v_{i+1}} \left(\frac{1}{\bar{\gamma}_{\mathrm{AR}}} \right)^{v_i} \right], \tag{67}$$

com $\beta_2 = \sum_{i=1}^{n_{\mathrm{R}}-1} v_i$, $v_0 = m$ e $v_{n_{\mathrm{R}}} = 0$ e

$$\begin{aligned} F_{\mathrm{E}}(x) = {} & \frac{1}{\bar{\gamma}_{\mathrm{AE}}^{n_{\mathrm{E}}} \Gamma(n_{\mathrm{E}})} \left[\frac{(n_{\mathrm{E}}-1)!}{\bar{\gamma}_{\mathrm{AE}}^{-n_{\mathrm{E}}}} - e^{-\frac{x}{\bar{\gamma}_{\mathrm{AE}}}} \sum_{m=0}^{n_{\mathrm{E}}-1} \frac{(n_{\mathrm{E}}-1)!}{m!} \frac{x^m}{\bar{\gamma}_{\mathrm{AE}}^{m-n_{\mathrm{E}}}} - \sum_{w=0}^{n_{\mathrm{E}}-1} \left(\frac{1}{w!}\right) \left(\frac{1}{\bar{\gamma}_{\mathrm{RE}}} \right)^{w} e^{-\frac{x}{\bar{\gamma}_{\mathrm{RE}}}} \right. \\ & \left. \sum_{k=0}^{w} \binom{w}{k} (-1)^k\, x^{w-k} \left\{ \frac{(k+n_{\mathrm{E}}-1)!}{\left[\frac{1}{\bar{\gamma}_{\mathrm{AE}}} - \frac{1}{\bar{\gamma}_{\mathrm{RE}}}\right]^{k+n_{\mathrm{E}}}} - e^{-x\left(\frac{1}{\bar{\gamma}_{\mathrm{AE}}} - \frac{1}{\bar{\gamma}_{\mathrm{RE}}}\right)} \sum_{m=0}^{k+n_{\mathrm{E}}-1} \frac{(k+n_{\mathrm{E}}-1)! x^m}{m! \left(\frac{1}{\bar{\gamma}_{\mathrm{AE}}} - \frac{1}{\bar{\gamma}_{\mathrm{RE}}}\right)^{k+n_{\mathrm{E}}-m}} \right\} \right]. \end{aligned} \tag{68}$$

A partir destas expressões, a solução de (58), iniciando com $\mathcal{O}_{\mathrm{ABE}}$, empregando

$f_{\mathrm{AB}}^{\mathrm{TAS/MRC}}$ e F_{E}, é dada por

$$\mathcal{O}_{\mathrm{ABE}} = \int_0^{\infty} F_{\mathrm{E}}\left[2^{-2\mathcal{R}}\left(1+\gamma'_{\mathrm{AB}}\right)-1\right] f_{\mathrm{AB}}^{\mathrm{TAS/MRC}}\left(\gamma'_{\mathrm{AB}}\right) \mathrm{d}\gamma'_{\mathrm{AB}} \tag{69}$$

a qual, utilizando a expansão binomial, aplicando (GRADSHTEYN; RYZHIK, 2007, §3.35.3), (CHOI et al., 2005, eq. (8)) e após manipulações algébricas, resulta em

$$\begin{aligned}\mathcal{O}_{\mathrm{ABE}} = {} & \frac{n_{\mathrm{A}}}{\Gamma(n_{\mathrm{B}})\,\Gamma(n_{\mathrm{E}})\;\bar{\gamma}_{\mathrm{AB}}^{n_{\mathrm{B}}}\;\bar{\gamma}_{\mathrm{AE}}^{n_{\mathrm{E}}}} \sum_{k=0}^{n_{\mathrm{A}}-1} \binom{n_{\mathrm{A}}-1}{k} (-1)^k \prod_{\bar{\gamma}_{\mathrm{AB}}} \times \left\{ \frac{(n_{\mathrm{E}}-1)!}{\bar{\gamma}_{\mathrm{AE}}^{-n_{\mathrm{E}}}} \mathcal{X}(0,0,\frac{k+1}{\bar{\gamma}_{\mathrm{AB}}}) \right. \\ & - e^{-\frac{2^{-2\mathcal{R}}-1}{\bar{\gamma}_{\mathrm{AE}}}} \sum_{m=0}^{n_{\mathrm{E}}-1} \frac{m!\Gamma(n_{\mathrm{E}})}{\bar{\gamma}_{\mathrm{AE}}^{m-n_{\mathrm{E}}}} \times \sum_{v=0}^{m} \binom{m}{v} \mathcal{X}\left(m,v,\phi(\bar{\gamma}_{\mathrm{AE}})\right) - \sum_{w=0}^{n_{\mathrm{E}}-1} \sum_{v=0}^{w} \frac{(-1)^v}{w!} \left(\frac{1}{\bar{\gamma}_{\mathrm{RE}}}\right)^w \\ & \times \left[e^{-\frac{2^{-2\mathcal{R}}-1}{\bar{\gamma}_{\mathrm{RE}}}} \sum_{z=0}^{w-v} \binom{w}{v} \mathcal{Z}(0)\; \mathcal{X}(w-v,z,\phi(\bar{\gamma}_{\mathrm{RE}})) \;-\; e^{-\frac{2^{-2\mathcal{R}}-1}{\bar{\gamma}_{\mathrm{AE}}}} \sum_{z=0}^{w-v} \sum_{m=0}^{v+n_{\mathrm{E}}-1} \right. \\ & \left. \left. \sum_{y=0}^{m} \binom{w}{v} \binom{m}{y} \mathcal{Z}(m) \mathcal{X}(w+m-v, z+y, \phi(\bar{\gamma}_{\mathrm{AE}})) \right] \right\}, \end{aligned} \tag{70}$$

onde

$$\phi(a) = \frac{k+1}{\bar{\gamma}_{\mathrm{AB}}} + \frac{2^{-2\mathcal{R}+1}}{a}, \tag{71}$$

$$\mathcal{Z}(x) = \frac{(v+n_{\mathrm{E}}-1)!}{x!\left(\frac{\bar{\gamma}_{\mathrm{RE}}-\bar{\gamma}_{\mathrm{AE}}}{\bar{\gamma}_{\mathrm{RE}}\bar{\gamma}_{\mathrm{AE}}}\right)^{v+n_{\mathrm{E}}-x}}, \tag{72}$$

$$\mathcal{X}(a,b,c) = \frac{(2^{-2\mathcal{R}}-1)^{a-b}(b+\beta_1+n_{\mathrm{B}}-1)!}{2^{b(-2\mathcal{R}+1)}c^{(b+\beta_1+n_{\mathrm{B}})}}. \tag{73}$$

Já a resolução de $\Pr\{\gamma_{\mathrm{E}} > 2^{-2\mathcal{R}}(1+\gamma_{\mathrm{AR}})-1\}$ resulta na seguinte integral

$$\mathcal{O}_{\mathrm{ARE}} = \int_0^{\infty} F_{\mathrm{E}}\left[2^{-2\mathcal{R}}(1+\gamma_{\mathrm{AR}})-1\right] f_{\mathrm{AR}}^{\mathrm{MRC}}(\gamma_{\mathrm{AR}})\,\mathrm{d}\gamma_{\mathrm{AR}}, \tag{74}$$

a qual pode ser resolvida de forma fechada utilizando as expressões de $f_{\mathrm{AR}}^{\mathrm{MRC}}$ e F_{E} definidas anteriormente, a partir de uma abordagem algébrica similar a (70). Desta forma, obtém-se

$$\begin{aligned}\mathcal{O}_{\mathrm{ARE}} = {} & \frac{\Gamma(n_{\mathrm{E}})^{-1}\Gamma(n_{\mathrm{R}})^{-1}}{\bar{\gamma}_{\mathrm{AE}}^{n_{\mathrm{E}}}\bar{\gamma}_{\mathrm{AR}}^{n_{\mathrm{R}}}} \left[\sum_{m=0}^{n_{\mathrm{E}}-1} \frac{(n_{\mathrm{E}}-1)!}{m!e^{\frac{2^{-2\mathcal{R}}-1}{\bar{\gamma}_{\mathrm{AE}}}}} \left(\frac{1}{\bar{\gamma}_{\mathrm{AE}}}\right)^{m-n_{\mathrm{E}}} \mathcal{J}(m,\bar{\gamma}_{\mathrm{AE}}) + \sum_{w=0}^{n_{\mathrm{E}}-1} \left(\frac{1}{w!}\right) \left(\frac{1}{\bar{\gamma}_{\mathrm{RE}}}\right)^w \right. \\ & \left. \sum_{k=0}^{w} \binom{w}{k} (-1)^k \left\{ \mathcal{T}(\bar{\gamma}_{\mathrm{RE}},0)\; \mathcal{J}(w-k,\bar{\gamma}_{\mathrm{RE}}) - \sum_{o=0}^{k+n_{\mathrm{E}}-1} \mathcal{T}(\bar{\gamma}_{\mathrm{AE}},o)\; \times \mathcal{J}(w-k+o,\bar{\gamma}_{\mathrm{AE}}) \right\} \right]. \end{aligned} \tag{75}$$

onde

$$\mathcal{T}(a,b)=\frac{b!\,(k+n_{\mathrm{E}}-1)!e^{-\frac{2^{-2\mathcal{R}}-1}{a}}}{\left[\frac{1}{\bar{\gamma}_{\mathrm{AE}}}-\frac{1}{\bar{\gamma}_{\mathrm{RE}}}\right]^{k+n_{\mathrm{E}}-b}} \tag{76}$$

e

$$\mathcal{J}(a,b)=\sum_{p=0}^{a}\binom{a}{p}\frac{\left(2^{-2\mathcal{R}}-1\right)^{a-p}(n_{\mathrm{R}}+p-1)!}{2^{2\mathcal{R}p}}\left(\frac{2^{-2\mathcal{R}}\bar{\gamma}_{\mathrm{AR}}+b}{\bar{\gamma}_{\mathrm{AR}}b}\right)^{-(n_{\mathrm{R}}+p)}. \tag{77}$$

Finalmente, $\mathcal{O}_{\mathrm{BE}}$ pode ser resolvida com o auxílio de F_{E} e f_{B}, de forma que

$$\mathcal{O}_{\mathrm{BE}}=\int_{0}^{\infty}F_{\mathrm{E}}\left[2^{-2\mathcal{R}}(1+\gamma_{\mathrm{B}})-1\right]f_{\mathrm{B}}(\gamma_{\mathrm{B}})\,\mathrm{d}\gamma_{\mathrm{B}}, \tag{78}$$

cuja expressão de forma fechada é obtida, utilizando (GRADSHTEYN; RYZHIK, 2007, §6.455.2) e algumas manipulações algébricas, por

$$\begin{aligned}\mathcal{O}_{\mathrm{BE}}=&\frac{n_{\mathrm{R}}n_{\mathrm{A}}\left(\bar{\gamma}_{\mathrm{AB}}\bar{\gamma}_{\mathrm{RB}}\right)^{-n_{\mathrm{B}}}}{\bar{\gamma}_{\mathrm{AE}}^{n_{\mathrm{E}}}\Gamma(n_{\mathrm{E}})\Gamma(n_{\mathrm{B}})^{2}}\sum_{k=0}^{n_{\mathrm{A}}-1}\sum_{m=0}^{n_{\mathrm{R}}-1}\binom{n_{\mathrm{A}}-1}{k}\binom{n_{\mathrm{R}}-1}{m}\prod_{\bar{\gamma}_{\mathrm{AB}}}\prod_{\bar{\gamma}_{\mathrm{AR}}}\sum_{l=0}^{n_{\mathrm{B}}-\beta_1-1}\frac{\binom{n_{\mathrm{B}}+\beta_1-1}{l}(-1)^{k+m+l}}{\left(\frac{m+1}{\bar{\gamma}_{\mathrm{RB}}}-\frac{k+1}{\bar{\gamma}_{\mathrm{AB}}}\right)^{(n_{\mathrm{B}}+\beta_2+l)}}\\
&\times\left[\frac{\Gamma(n_{\mathrm{E}})}{\bar{\gamma}_{\mathrm{AE}}^{-n_{\mathrm{E}}}}\mathcal{B}\left(0,\mu(0),\psi(0)\right)-\sum_{p=0}^{n_{\mathrm{E}}-1}\frac{\Gamma(n_{\mathrm{E}})\,e^{-\frac{2^{-2\mathcal{R}}-1}{\bar{\gamma}_{\mathrm{AE}}}}\bar{\gamma}_{\mathrm{AE}}^{n_{\mathrm{E}}-p}}{p!}\mathcal{B}\left(p,\mu(s),\psi\left(\frac{2^{-2\mathcal{R}}}{\bar{\gamma}_{\mathrm{AE}}}\right)\right)\right.\\
&-\sum_{w=0}^{n_{\mathrm{E}}-1}\left(\frac{1}{w!}\right)\left(\frac{1}{\bar{\gamma}_{\mathrm{RE}}}\right)^{w}\sum_{o=0}^{w}\binom{w}{o}(-1)^{o}\times\left\{\mathcal{C}(\bar{\gamma}_{\mathrm{RE}},0)\mathcal{B}\left(w-o,\mu(s),\psi\left(\frac{2^{-2\mathcal{R}}}{\bar{\gamma}_{\mathrm{RE}}}\right)\right)\right.\\
&\left.\left.+\mathcal{C}(\bar{\gamma}_{\mathrm{AE}},z)\mathcal{B}\left(w+z-o,\mu(s),\psi\left(\frac{2^{-2\mathcal{R}}}{\bar{\gamma}_{\mathrm{AE}}}\right)\right)\right\}\right],\end{aligned} \tag{79}$$

onde

$$\mathcal{B}(a,b,c)=\sum_{s=0}^{a}\binom{a}{s}\frac{\left(2^{-2\mathcal{R}}-1\right)^{a-s}}{2^{2\mathcal{R}s}}\frac{\alpha^{v}\Gamma(b+v)}{v\,(\alpha+c)}{}_2F_1\left(1;b+v;v+1;\frac{\alpha}{\alpha+c}\right), \tag{80}$$

com ${}_2F_1\left(\alpha,\beta;\gamma;z\right)$ sendo a função hipergeométrica de Gauss (GRADSHTEYN; RYZHIK, 2007, §9.111), e

$$\alpha=\frac{\bar{\gamma}_{\mathrm{AB}}(m-1)-\bar{\gamma}_{\mathrm{RB}}(k+1)}{\bar{\gamma}_{\mathrm{AB}}\bar{\gamma}_{\mathrm{RB}}}, \tag{81}$$

$$v=n_{\mathrm{B}}+\beta_2+l, \tag{82}$$

$$\mu(a)=a+n_{\mathrm{B}}+\beta_1-l, \tag{83}$$

$$\psi(a)=\frac{k+1}{\bar{\gamma}_{\mathrm{AB}}}+a, \tag{84}$$

$$\mathcal{C}(a,b)=\sum_{i=0}^{b}\frac{(o+n_{\mathrm{E}}-1)!e^{-\frac{2^{-2\mathcal{R}}-1}{a}}}{b!\left[\frac{\bar{\gamma}_{\mathrm{RE}}-\bar{\gamma}_{\mathrm{AE}}}{\bar{\gamma}_{\mathrm{AE}}\bar{\gamma}_{\mathrm{RE}}}\right]^{o+n_{\mathrm{E}}-b}}. \tag{85}$$

Portanto, a expressão em forma fechada para a SOP do CSI-DF é obtida após a substituição de (70), (75) e (79) em (58).

4.1.2 Artificial-Noise (AN)

Diversos trabalhos na literatura tem mostrado que múltiplas antenas permitem aumentar a segurança na camada física. Uma notável estratégia é utilizar ruído para confundir Eve, assim como em (COSTA et al., 2016), no qual Alice emprega TAS e Bob emprega MRC enquanto a comunicação para Eve é degradada por múltiplos sinais interferentes. Contudo, diferentemente de (COSTA et al., 2016), consideramos que os sinais interferentes são gerados por múltiplas antenas do *relay*, o qual cria um vetor *beamforming* de modo que o ruído é nulo na direção de Bob. Assim, o sinal de interferência empregado somente afeta Eve, sem interferir em Bob. Uma importante suposição com relação à criação do vetor *beamforming* é que o número de antenas no *relay* deve ser maior que o número de antenas em Bob (COSTA et al., 2016; ZHU et al., 2013); portanto, $n_{\mathrm{B}} \leq n_{\mathrm{R}} - 1$ é sempre considerado para o esquema AN. No decorrer deste documento será considerado que os custos relacionados à geração do vetor de *beamforming* são negligenciáveis em comparação com as potências alocadas em Alice e no *relay*, além dos custos relacionados à transmissão e recepção.

A capacidade do canal legítimo para o esquema AN é dada por

$$C_{\mathrm{L}}^{(\mathrm{AN})} = \frac{1}{2}\log_2\left(1+\gamma_{\mathrm{AB}}\right). \tag{86}$$

Já a capacidade com relação a Eve é limitada pelo sinal *jamming* gerado pelo nó *relay*. Então, nós representamos a relação sinal-para-interferência SIR (do inglês, *Signal-to-Interference Ratio*) em Eve seguindo a mesma notação de (COSTA et al., 2016), de modo que $\Upsilon_{\mathrm{I}} = \frac{\gamma_{\mathrm{AE}}}{\gamma_{\mathrm{I}}}$, onde $\gamma_{\mathrm{I}} = \sum_{k=0}^{n_{\mathrm{R}}} \bar{\gamma}_{\mathrm{RE},k}\left|h_{\mathrm{RE},k}\right|^2$ é a interferência gerada pelo *jamming*, escrito como a soma de todos os sinais interferentes enviados por cada k-ésima antena do *relay*. Como resultado, a capacidade do canal de Eve é definida por

$$C_{\mathrm{E}}^{(\mathrm{AN})} = \frac{1}{2}\log_2\left(1+\Upsilon_{\mathrm{I}}\right). \tag{87}$$

A partir das capacidades, a probabilidade de *outage* de segurança para o esquema AN pode ser definida por

$$p_{\mathrm{out}}^{(\mathrm{AN})} = \Pr\left\{\frac{1+\gamma_{\mathrm{AB}}}{1+\Upsilon_{\mathrm{I}}} < 2^{2\mathcal{R}}\right\} = \int_0^{\infty} F_{\mathrm{AB}}^{\mathrm{TAS/MRC}}\left[2^{2\mathcal{R}}\left(1+x\right)-1\right] f_{\frac{\gamma_{\mathrm{AE}}}{\gamma_{\mathrm{I}}}}\left(x\right)\mathrm{d}x, \tag{88}$$

onde

$$F_{\mathrm{AB}}^{\mathrm{TAS/MRC}}(z)=\left[1-e^{-\frac{\gamma_{\mathrm{AB}}}{\bar{\gamma}_{\mathrm{AB}}}}\sum_{w=0}^{n_{\mathrm{B}}-1}\left(\frac{1}{w!}\right)\left(\frac{\gamma_{\mathrm{AB}}}{\bar{\gamma}_{\mathrm{AB}}}\right)^{w}\right]^{n_{\mathrm{A}}} \tag{89}$$

é dado por (COSTA et al., 2016, eq. (13)) e,

$$f_{\frac{\gamma_{\mathrm{AE}}}{\gamma_{\mathrm{I}}}}(x)=\frac{\partial}{\partial x}\left[\int_{0}^{\infty}F_{\mathrm{AE}}^{\mathrm{MRC}}(xz)\,f_{\gamma_{\mathrm{I}}}(z)\,\mathrm{d}z\right], \tag{90}$$

com

$$F_{\mathrm{AE}}^{\mathrm{MRC}}(\gamma_{\mathrm{AE}})=1-e^{-\frac{\gamma_{\mathrm{AE}}}{\bar{\gamma}_{\mathrm{AE}}}}\sum_{w=0}^{n_{\mathrm{E}}-1}\left(\frac{1}{w!}\right)\left(\frac{\gamma_{\mathrm{AE}}}{\bar{\gamma}_{\mathrm{AE}}}\right)^{w} \tag{91}$$

e

$$f_{\gamma_{\mathrm{I}}}(z)=\sum_{i=1}^{n_{\mathrm{R}}}\frac{e^{-\frac{z}{\bar{\gamma}_{\mathrm{I}}}}}{\bar{\gamma}_{\mathrm{I}}}, \tag{92}$$

é dado conforme (COSTA et al., 2016, eq. (19)). Para simplificar a análise, cabe ressaltar que consideramos que a potência é igualmente distribuída entre os sinais *jamming*.

Então, a equação da SOP para o esquema AN (COSTA et al., 2016) é dada por

$$\begin{aligned}p_{\mathrm{out}}^{(\mathrm{AN})}=1-\sum_{k=1}^{n_{\mathrm{A}}}\binom{k}{n_{\mathrm{A}}}\prod_{\bar{\gamma}_{\mathrm{AB}}}\sum_{u=0}^{n_{\mathrm{E}}-1}\frac{(-1)^{k+1}}{u!}\frac{\Gamma(u+n_{\mathrm{R}})}{\Gamma(n_{\mathrm{R}})}\sum_{p=0}^{\beta_1}\binom{\beta_1}{p}\left(\frac{\bar{\gamma}_{\mathrm{AE}}}{\bar{\gamma}_{\mathrm{RE}}}\right)^{p}\left(2^{2\mathcal{R}}-1\right)^{\beta_1-p}\\ \times 2^{2\mathcal{R}p}e^{-\frac{k(z-1)}{\bar{\gamma}_{\mathrm{AB}}}}\left[n_{\mathrm{R}}\Gamma(p+u+1)\Psi\left(p+u+1,p-n_{\mathrm{R}}+1,\frac{k\bar{\gamma}_{\mathrm{AE}}2^{2\mathcal{R}}}{\bar{\gamma}_{\mathrm{RE}}\bar{\gamma}_{\mathrm{AB}}}\right)-\mathcal{L}\right],\end{aligned} \tag{93}$$

onde

$$\mathcal{L}=\begin{cases}u\Gamma(p+u)\Psi\left(p+u,p-n_{\mathrm{R}},\frac{k\bar{\gamma}_{\mathrm{AE}}2^{2\mathcal{R}}}{\bar{\gamma}_{\mathrm{RE}}\bar{\gamma}_{\mathrm{AB}}}\right) & \text{se } u\neq 0\\ 0, & \text{se } u=0\end{cases}$$

com $\Psi(.,.,.)$ representando a função hipergeométrica confluente de Tricomi (GRADSHTEYN; RYZHIK, 2007, §9.211.4). Cabe destacar que (93) é associada com n_{B} devido ao termo $\prod_{\bar{\gamma}_{\mathrm{AB}}}$ definido em (66).

4.2 EFICIÊNCIA ENERGÉTICA SEGURA E OTIMIZAÇÃO

De forma a capturar ambas métricas relacionadas a questões de confidencialidade e eficiência energética, definimos a métrica da SEE, similarmente a (41), por

$$\eta_{\mathrm{s}}=\frac{\mathcal{R}\left(1-p_{\mathrm{out}}^{(\mathrm{esq})}\right)}{P_{\mathrm{total}}^{(\mathrm{esq})}}. \tag{94}$$

O consumo total de potência, $P_{\text{total}}^{(\text{esq})}$, para o esquema CSI-DF é dado por

$$\begin{aligned} P_{\text{total}}^{(\text{CSI-DF})} &= 2\left[(1+\omega)P_{\text{A}} + P_{\text{TX}} + n_{\text{B}}\,P_{\text{RX}}\right] p_{\text{dir}} \\ &\quad + \left[(1+\omega)(P_{\text{A}}+P_{\text{R}}) + 2\,P_{\text{TX}} + (2\,n_{\text{B}}+n_{\text{R}})\,P_{\text{RX}}\right] p_{\text{coop}}, \end{aligned} \tag{95}$$

onde p_{coop} (p_{dir}), conforme demonstrado na Subseção 3.2.1, representa a probabilidade que a transmissão cooperativa (direta) ocorra, dada por $p_{\text{coop}} = 1 - p_{\text{dir}} = \frac{\bar{\gamma}_{\text{AR}}}{\bar{\gamma}_{\text{AR}}+\bar{\gamma}_{\text{AB}}}$.

Já com relação ao esquema AN temos

$$P_{\text{total}}^{(\text{AN})} = 2\left[(1+\omega)\,(P_{\text{A}}+P_{\text{R}}) + (n_{\text{R}}+1)\,P_{\text{TX}} + n_{\text{B}}\,P_{\text{RX}}\right]. \tag{96}$$

Desta maneira, o problema geral de otimização da SEE para cada esquema a partir da alocação de P_{A}, P_{R} e da taxa de confidencialidade, pode ser formalizado como

$$\begin{aligned} \underset{(P_{\text{A}},P_{\text{R}},\mathcal{R})}{\text{maximize}} \quad & \eta_{\text{s}}^{(\text{esq})} = \frac{\mathcal{R}\left(1-p_{\text{out}}^{(\text{esq})}\right)}{P_{\text{total}}^{(\text{esq})}} \quad \left[\frac{\text{bits seguros}}{\text{J}\times\text{Hz}}\right] \\ \text{sujeito a} \quad & 0 < P_i \leq P_{\max}, \text{ com } i \in \{\text{A},\text{R}\}, \\ & 0 \leq \mathcal{R} \leq \mathcal{R}_{\max}, \\ & p_{\text{out}}^{(\text{esq})} \leq \varphi, \end{aligned} \tag{97}$$

onde $P_{\max}$ é uma variável que representa a restrição com relação a máxima potência de transmissão, φ é o máximo valor aceitável da SOP para o sistema e $\mathcal{R}_{\max} = C_{\text{B}} - \mathcal{R}_{\text{E}}$ é a máxima taxa de confidencialidade, assumindo que C_{B} é conhecida e que a taxa de equívoco alvo é dada por $\mathcal{R}_{\text{E}}$. Cabe ressaltar que o conjunto de restrições apresentado em Eq. (97) é convexo e o efeito prático da terceira restrição, conforme demonstrado na Figura 19, é limitar quais são os valores máximos de probabilidade de *outage* de segurança permitidos. Desta forma, tais restrições apenas delimitam as métricas de confidencialidade, probabilidade de *outage* de segurança e *throughput* seguro, a um intervalo, de modo que tais funções permanecem côncavas.

A alocação da potência em Alice e no *relay* pode ser resolvida, similarmente à Seção 3.2.2.1, pelo algoritmo Dinkelbach. Devido a alocação de potência em ambos os nós, Alice e *relay*, a alocação de potência tem que ser separada em duas etapas: iniciando com alocação em Alice e posteriormente pela alocação no *relay*. Portanto, com relação a Alice, a Eq. (49) pode ser reescrita como

$$F_1(\lambda) = \underset{P_{\text{A}}\geq 0}{\text{maximize}}\; f_1(P_{\text{A}}) - \lambda f_2(P_{\text{A}}) = 0, \tag{98}$$

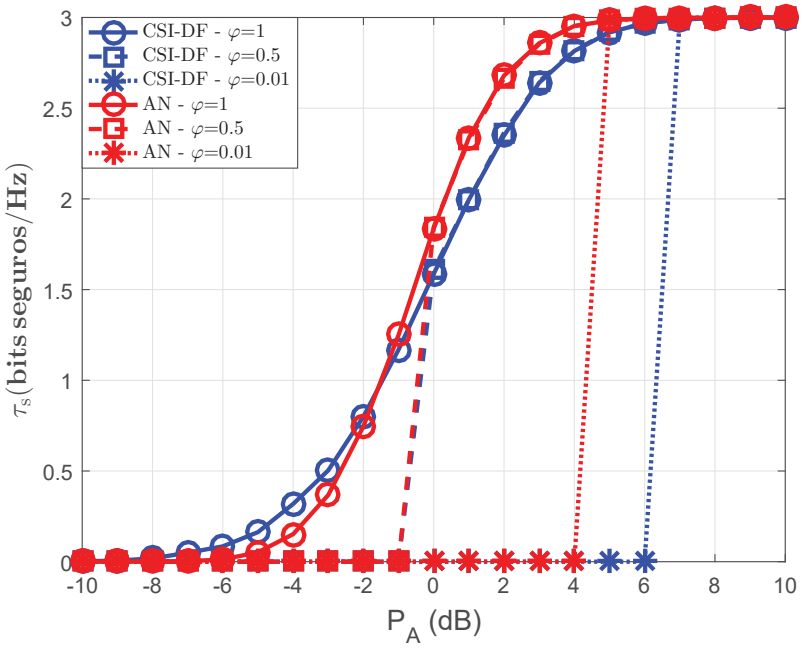


Figura 19 – *Throughput* **seguro para os esquemas CSI-DF e AN, em função de P_{A}, para diferentes restrições com relação ao máximo valor aceitável para SOP.**

onde $f_1(P_{\mathrm{A}}) = \mathcal{R}\left(1 - p_{\mathrm{out}}^{(\mathrm{esq})}\right)$ e $f_2(P_{\mathrm{A}}) = P_{\mathrm{total}}^{(\mathrm{esq})}$. Além do mais, a condição estacionária é dada por

$$\left.\frac{\partial f_1(P_{\mathrm{A}})}{\partial P_{\mathrm{A}}}\right|_{P_{\mathrm{A}}=P_{\mathrm{A}}^{\star}} - \lambda \left.\frac{\partial f_2(P_{\mathrm{A}})}{\partial P_{\mathrm{A}}}\right|_{P_{\mathrm{A}}=P_{\mathrm{A}}^{\star}} = 0, \tag{99}$$

onde $P_{\mathrm{A}}^{\star}$ é obtido pelo algoritmo Dinkelbach.

Na sequência, considerando a alocação de potência no *relay*, definimos

$$F_2(\lambda) = \underset{P_{\mathrm{R}} \geq 0}{\text{maximize}}\; f_1(P_{\mathrm{R}}) - \lambda f_2(P_{\mathrm{R}}) = 0, \tag{100}$$

onde $f_1(P_{\mathrm{R}}) = \mathcal{R}\left(1 - p_{\mathrm{out}}^{(\mathrm{esq})}\right)$, $f_2(P_{\mathrm{R}}) = P_{\mathrm{total}}^{(\mathrm{esq})}$ e cuja condição estacionária é

$$\left.\frac{\partial f_1(P_{\mathrm{R}})}{\partial P_{\mathrm{R}}}\right|_{P_{\mathrm{R}}=P_{\mathrm{R}}^{\star}} - \lambda \left.\frac{\partial f_2(P_{\mathrm{R}})}{\partial P_{\mathrm{R}}}\right|_{P_{\mathrm{R}}=P_{\mathrm{R}}^{\star}} = 0, \tag{101}$$

com $P_{\mathrm{R}}^{\star}$ também obtido a partir do algoritmo Dinkelbach. Como é possível observar, a complexidade do método é inerente à complexidade das expressões de SOP para cada esquema cooperativo, devido as derivadas especificadas em (99) e (101). Contudo, apesar da complexidade das expressões da SOP para números arbitrários de antenas para cada nó, as expressões podem ser simplificadas consideravelmente fixando n_{A}, n_{B}, n_{R} e n_{E}.

Finalmente, com relação à otimização de $\mathcal{R}$, empregamos um algoritmo de

golden section search com interpolação parabólica assim como na Subseção 3.2.2.2 deste documento. Tal algoritmo permite encontrar o valor máximo de uma função unimodal a partir do estreitamento do intervalo de valores dentro de um intervalo pré-definido (PRESS et al., 2007).

Cabe ressaltar que o algoritmo utilizado para alocação das potências e taxa é muito similar ao algoritmo proposto e detalhado no Algoritmo 1, porém com a diferença que a maximização da eficiência energética segura neste cenário de múltiplas antenas é obtida a partir da alocação de $\mathcal{R}$ ao invés de θ.

4.3 RESULTADOS NUMÉRICOS

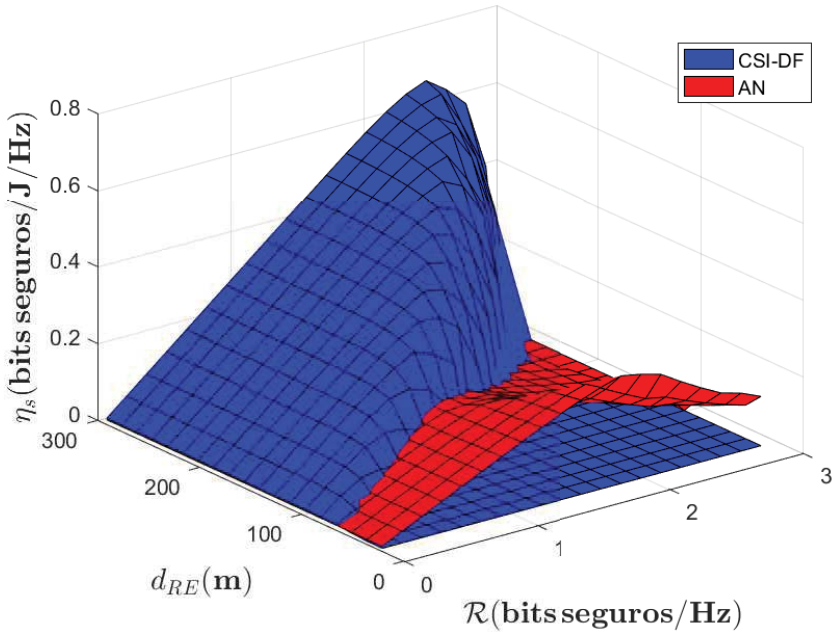
Consideramos $\mathcal{R} = 3$ bps/Hz, $d_{\mathrm{AB}} = 100$ m, $\upsilon = 3$ e $\varphi = 10^{-1}$. Adicionalmente, similarmente a Subseção 3.3, $P_{\mathrm{TX}} = 112{,}2$ mW, $P_{\mathrm{RX}} = 97{,}9$ mW, $B = 10$ kHz, $N_0 = -174$ dBm/Hz, $M_{\mathrm{l}} = 40$ dB, $G = 5$ dBi, $N_{\mathrm{f}} = 10$ dB e $f_{\mathrm{c}} = 2{,}5$ GHz.

Primeiramente, na Figura 20 demonstramos a SEE em função de $\mathcal{R}$ e d_{RE}. É possível observar que, quando Eve está próximo ao *relay*, AN apresenta um melhor desempenho visto que o *relay* interfere com maior intensidade em Eve, aumentando, desta forma, a SEE. Já o esquema CSI-DF permite importantes melhorias na SEE quando $\mathcal{R}$ aumenta, sendo também o esquema com o maior valor de SEE.

Na sequência, na Figura 21 comparamos a SEE para potência e taxas fixas, para taxa fixa e alocação de potência e para alocação de taxa e potência conforme definido em (97). Adicionalmente, comparamos as expressões da SEE com as simulações por Monte Carlo, de modo que uma ótima concordância é demonstrada. Como podemos observar, um significante ganho de desempenho é obtido quando a alocação de potência e taxa é realizada. Em particular, vale a pena destacar que a alocação de potência desempenha um papel importante na maximização da SEE.

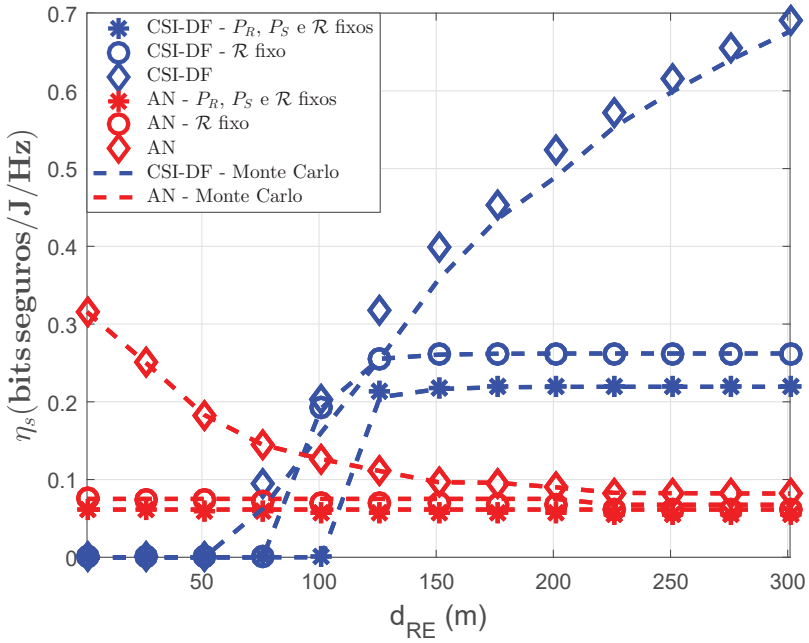
Já na Figura 22 plotamos a SEE, representada pelas linhas sólidas, e a SOP, representada pelas linhas tracejadas, em função de φ, o requisito mínimo para a SOP, o qual demonstra que um valor elevado de φ aumenta a SEE, apesar da penalidade relacionada ao número de bits transmitidos de maneira segura. Contudo, cabe destacar que mesmo com o aumento da SEE com φ, a SOP que maximiza a SEE não é próximo a um. Isto ocorre devido ao fato que uma SOP próxima a um implica em uma SEE que tende a zero em (94).

Figura 20 – SEE do CSI-DF e AN em função de $\mathcal{R}$ e d_{RE}, com $d_{\mathrm{AR}} = 0{,}5\,d_{\mathrm{AB}}$ e $n_{\mathrm{A}} = n_{\mathrm{R}} = n_{\mathrm{E}} = 2$ com $n_{\mathrm{B}} = 1$ para o esquema AN.



Fonte: Autoria própria.

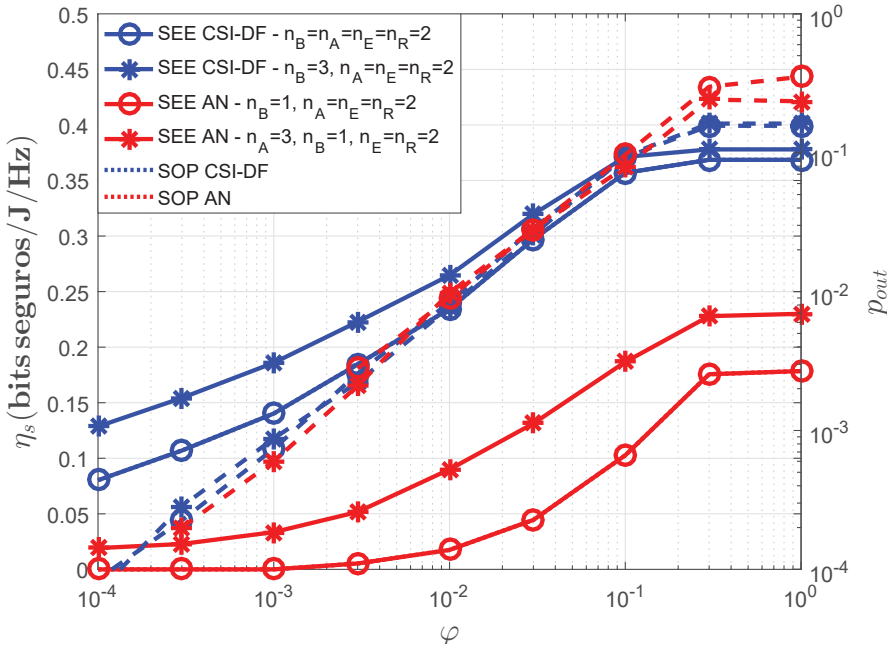
Figura 21 – SEE do CSI-DF e AN em função de d_{RE} para diferentes estratégias de alocação, com $d_{\mathrm{AR}} = 0{,}5\,d_{\mathrm{AB}}$ e $n_{\mathrm{A}} = n_{\mathrm{R}} = n_{\mathrm{E}} = 2$ com $n_{\mathrm{B}} = 1$.



Fonte: Autoria própria.

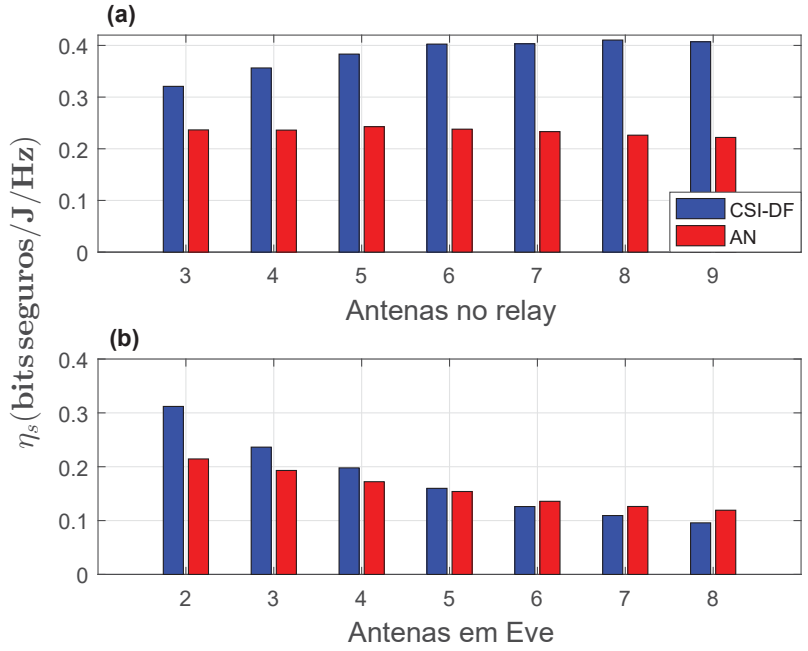
Por fim, na Figura 23 ilustramos a SEE em função do número de antenas, com

Figura 22 – SEE, representada pelas linhas sólidas, e SOP, representada pelas linhas tracejadas, do CSI-DF e AN em função de φ, com $d_{\mathrm{RE}} = 1,5\,d_{\mathrm{AB}}$, $d_{\mathrm{AR}} = 0,5\,d_{\mathrm{AB}}$.



Fonte: Autoria própria.

Figura 23 – SEE do CSI-DF e AN em função do número de antenas no *relay* e em Eve para $d_{\mathrm{AR}} = 0,5\,d_{\mathrm{AB}}$, $d_{\mathrm{RE}} = 1,25\,d_{\mathrm{AB}}$.



Fonte: Autoria própria.

$n_{\mathrm{A}} = n_{\mathrm{B}} = n_{\mathrm{E}} = 2$ enquanto variamos n_{R} na Figura 23a, e enquanto variamos n_{E} fixando

$n_{\mathrm{B}} = n_{\mathrm{A}} = 2$ e com $n_{\mathrm{R}} = 3$ na Figura 23b. Como observamos, o aumento de n_{R} é mais vantajoso para o CSI-DF de que para o AN, visto que o aumento de n_{R} implica em um ganho de diversidade no caso do CSI-DF quando a cooperação ocorre enquanto que o aumento de n_{R} para o esquema AN somente implica em um maior consumo de potência. Já na Figura 23b podemos observar que o AN torna-se mais vantajoso com o aumento de n_{E}. Isto é explicado pelo fato que quando o número de antenas em Eve é muito maior do que nos nós legítimos, é mais vantajoso para o *relay* interferir em Eve injetando ruído do que cooperar com Bob.

5 CONFIDENCIALIDADE COM BLOCOS DE TAMANHOS FINITOS

A perspectiva da IoT (do inglês, *Internet of Things*) é promover a conectividade sem fio entre os mais variados equipamentos, desde sensores até veículos (DURISI et al., 2016). Para que tal objetivo seja atendido, os próximos sistemas de comunicação sem fio, como sistemas de quinta geração (5G), deverão, dentre outros desafios, suportar os mais variados tipos de tráfegos de comunicação, dentre estes, os que utilizam pacotes de tamanho limitado (DURISI et al., 2016; POPOVSKI, 2014). Exemplos destes tipos de comunicação são representados, como mostrado em (DURISI et al., 2016), por sensores e outros dispositivos envolvendo comunicações *machine-to-machine* (M2M).

Desta forma, neste capítulo consideramos as métricas de segurança apropriadas para cenários com blocos de tamanho finito e limitado e realizamos uma análise comparativa entre cenários cooperativos e não-cooperativos considerando sistemas com limite de atraso.

5.1 MODELO DE SISTEMAS COM BLOCOS DE TAMANHOS FINITOS

A formulação usual da capacidade de canal representa a maior taxa em que é possível se ter uma comunicação confiável, ou seja, a probabilidade de erro tende a zero quando não existem restrições no tamanho do pacote. Porém, conforme (YANG et al., 2013), em cenários em que o desvanecimento do canal se torna constante pela duração de cada palavra código transmitida, a capacidade é zero para muitas distribuições de interesse prático, como Rayleigh. Isto ocorre porque a comunicação confiável não pode ser garantida para qualquer taxa de dados positiva. Em cenários como este, uma métrica de desempenho mais apropriada é a capacidade de *outage*, que representa a máxima taxa de dados possível para uma probabilidade de erro positiva quando também não existem limitações para o tamanho de pacote.

Tais medidas são razoáveis para os atuais sistemas de comunicações sem fio quando os tamanhos de pacote são grandes (DURISI et al., 2016). Porém, uma análise mais refinada deve ser determinada para a máxima taxa atingível quando os blocos apresentam tamanho finito e limitado. Para tais casos, a métrica da máxima taxa atingível depende do tamanho da palavra-código empregada, n, e da probabilidade de erro de

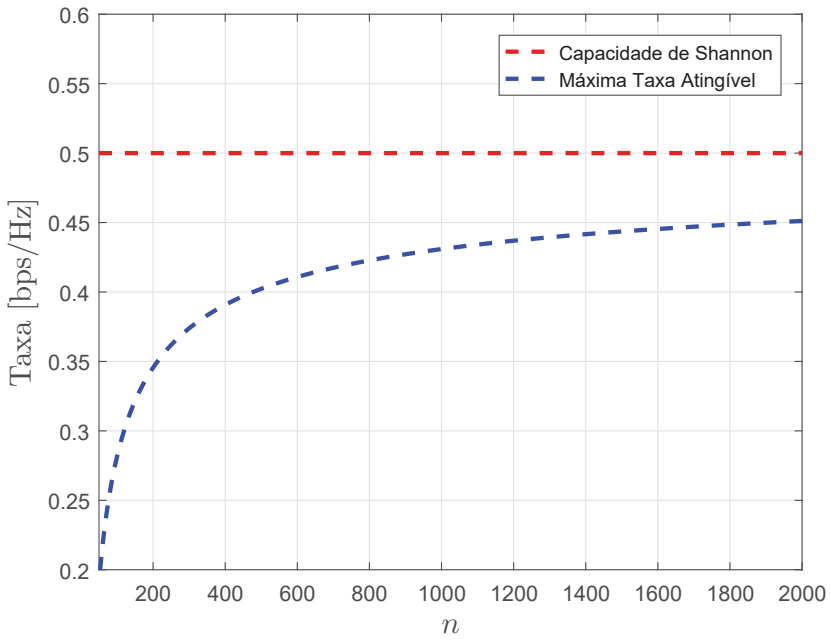
pacote, ϵ, a qual é dada por (DURISI et al., 2016; YANG et al., 2013)

$$R^{\star}(n,\epsilon) = C - \sqrt{\frac{V}{n}}Q^{-1}(\epsilon) + \mathcal{O}\left(\frac{\log(n)}{n}\right), \tag{102}$$

onde $\mathcal{O}\left(\frac{\log(n)}{n}\right)$ representa termos de ordem $\frac{\log(n)}{n}$, C é a capacidade ergódica do canal e $Q^{-1}(.)$ é o inverso da função Q. Ainda, $V = 1 - 2^{-2C}$ representa uma medida precisa da variação aleatória de um canal de capacidade C, denominada dispersão do canal (POLYANSKIY et al., 2010; DURISI et al., 2016).

Cabe ressaltar que tal formulação da máxima taxa atingível tende à capacidade de Shannon quando o tamanho de bloco, n, tende a infinito. Porém, para valores limitados e finitos de n, a máxima taxa atingível tem fundamental importância devido a considerável diferença, conforme Figura 24, verificada para as duas métricas.

Figura 24 – Comparação entre a capacidade de Shannon e a máxima taxa atingível, em termos de bps/Hz, a partir da variação do tamanho do bloco, n.



5.2 MÉTRICA DE SEGURANÇA PARA BLOCOS DE TAMANHO FINITO

Neste cenário com blocos de tamanho finito consideramos um código de escuta com $2^{n\mathcal{R}_{\mathrm{B}}}$ palavras-códigos, onde $\mathcal{R}_{\mathrm{B}} = \frac{k_{\mathrm{B}}}{n}$ é a taxa do canal legítimo, com k_{B} sendo o total de bits transmitidos por Alice em cada *frame* (BLOCH; BARROS, 2011). Com relação a Eve, definimos um número de palavras-códigos por binário igual a $2^{n\mathcal{R}_{\mathrm{E}}}$, onde

$\mathcal{R}_{\mathrm{E}}$ é a taxa de equivocação em Eve. Desta maneira, a taxa de comunicação segura é dada por $\mathcal{R} = \mathcal{R}_{\mathrm{B}} - \mathcal{R}_{\mathrm{E}}$. Cabe ressaltar que a definição de $\mathcal{R}_{\mathrm{E}} = \frac{k_{\mathrm{E}}}{n}$ implica que $k_{\mathrm{S}} = k_{\mathrm{B}} - k_{\mathrm{E}}$ bits de informação são transmitidos de maneira segura em cada *frame*.

Além do mais, com relação ao conhecimento do estado do canal, supomos uma abordagem mais realista, na qual a CSI com relação a Eve é desconhecida por se tratar de uma escuta passiva e a CSI do canal legítimo é desconhecida devido aos requisitos de latência e de tamanho dos blocos que acabam por tornar inviável tal aquisição. Desta forma, a confidencialidade perfeita não pode ser garantida e o evento de *outage* de confidencialidade é definido como a probabilidade que a capacidade instantânea do canal de Eve exceda a taxa $\mathcal{R}_{\mathrm{E}}$ (BLOCH et al., 2008). Além do mais, visto que a CSI instantânea com relação a Bob também não está disponível, devemos escolher um número total fixo de $2^{n\mathcal{R}_{\mathrm{B}}}$ palavras-códigos e um número fixo de palavras-códigos por binário igual a $2^{n\mathcal{R}_{\mathrm{E}}}$, de forma que o evento de *outage* de confiabilidade pode ocorrer também se $\mathcal{R}_{\mathrm{B}}$ exceder a capacidade do canal legítimo (BRANTE et al., 2015).

Portanto, dadas as estimativas de $\tilde{\mathcal{R}}_{\mathrm{B}}$ e $\tilde{\mathcal{R}}_{\mathrm{E}}$, as quais não são necessariamente os máximos já que nenhuma CSI está disponível, a probabilidade de erro de pacote para o esquema (esq) pode ser escrita como

$$\epsilon_j^{(\mathrm{esq})} \approx \mathbb{E}\left[Q\left(\frac{C_j - \tilde{\mathcal{R}}_j}{\sqrt{V_j/n}}\right)\right] = \int_0^{\infty} Q\left(\frac{C_j - \tilde{\mathcal{R}}_j}{\sqrt{V_j/n}}\right) f_{\gamma}(\gamma_j)\, \mathrm{d}\gamma_j, \tag{103}$$

onde $j \in \{\mathrm{B}, \mathrm{E}\}$, de modo que ϵ_{B} é a probabilidade de erro de pacote, enquanto ϵ_{E} representa a probabilidade de erro de vazamento de informação em Eve.

Para obtermos uma equação de forma fechada para (103), recorremos à linearização da função Q, como sugerido em (MAKKI et al., 2016), de forma que

$$Q(p(\gamma_j)) \approx \Omega(\gamma_j) = \begin{cases} 1, & \gamma_j \leq \zeta^2 \\ \frac{1}{2} - \frac{\beta}{\sqrt{2\pi}}(\mu z - \theta), & \zeta^2 < \gamma_j < \varrho^2 \\ 0, & \gamma_j \geq \varrho^2 \end{cases}, \tag{104}$$

onde

$$p(\gamma_j) = \frac{C(\gamma_j) - \tilde{\mathcal{R}}_j}{\sqrt{V(\gamma_j)/n}}, \tag{105}$$

$$\zeta^2 = \theta - \frac{1}{\beta}\sqrt{\frac{\pi}{2}}, \tag{106}$$

$$\varrho^2 = \theta + \frac{1}{\beta}\sqrt{\frac{\pi}{2}}, \tag{107}$$

$$\theta = 2^{\frac{k_j}{n}} - 1, \tag{108}$$

$$\beta = \sqrt{\frac{n}{2\pi}} \left(2^{\frac{2k_j}{n}} - 1\right)^{-\frac{1}{2}}. \tag{109}$$

Para este cenário, seguindo (ALVES et al., 2016), a métrica de *throughput* seguro é dada por

$$\tau_{\mathrm{s}}^{(\mathrm{esq})} = \mathcal{R}_{\mathrm{S}} \left(1 - \epsilon_{\mathrm{B}}^{(\mathrm{esq})}\right) \epsilon_{\mathrm{E}}^{(\mathrm{esq})}, \tag{110}$$

o qual leva em conta a confiabilidade, a partir do termo $(1-\epsilon_{\mathrm{B}})$, e a confidencialidade, pelo termo ϵ_{E}. Para maximização do desempenho do sistema, definimos o seguinte problema de otimização

$$\begin{aligned}
\underset{P_{\mathrm{A}},P_{\mathrm{R}},k_{\mathrm{B}},k_{\mathrm{E}},n}{\text{maximize}} \quad & \tau_{\mathrm{s}}^{(\mathrm{esq})} = \mathcal{R}_{\mathrm{S}} \left(1 - \epsilon_{\mathrm{B}}^{(\mathrm{esq})}\right) \epsilon_{\mathrm{E}}^{(\mathrm{esq})} \quad \left[\frac{\text{bits seguros}}{\text{Hz}}\right] \\
\text{sujeito a} \quad & 0 < P_i \leq P_{\max}, \quad \text{com} \quad i \in \{\mathrm{A}, \mathrm{R}\}, \\
& n_{\min} < n \leq n_{\max}, \\
& (1 - \epsilon_{\mathrm{B}}^{(\mathrm{esq})}) \geq \xi, \\
& (1 - \epsilon_{\mathrm{E}}^{(\mathrm{esq})}) \leq \sigma, \\
& \mathcal{R}_{\mathrm{S}} = \frac{k_{\mathrm{S}}}{n} > 0.
\end{aligned} \tag{111}$$

o qual permite maximizar τ_s dada uma probabilidade mínima de decodificação de pacote em Bob (ξ), uma probabilidade máxima de decodificação de pacote em Eve (σ), realizada através de alocação de P_{A} e P_{R}, dada uma restrição com relação a potência de transmissão máxima $P_{\max}$, e com tamanho de palavra código limitada no intervalo entre $n_{\min}$ e $n_{\max}$.[1]

5.3 PROTOCOLOS COOPERATIVOS COM BLOCOS DE TAMANHO FINITO

Nesta seção derivamos as equações das probabilidade de erro de pacote e *throughput* seguro para os esquemas direto e SDF considerando blocos de tamanho finito.

[1]Cabe ressaltar que P_{A} e P_{R} podem não ser sempre iguais a $P_{\max}$ visto que são beneficiais a Eve também. Além do mais, $n_{\min}$ é empregado aqui somente devido a fato que a aproximação proposta em (104) não é válida a menos que $n > 100$ (MAKKI et al., 2016).

5.3.1 Transmissão Direta

Na transmissão direta, a comunicação ocorre sem a presença do *relay* de forma que a capacidade do canal legítimo e de escuta são dadas, respectivamente, por

$$C_{\mathrm{L}}^{(\mathrm{Direto})} = \log_2(1+\gamma_{\mathrm{AB}}) \tag{112}$$

e

$$C_{\mathrm{E}}^{(\mathrm{Direto})} = \log_2(1+\gamma_{\mathrm{AE}}). \tag{113}$$

As probabilidades de erro de pacote então $\epsilon_j^{(\mathrm{Direto})}$, com $j \in \{\mathrm{B},\mathrm{E}\}$, podem ser escritas como

$$\begin{aligned}
\epsilon_j^{(\mathrm{Direto})} &\approx \int_0^{\infty} Q\left(\frac{C_j^{(\mathrm{Direto})} - \tilde{\mathcal{R}}_j}{\sqrt{V_j^{(\mathrm{Direto})}/n}}\right) f_\gamma\left(\gamma_{\mathrm{A}j}\right) \mathrm{d}\gamma_{\mathrm{A}j} \\
&= \int_0^{\zeta^2} f_\gamma\left(\gamma_{\mathrm{A}j}\right) \mathrm{d}\gamma_{\mathrm{A}j} + \int_{\zeta^2}^{\varrho^2} \frac{1}{2} f_\gamma\left(\gamma_{\mathrm{A}j}\right) \mathrm{d}\gamma_{\mathrm{A}j} - \int_{\zeta^2}^{\varrho^2} \frac{\beta}{\sqrt{2\,\pi}} \left(\gamma_{\mathrm{A}j} - \theta\right) f_\gamma\left(\gamma_{\mathrm{A}j}\right) \mathrm{d}\gamma_{\mathrm{A}j} \\
&= 1 + \frac{\psi(\bar{\gamma}_{\mathrm{A}j}, \varrho) - \phi(\bar{\gamma}_{\mathrm{A}j}, \zeta)}{2\sqrt{\pi}},
\end{aligned} \tag{114}$$

onde

$$\psi(x,y) = e^{-\frac{y^2}{x}} \left(\sqrt{2}\beta(x-\theta+y^2) - \sqrt{\pi}\right) \tag{115}$$

e

$$\phi(x,y) = e^{-\frac{y^2}{x}} \left(\sqrt{2}\beta(x-\theta+y^2) + \sqrt{\pi}\right). \tag{116}$$

Note ainda que (114) depende de $\tilde{\mathcal{R}}_j$ e, consequentemente, de k_j e n devido aos termos θ e β dados por (108)-(109).

5.3.2 Selective Decode-and-Forward (SDF)

No protocolo cooperativo SDF a comunicação ocorre em dois intervalos de tempo. O *relay* somente coopera com Alice se foi possível decodificar a mensagem transmitida no primeiro intervalo de tempo. Caso contrário, assumimos que Alice retransmite a informação no segundo intervalo de tempo. Por sua vez, Bob e Eve sempre aplicam MRC nas transmissões recebidas durante o primeiro e segundo intervalo de tempo, sendo estas as duas cópias enviadas por Alice ou a transmissão por Alice e a repetição pelo *relay*.

Portanto, a capacidade do canal legítimo pode ser definida por

$$C_{\mathrm{L}}^{(\mathrm{SDF})} = \epsilon_{\mathrm{AR}}^{(\mathrm{SDF})} \cdot \log_2(1+\gamma'_{\mathrm{AB}}) + (1-\epsilon_{\mathrm{AR}}^{(\mathrm{SDF})}) \cdot \log_2(1+\gamma_{\mathrm{B}}), \tag{117}$$

onde $\gamma_{\mathrm{B}} = \gamma_{\mathrm{AB}} + \gamma_{\mathrm{RB}}$, $\epsilon_{\mathrm{AR}}^{(\mathrm{SDF})}$ é a probabilidade de erro de pacote no *relay* e $\gamma'_{\mathrm{AB}} = \gamma_{\mathrm{AB},1} + \gamma_{\mathrm{AB},2}$ representa que Alice transmite a mesma informação nos dois *slots* de tempo. Desta maneira, $\log_2(1+\gamma'_{\mathrm{AB}})$ é a capacidade quando o *relay* não decodifica a mensagem transmitida por Alice, de forma que Alice retransmite a mensagem no segundo intervalo de tempo. Caso contrário, $\log_2(1+\gamma_{\mathrm{B}})$ é a capacidade quando o *relay* é capaz de colaborar com Alice e transmite a mensagem para Bob no segundo intervalo de tempo.

Similarmente, a capacidade do canal de Eve é

$$C_{\mathrm{E}}^{(\mathrm{SDF})} = \epsilon_{\mathrm{AR}}^{(\mathrm{SDF})} \cdot \log_2(1+\gamma'_{\mathrm{AE}}) + (1-\epsilon_{\mathrm{AR}}^{(\mathrm{SDF})}) \cdot \log_2(1+\gamma_{\mathrm{E}}), \tag{118}$$

onde $\gamma_{\mathrm{E}} = \gamma_{\mathrm{AE}} + \gamma_{\mathrm{RE}}$ e $\gamma'_{\mathrm{AE}} = \gamma_{\mathrm{AE},1} + \gamma_{\mathrm{AE},2}$.

As probabilidades de erro de pacote e erro de vazamento, $\epsilon_{\mathrm{B}}^{(\mathrm{SDF})}$ e $\epsilon_{\mathrm{E}}^{(\mathrm{SDF})}$, associadas ao protocolo SDF podem ser escritas como

$$\epsilon_{j}^{(\mathrm{SDF})} = \epsilon_{\mathrm{A}j}^{(\mathrm{SDF})}\, \epsilon_{\mathrm{AR}}^{(\mathrm{SDF})} + (1-\epsilon_{\mathrm{AR}}^{(\mathrm{SDF})})\, \epsilon_{\mathrm{AR}j}^{(\mathrm{SDF})}, \tag{119}$$

onde $\epsilon_{\mathrm{AR}j}^{(\mathrm{SDF})}$ é a probabilidade de erro de pacote após o MRC nas transmissões recebidas por Alice e o *relay*, em Bob ou Eve, ou seja, com $j \in \{\mathrm{B}, \mathrm{E}\}$.

Resolvendo $\epsilon_{\mathrm{A}j}^{(\mathrm{SDF})}$ e $\epsilon_{\mathrm{AR}}^{(\mathrm{SDF})}$ obtemos, respectivamente,

$$\begin{aligned}
\epsilon_{\mathrm{AR}}^{(\mathrm{SDF})} &\approx \int_0^{\infty} Q\left(\frac{{C_{\mathrm{AR}}}^{(\mathrm{SDF})} - \tilde{\mathcal{R}}_{\mathrm{B}}}{\sqrt{V_{\mathrm{AR}}^{(\mathrm{SDF})}/n}}\right) f_{\gamma}\left(\gamma_{\mathrm{AR}}\right) \mathrm{d}\gamma_{\mathrm{AR}} \\
&= \int_0^{\zeta^2} f_{\gamma}\left(\gamma_{\mathrm{AR}}\right) \mathrm{d}\gamma_{\mathrm{AR}} + \int_{\zeta^2}^{\varrho^2} \frac{1}{2} f_{\gamma}\left(\gamma_{\mathrm{AR}}\right) \mathrm{d}\gamma_{\mathrm{AR}} - \int_{\zeta^2}^{\varrho^2} \frac{\beta}{\sqrt{2\,\pi}} \left(\gamma_{\mathrm{AR}} - \theta\right) f_{\gamma}\left(\gamma_{\mathrm{AR}}\right) \mathrm{d}\gamma_{\mathrm{AR}} \\
&= 1 + \frac{\psi(\bar{\gamma}_{\mathrm{AR}}, \varrho) - \phi(\bar{\gamma}_{\mathrm{AR}}, \zeta)}{2\sqrt{\pi}}
\end{aligned} \tag{120}$$

e

$$\epsilon_{\mathrm{A}j}^{(\mathrm{SDF})} \approx \int_0^{\infty} Q\left(\frac{{C_{\mathrm{A}j}}^{(\mathrm{SDF})} - \tilde{\mathcal{R}}_{j}}{\sqrt{V_{\mathrm{A}j}^{(\mathrm{SDF})}/n}}\right) f_{\gamma}\left(\gamma_{\mathrm{A}j}\right) \mathrm{d}\gamma_{\mathrm{A}j} = 1 + \frac{\psi(2\,\bar{\gamma}_{\mathrm{A}j}, \varrho) - \phi(2\,\bar{\gamma}_{\mathrm{A}j}, \zeta)}{2\sqrt{\pi}}, \tag{121}$$

onde $C_{\mathrm{AR}}^{(\mathrm{SDF})} = \log_2(1+\gamma_{\mathrm{AR}})$ é a capacidade associada ao canal A-R.

Quando a transmissão cooperativa é empregada, a probabilidade de erro de

pacote, $\epsilon_{\mathrm{ARB}}^{(\mathrm{SDF})}$, e a probabilidade de erro de vazamento, $\epsilon_{\mathrm{ARE}}^{(\mathrm{SDF})}$, podem ser obtidas considerando as PDFs associadas com γ_{B} e γ_{E}, as quais levam em conta a PDF da soma de duas variáveis aleatórias exponencialmente distribuídas. Pelo teorema da convolução, a PDF de γ_j é (PAPOULIS, 1991)

$$g_{\gamma_j}(\gamma_j) = \frac{1}{\overline{\gamma}_{\mathrm{R}j} - \overline{\gamma}_{\mathrm{A}j}} \left(e^{-\frac{\gamma_j}{\overline{\gamma}_{\mathrm{R}j}}} - e^{-\frac{\gamma_j}{\overline{\gamma}_{\mathrm{A}j}}} \right), \tag{122}$$

onde $j \in \{\mathrm{B}, \mathrm{E}\}$.

Portanto, $\epsilon_{\mathrm{AR}j}^{(\mathrm{SDF})}$ é definida por

$$\begin{aligned} \epsilon_{\mathrm{AR}j}^{(\mathrm{SDF})} &\approx \int_0^{\infty} Q\left(\frac{C_j^{(\mathrm{SDF})} - \tilde{\mathcal{R}}_j}{\sqrt{V_j^{(\mathrm{SDF})}/n}} \right) g_{\gamma}\left(\gamma_j\right) \mathrm{d}\gamma_j \\ &= \frac{\nu(\bar{\gamma}_{\mathrm{A}j}, \bar{\gamma}_{\mathrm{R}j})}{\bar{\gamma}_{\mathrm{A}j} - \bar{\gamma}_{\mathrm{R}j}} - \frac{\bar{\gamma}_{\mathrm{A}j}\left[\psi(\bar{\gamma}_{\mathrm{A}j}, \varrho) - \psi(\bar{\gamma}_{\mathrm{A}j}, \zeta)\right]}{2\sqrt{\pi}(\bar{\gamma}_{\mathrm{R}j} - \bar{\gamma}_{\mathrm{A}j})} + \frac{\bar{\gamma}_{\mathrm{R}j}\left[\psi(\bar{\gamma}_{\mathrm{R}j}, \varrho) + \psi(\bar{\gamma}_{\mathrm{R}j}, \zeta)\right]}{2\sqrt{\pi}(\bar{\gamma}_{\mathrm{R}j} - \bar{\gamma}_{\mathrm{A}j})}, \end{aligned} \tag{123}$$

onde

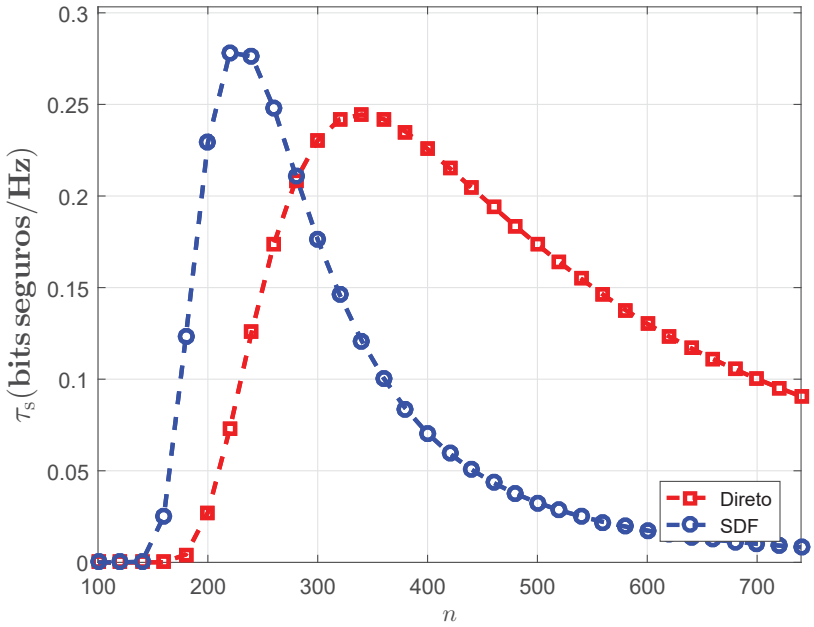
$$\nu(x, y) = x\left(1 - e^{-\frac{\zeta^2}{x}}\right) - y\left(1 - e^{-\frac{\zeta^2}{y}}\right). \tag{124}$$

5.4 OTIMIZAÇÃO DO TAMANHO DO BLOCO

Nesta seção definimos as expressões para o valor ótimo para o tamanho bloco, $n^{\star}$, que maximiza τ_s para cada esquema de transmissão. Para tal definição, encontramos primeiramente a derivada de τ_s com respeito a n e então igualamos tal expressão a zero. Contudo, devido a complexidade das equações, não é possível isolar n de modo a obter uma solução fechada para o tamanho de bloco ótimo. Desta forma, expressamos os resultados em termos de equações de ponto fixo, as quais podem ser resolvidas diretamente por métodos numéricos.

Cabe ressaltar que os valores ótimos para o tamanho bloco, $n^{\star}$, foram comparadas com as soluções ótimas, a partir da busca exaustiva, e resultados semelhantes foram obtidos. Adicionalmente, conforme a Figura 25, é possível observar observar que a curva do *throughput* seguro apresenta características de uma função quase-côncava, visto que existe um ponto de inflexão m, de modo que para qualquer ponto $t \leq m$ a função é não decrescente, enquanto para $t \geq m$ a função é não crescente.

Figura 25 – *Throughput* **seguro a partir da variação de n para os esquemas de transmissão direta e cooperativa.**



5.4.1 Transmissão Direta

O tamanho do bloco ótimo, $n^\star$ que maximiza o *throughput* seguro do esquema de transmissão direta pode ser obtido realizando

$$\frac{\partial \tau}{\partial n} = \frac{\partial \left\{ \mathcal{R}_{\mathrm{S}} \left(1 - \epsilon_{\mathrm{B}}^{(\mathrm{Direto})} \right) \epsilon_{\mathrm{E}}^{(\mathrm{Direto})} \right\}}{\partial n} = 0 \tag{125}$$

onde $\epsilon_{\mathrm{B}}^{(\mathrm{Direto})}$ e $\epsilon_{\mathrm{E}}^{(\mathrm{Direto})}$ são dados por (114). A partir da regra de Leibniz (GRADSHTEYN; RYZHIK, 2007, §0.42), podemos reescrever

$$\begin{aligned} \frac{\partial \tau}{\partial n} = {} & \frac{\partial \mathcal{R}_{\mathrm{S}}}{\partial n} \epsilon_{\mathrm{B}}^{(\mathrm{Direto})} \epsilon_{\mathrm{E}}^{(\mathrm{Direto})} - \mathcal{R}_{\mathrm{S}} \frac{\partial \epsilon_{\mathrm{B}}^{(\mathrm{Direto})}}{\partial n} \epsilon_{\mathrm{E}}^{(\mathrm{Direto})} \\ & + \mathcal{R}_{\mathrm{S}} \frac{\partial \epsilon_{\mathrm{E}}^{(\mathrm{Direto})}}{\partial n} + \frac{\partial \mathcal{R}_{\mathrm{S}}}{\partial n} \epsilon_{\mathrm{E}}^{(\mathrm{Direto})} - \mathcal{R}_{\mathrm{S}} \epsilon_{\mathrm{B}}^{(\mathrm{Direto})} \frac{\partial \epsilon_{\mathrm{E}}^{(\mathrm{Direto})}}{\partial n}, \end{aligned} \tag{126}$$

onde $\frac{\partial \mathcal{R}_{\mathrm{S}}}{\partial n} = \frac{k_{\mathrm{E}} - k_{\mathrm{B}}}{n^2}$ e a derivada de (114) com respeito a n é dada por

$$\frac{\partial \epsilon_j^{(\mathrm{Direto})}}{\partial n} = \frac{\psi'(\bar{\gamma}_{\mathrm{A}j}, \varrho) - \psi'(\bar{\gamma}_{\mathrm{A}j}, \zeta)}{2\sqrt{\pi}}, \tag{127}$$

onde $\psi'(x,y) = \frac{\partial \psi(x,y)}{\partial n}$ é definida por

$$\psi'(x,y) = \frac{e^{-\frac{y^2}{x}}}{\sqrt{2\pi} n^{\frac{3}{2}} \left(2^{\frac{k_j}{n}} - 1\right)^{\frac{3}{2}}} \left\{ 2^{\frac{k_j}{2n}} \left(n - k_j \log(2)\right) \right.$$
$$\left. -2^{\frac{3k_j}{2n}} n + \left(x + y^2 + 1\right) \left[2^{\frac{k_j}{n}} \left(k_j \log(2) + n\right) - n \right] \right\}. \tag{128}$$

5.4.2 Selective Decode-and-Forward (SDF)

Já para o esquema SDF, o tamanho do bloco ótimo, $n^\star$, é obtido a partir de

$$\frac{\partial \tau}{\partial n} = \frac{\partial \left\{ \mathcal{R}_{\mathrm{S}} \left(1 - \epsilon_{\mathrm{B}}^{(\mathrm{SDF})}\right) \epsilon_{\mathrm{E}}^{(\mathrm{SDF})} \right\}}{\partial n}$$
$$= \frac{\partial}{\partial n} \left\{ \mathcal{R}_{\mathrm{S}} \left(1 - \left[\epsilon_{\mathrm{AB}}^{(\mathrm{SDF})} \epsilon_{\mathrm{AR}}^{(\mathrm{SDF})} + (1 - \epsilon_{\mathrm{AR}}^{(\mathrm{SDF})}) \epsilon_{\mathrm{ARB}}^{(\mathrm{SDF})} \right] \right) \right.$$
$$\left. \times \left(\epsilon_{\mathrm{AE}}^{(\mathrm{SDF})} \epsilon_{\mathrm{AR}}^{(\mathrm{SDF})} + (1 - \epsilon_{\mathrm{AR}}^{(\mathrm{SDF})}) \epsilon_{\mathrm{ARE}}^{(\mathrm{SDF})} \right) \right\} = 0, \tag{129}$$

onde $\frac{\partial \epsilon_{\mathrm{AB}}^{(\mathrm{SDF})}}{\partial n}$, $\frac{\partial \epsilon_{\mathrm{AR}}^{(\mathrm{SDF})}}{\partial n}$ e $\frac{\partial \epsilon_{\mathrm{AE}}^{(\mathrm{SDF})}}{\partial n}$ são obtidos utilizando (127), enquanto $\epsilon_{\mathrm{ARB}}^{(\mathrm{SDF})}$ e $\epsilon_{\mathrm{ARE}}^{(\mathrm{SDF})}$, devido ao MRC em Bob e em Eve, são dados por

$$\frac{\partial \epsilon_{\mathrm{AR}j}^{(\mathrm{SDF})}}{\partial n} = \frac{\nu'(\bar{\gamma}_{\mathrm{R}j}, \bar{\gamma}_{\mathrm{A}j})}{\bar{\gamma}_{\mathrm{R}j} - \bar{\gamma}_{\mathrm{A}j}} - \frac{\bar{\gamma}_{\mathrm{R}j} \left[\psi'(\bar{\gamma}_{\mathrm{R}j}, \varrho) - \psi'(\bar{\gamma}_{\mathrm{R}j}, \zeta) \right]}{2\sqrt{\pi}(\bar{\gamma}_{\mathrm{A}j} - \bar{\gamma}_{\mathrm{R}j})} - \frac{\bar{\gamma}_{\mathrm{A}j} \left[\psi'(\bar{\gamma}_{\mathrm{A}j}, \varrho) + \psi'(\bar{\gamma}_{\mathrm{A}j}, \zeta) \right]}{2\sqrt{\pi}(\bar{\gamma}_{\mathrm{A}j} - \bar{\gamma}_{\mathrm{R}j})}, \tag{130}$$

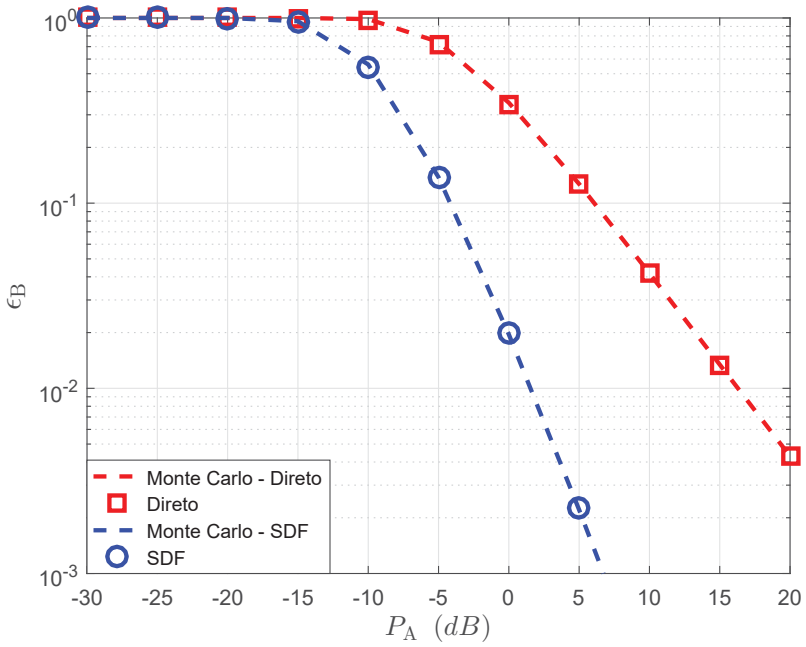
com $\nu'(x,y) = \frac{\partial \nu(x,y)}{\partial n}$, de modo que

$$\nu'(x,y) = -\frac{\left[2\pi\sqrt{2^{\frac{k_j}{n}} - 1} - \sqrt{4n} \left(2^{\frac{k_j}{2n}} - 1\right) \right]}{n^3 \sqrt{2^{\frac{k_j}{n}+3} - 8}} \left[2^{\frac{k_j}{n}} k_j \log(2) \sqrt{2n \left(2^{\frac{k_j}{n}} - 1\right)} - n\pi \left(2^{\frac{k_j}{n}} - 1\right) \right]$$
$$- \frac{e^{-\left[\sqrt{2}\pi\sqrt{2^{\frac{k_j}{n}} - 1} - 2\sqrt{n}\left(2^{\frac{k_j}{2n}} - 1\right) \right]^2 (x+y)(4nxy)^{-1}}}{n^3 \sqrt{2^{\frac{k_j}{n}+3} - 8}} \left(e^{x^{-1}} - e^{y^{-1}} \right) e^{\left[\frac{\pi\sqrt{2^{\frac{k_j}{n}} - 1}}{\sqrt{2n}} - 2^{\left(\frac{k_j}{2n}\right)} + 1 \right]^2}. \tag{131}$$

5.5 RESULTADOS NUMÉRICOS

Consideramos $\upsilon = 3$, $B = 10$ kHz, $N_0 = -174$ dBm/Hz, $M_{\mathrm{l}} = 30$ dB, $N_{\mathrm{f}} = 10$ dB, $G = 5$ dBi e $f_{\mathrm{c}} = 2{,}5$ GHz. Adicionalmente, assumimos que Alice, *relay* e Bob são dispostos

Figura 26 – Probabilidade de erro de pacote, ϵ_{B}, para os esquemas direto e CSI-DF considerando n=200, $k_{\mathrm{B}} = 1000$, $k_{\mathrm{E}} = 500$, d_{AR}=0,5 d_{AB} e d_{AE}=2 d_{AB} a partir da variação de P_{A}.



Fonte: Autoria própria.

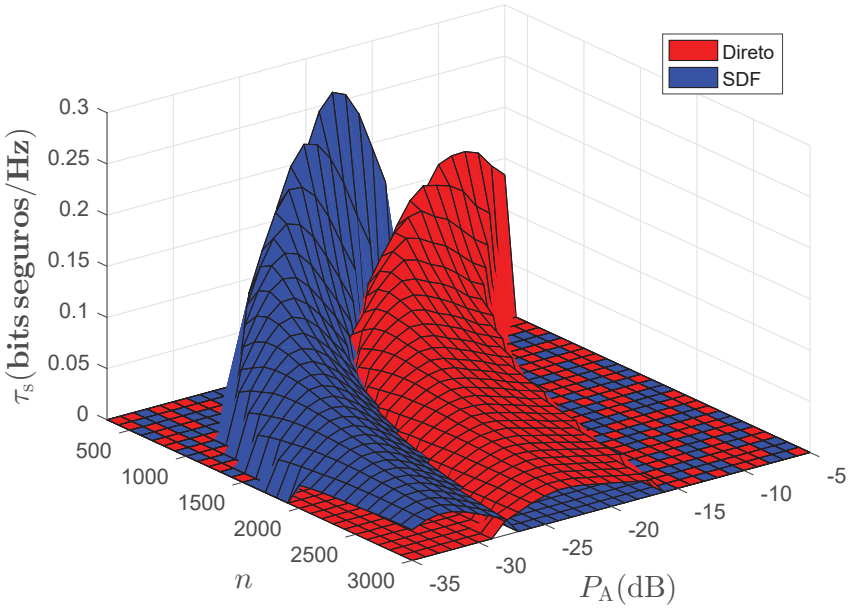
ao longo de uma linha, com $d_{\mathrm{AB}} = 100$ m e $d_{\mathrm{AR}} = 50$ m, enquanto Eve está 10 m distante de Bob, com $d_{\mathrm{AE}} = 110$ m e $d_{\mathrm{RE}} = 60$ m.

Primeiramente, na Figura 26 comparamos as expressões derivadas das probabilidades de erro de pacote, $\epsilon_{\mathrm{B}}^{(\mathrm{Direto})}$ e $\epsilon_{\mathrm{B}}^{(\mathrm{SDF})}$, dadas por (114) e (119), com as simulações por Monte Carlo. É possível observar uma ótima concordância com as expressões obtidas.

Já na Figura 27 demonstramos o comportamento do *throughput* seguro, τ_{s}, em função de P_{A} e n, para $k_{\mathrm{B}} = 1000$ bits, $k_{\mathrm{E}} = 500$ bits, $\xi = 0,1$, $\sigma = 0,9$ e $P_{\mathrm{R}} = -10$ dB. Como é possível observar, a potência e o tamanho do bloco são importantes parâmetros de otimização para maximizar τ_{s}. Adicionalmente, observamos que o esquema SDF emprega um valor menor de P_{A} em comparação com o direto para maximizar τ_{s}, enquanto n é relativamente pequeno para ambos esquemas.

Na sequência, na Figura 28 demonstramos a solução do problema de otimização formulado em (111) em função do número de bits seguros (k_{S}). Para resolver a otimização, consideramos que $n_{\min} = 100$ e $n_{\max} = 3000$ por intervalo de tempo, de forma que o SDF emprega dois intervalos de tempo utilizando $n^{\star}$, enquanto para o esquema de transmissão

Figura 27 – *Throughput* **seguro em função de n e P_{A} com $k_{\mathrm{B}} = 1000$, $k_{\mathrm{E}} = 500$, $\xi = 0,1$, $\sigma = 0,9$ e $P_{\mathrm{R}} = -10$ dB.**

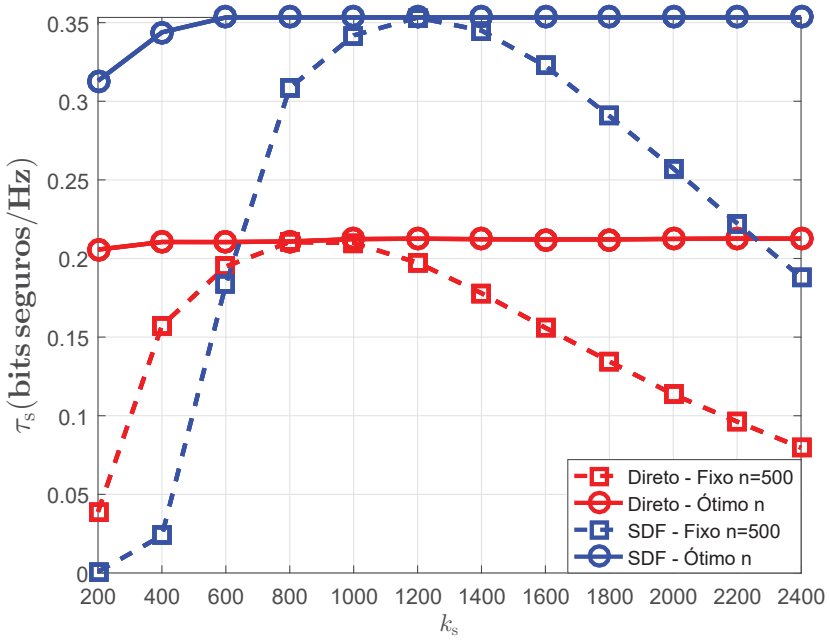


Fonte: Autoria própria.

direta nós permitimos que a otimização ocorra com $n_{\max} = 6000$ bits com o intuito de ser realizada uma comparação justa. É possível observar que o SDF supera a transmissão direta para todo intervalo de k_{S} neste cenário. Além do mais, o caso com tamanho de bloco fixo em $n = 500$ bits também é mostrado para comparação. Conforme simulações, a otimização de n é de fundamental importância para melhorar τ_{S}. Para cada k_{S}, a adaptação de n em (111) permite ao código *wiretap* modificar k_{B} e k_{E}, ainda mantendo fixo k_{S} para a aplicação.

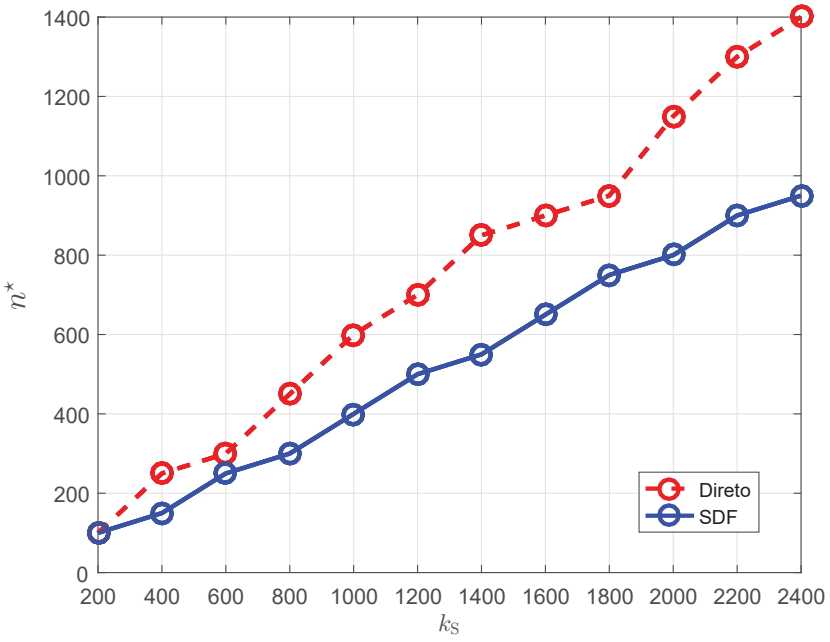
Complementando a análise, a Figura 29 ilustra $n^{\star}$ para os esquemas SDF e direto, no mesmo cenário da Figura 28. Como observamos, $n^{\star}$ aumenta com k_{S} para ambos esquemas, com a importante ressalva que o esquema SDF opera com um atraso correspondente a $2n^{\star}$, visto que dois intervalos de tempo são necessários.

Figura 28 – *Throughput seguro* em função de k_S comparando a otimização de (111) com o caso em que o tamanho do bloco é fixo em $n = 500$ bits.



Fonte: Autoria própria.

Figura 29 – Ótimo tamanho de bloco, $n^\star$, em função de k_S para os esquemas de transmissão direto e SDF.



Fonte: Autoria própria.

6 CONCLUSÕES E COMENTÁRIOS FINAIS

Em um contexto no qual a segurança se torna um item fundamental a ser considerado no desenvolvimento de novos sistemas, este trabalho propõe realizar uma investigação sobre diferentes aspectos da confidencialidade em sistemas cooperativos com a presença de dois usuários legítimos, Alice e Bob, comunicando-se com auxílio de um nó *relay*, na presença de um espião passivo, Eve.

Com relação à probabilidade generalizada de *outage* de segurança, que engloba diferentes requisitos de segurança implementados através de um parâmetro de equivocação fracionária, $\theta \in (0, 1]$, considerando que Alice tem CSI perfeita do canal legítimo, dois esquemas cooperativos são propostos de forma a explorar completamente a CSI disponível pela escolha entre o caminho mais vantajoso, direto ou cooperativo. Os protocolos propostos são denominados CSI-RC, que é realizado empregando a mesma palavra-código que Alice na retransmissão, e CSI-PC, que emprega codificação paralela, ou seja, diferentes palavras-códigos são utilizadas na retransmissão. Os esquemas propostos são comparados com o DF tradicional, o AF e o CJ. Além do mais, buscando um cenário de baixa complexidade para alocação de potência e θ para maximização da eficiência energética segura, o algoritmo Dinkelbach é combinado com o algoritmo *golden section search* para alocação conjunta das potências em Alice, no *relay* e também do parâmetro θ. Nossos resultados demonstram que o esquema CSI-RC supera os outros esquemas cooperativos para a maior parte dos cenários, exceto se o *relay* está posicionado muito próximo à Alice ou Bob, quando o esquema CSI-PC se torna mais vantajoso se $\theta \to 1$. Adicionalmente, o esquema CJ tem um melhor desempenho se Eve está próxima ao *relay* e se o *relay* está próximo à Alice, independentemente do valor do parâmetro θ.

Com relação aos cenários cooperativos MIMO, investigamos a eficiência energética segura para diferentes configurações com relação ao número de antenas e à máxima probabilidade de *outage* de segurança aceitável, também considerando alocações de potência e taxa de confidencialidade. Neste casos, comparamos os esquemas CSI-DF, o qual explora a CSI disponível para escolha entre transmissões diretas ou cooperativas, com o esquema AN, o qual o *relay* utiliza um vetor *beamforming* para interferir somente em Eve. Os resultados mostram que o CSI-DF supera o esquema AN na maior parte dos cenários, exceto se Eve está próximo ao *relay* ou com o aumento das antenas Eve, quando o AN se torna mais vantajoso.

Por fim, com relação aos cenários de blocos de tamanhos finitos, comparamos o

throughput seguro da cooperação via SDF com o protocolo de transmissão direto em um cenário com limite de atraso. O impacto, em termos da probabilidade de erro, é levado em conta, assim como os efeitos do máximo tamanho de bloco limitado por um máximo atraso permitido. Assumindo que o transmissor legítimo não tem conhecimento da CSI instantânea de nenhum dos canais, legítimo e da escuta, investigamos o *throughput* seguro considerando os efeitos conjuntos da probabilidade de erro de pacote no receptor legítimo e do vazamento de informação à Eve. Nossos resultados mostram que a otimização do tamanho do bloco, sujeito a um limite superior, é de suma importância para maximização do *throughput* seguro, visto que a adaptação do tamanho do bloco, n, permite ao código de escuta modificar k_{B} e k_{E}, ainda mantendo k_{S}, o número de bits de informação seguros, fixo na aplicação. Adicionalmente, é mostrado que a comunicação cooperativa permite superar consideravelmente as transmissões não cooperativas, permitindo grandes vantagens em termos do *throughput* seguro.

6.1 TRABALHOS FUTUROS

Como trabalhos futuros, contempla-se a utilização da métrica da probabilidade generalizada de *outage* de segurança para outros cenários de CSI. Em (TANG et al., 2009; BRANTE et al., 2015; LIU et al., 2015) são analisadas métricas de segurança considerando que Alice não tem conhecimento da CSI de nenhum dos canais. Desta forma, uma possível extensão é considerar a métrica da probabilidade generalizada de *outage* de segurança para este cenário de CSI, o qual é bastante prático em redes de sensores sem fio com um número de nós elevado, no qual torna-se difícil ao transmissor ter qualquer tipo de CSI. Além do mais, outra interessante extensão dos trabalhos atuais é considerar um cenário de CSI desatualizada ou imprecisa, assim como em (LIN et al., 2016), nos quais os esquemas que exploram completamente a CSI disponível para maximização das métricas do sistema podem se tornam menos robustos. Em (BURICH et al., 2017) o impacto, em termos de eficiência energética e *throughput* seguro, de sistemas considerando mecanismos HARQ (do inglês, *Hybrid Automatic Retransmission Request*) são analisados considerando tanto a camada física quanto a de enlace. Em (SU et al., 2011; WU et al., 2014) os autores consideram uma alocação ótima de potência para HARQ a fim de minimizar a potência de transmissão em cenários de desvanecimento quasi-estáticos visando a maximização da eficiência energética do sistema. Desta maneira, outra possível extensão deste trabalho está relacionada à utilização da métrica generalizada da *outage* de segurança em cenários HARQ. Adicionalmente, em (MUCCHI et al., 2017) uma nova métrica de

confidencialidade, denominada pressão de confidencialidade, é apresentada. Tal métrica determina o nível de segurança em uma superfície independentemente do posicionamento de Eve. Uma possível extensão é analisar diferentes cenários de comunicação segura a partir de tal métrica.

Com relação aos cenários MIMO, em (WANG et al., 2015c) realiza-se uma comparação inicial entre a técnica do *beamforming* e do *artificial fast-fading*, caracterizando a taxa de confidencialidade para estes sistemas, considerando múltiplas antenas no transmissor. Desta maneira, uma proposta de continuação do trabalho está relacionada à utilização das múltiplas antenas no sistema para emular um canal *fast-fading* para Eve de modo que a informação não possa ser decodificada. Outra futura extensão deste trabalho está relacionada ao uso conjunto de outros métodos de cooperação, por exemplo, a partir da utilização de múltiplos *relays*.

Com relação à cooperação considerando blocos de tamanhos finitos, em (HU et al., 2016c, 2016a, 2016b) os autores analisam diferentes cenários cooperativos com o *relay* realizando o DF convencional para auxiliar a comunicação entre os nós legítimos. Em (HU et al., 2016c) os autores estudam o desempenho de um sistema com múltiplos *relays* realizando cooperação via DF em um cenário *dual-hop*. Já em (HU et al., 2016a) os autores investigam a performance da cooperação em um cenário *single-hop* com a presença de um nó *relay* a partir das probabilidades de erro da retransmissão pelo *relay*. Enquanto em (HU et al., 2016b) investiga-se o cenário em que apenas a CSI média dos canais está disponível à Alice. Desta forma, possíveis extensões para o estudo de blocos de tamanho finito estão relacionadas a comparações com outros protocolos cooperativos como, por exemplo, o AF e o CJ, além de analisar as métricas de segurança para outros cenários de CSI.

Já com relação às métricas de eficiência energética, possíveis propostas de continuidade estão relacionadas à análise dos resultados considerando, por exemplo, outros algoritmos ótimos e sub-ótimos para alocação de potência, taxa e demais parâmetros do sistema.

Além das propostas de continuidade citadas, outras extensões na área de segurança estão relacionadas aos próximos sistemas de comunicação sem fio, como, por exemplo, sistemas 5G. Em tais sistemas, novas tecnologias de acesso ao meio sem fio, como mmWave (do inglês, *Millimeter Wave*) podem ser utilizadas. Em (JU et al., 2017), a segurança em tais sistemas considerando MISOSE (do inglês, *Multiple-Input Single-Output Single-Antenna Eavesdropper*) são estudadas. Já em (ZHU et al., 2017), os autores

investigam a confidencialidade em redes *ad hoc* de larga escala. Desta forma, futuros trabalhos utilizando comunicações com mmWave podem considerar diferentes aspectos da confidencialidade, por exemplo, a partir da comunicação com MIMO massivo.

Ainda considerando sistemas 5G, futuras extensões de trabalho podem considerar cenários NOMA (do inglês, *Non-Orthogonal Multiple Access*). Tal técnica utiliza o domínio da potência para múltiplos acessos na rede. Em (CHEN et al., 2018) o desempenho de segurança para sistemas NOMA cooperativos são estudados considerando os protocolos AF e DF. Já em (QIN et al., 2016), a confidencialidade com o protocolo NOMA é estudada em redes de larga escala. Em (HE et al., 2017), os autores estudam o design ótimo para esquemas NOMA seguros. Para o cenário estudado, os atributos ótimos de taxas de transmissão e alocação de potência são investigados para cada usuário. Desta forma, possíveis extensões considerando segurança na camada física em conjunto com sistemas NOMA podem estar relacionadas a utilização de redes heterogêneas, múltiplas antenas e outros esquemas cooperativos.

Outra abordagem para futuros trabalhos pode considerar a combinação de técnicas de segurança entre camadas, por exemplo, combinando a exploração das características da camada física com as abordagens de criptografia das camadas superiores para aumentar o sigilo da informação (ZOU et al., 2016; SUN; DU, 2017). Por fim, os autores em (LI et al., 2017; TANG et al., 2017) consideram um cenário em que Eve é uma escuta ativa capaz de interceptar a transmissão entre os nós legítimos enquanto envia sinais de *jamming*. Desta forma, possíveis extensões podem considerar tal cenário *full-duplex*, por exemplo, para múltiplos *relays*, múltiplos Eves e demais cenários de confidencialidade.

APÊNDICE A – PROVA DO TEOREMA 1

Para cálculo da probabilidade generalizada de *outage* de segurança do CSI-RC, consideramos o máximo entre $\log_2(1+\gamma'_{\mathrm{AB}})$ e $\min\{\log_2(1+\gamma_{\mathrm{AR}}), \log_2(1+\gamma_{\mathrm{B}})\}$, ou seja, as capacidades considerando transmissões direta e cooperativa, respectivamente. Contudo, devido ao fato da solução analítica ser complexa de ser obtida de forma fechada, consideramos uma aproximação assumindo que o *relay* está em uma posição intermediária entre Alice e Bob. Consideramos que Alice escolhe entre a transmissão direta sempre que $\gamma_{\mathrm{AB}} \geq \gamma_{\mathrm{AR}}$. Pelo contrário, a cooperação ocorre se $\gamma_{\mathrm{AR}} > \gamma_{\mathrm{AB}}$. Portanto, três sub-casos devem ser considerados:

- $\mathcal{E}_1 = \{\gamma_{\mathrm{AB}} \geq \gamma_{\mathrm{AR}}\}$, indicando a escolha por Alice pela transmissão direta;
- $\mathcal{E}_2 = \{\gamma_{\mathrm{AB}} < \gamma_{\mathrm{AR}} \bigcap \gamma_{\mathrm{AR}} < \gamma_{\mathrm{B}}\}$, indicando a escolha pela transmissão cooperativa com a capacidade limitada pelo canal A-R;
- $\mathcal{E}_3 = \{\gamma_{\mathrm{AB}} < \gamma_{\mathrm{AR}} \bigcap \gamma_{\mathrm{AR}} \geq \gamma_{\mathrm{B}}\}$, indicando cooperação com a capacidade limitada pelo MRC em Bob.

$$\text{Portanto,} \quad p_{\mathrm{gso}}^{(\mathrm{esq})} = \underbrace{\Pr\{C_{\mathrm{L}} \leq C_{\mathrm{E}}\}}_{A_1} + \underbrace{\Pr\left\{C_{\mathrm{L}} - C_{\mathrm{E}} < 2\theta\mathcal{R} \bigcap C_{\mathrm{L}} - 2\mathcal{R} < C_{\mathrm{E}} < C_{\mathrm{L}}\right\}}_{A_2}$$

pode ser expresso pela soma de dois termos A_1 e A_2. Note que é considerado $2\mathcal{R}$ devido à perda de multiplexação pela transmissão cooperativa. Além do mais, o sobrescrito (CSI-RC) não é mostrado para simplificar a notação. A solução de A_1 é dada por

$$\begin{aligned}
A_1 &= \Pr\left\{C_{\mathrm{L}} \leq C_{\mathrm{E}} \bigcap \mathcal{E}_1\right\} + \Pr\left\{C_{\mathrm{L}} \leq C_{\mathrm{E}} \bigcap \mathcal{E}_2\right\} + \Pr\left\{C_{\mathrm{L}} \leq C_{\mathrm{E}} \bigcap \mathcal{E}_3\right\} \\
&= \int_0^{\infty}\int_0^{\gamma_{\mathrm{AB}}}\int_{\gamma_{\mathrm{AB}}}^{\infty} f_{\gamma_{\mathrm{AB}}} f_{\gamma_{\mathrm{AR}}} f_{\gamma_{\mathrm{AE}}} \,\mathrm{d}\gamma_{\mathrm{AE}}\,\mathrm{d}\gamma_{\mathrm{AR}}\,\mathrm{d}\gamma_{\mathrm{AB}} \\
&+ \int_0^{\infty}\int_0^{\gamma_{\mathrm{AR}}}\int_{\gamma_{\mathrm{AR}}}^{\infty}\int_{\gamma_{\mathrm{AR}}}^{\infty} f_{\gamma_{\mathrm{E}}} f_{\gamma_{\mathrm{B}}} f_{\gamma_{\mathrm{AR}}} f_{\gamma_{\mathrm{AB}}} \,\mathrm{d}\gamma_{\mathrm{E}}\,\mathrm{d}\gamma_{\mathrm{B}}\,\mathrm{d}\gamma_{\mathrm{AB}}\,\mathrm{d}\gamma_{\mathrm{AR}} \\
&+ \int_0^{\infty}\int_{\gamma_{\mathrm{AB}}}^{\infty}\int_0^{\gamma_{\mathrm{AR}}}\int_{\gamma_{\mathrm{B}}}^{\infty} f_{\gamma_{\mathrm{E}}} f_{\gamma_{\mathrm{B}}} f_{\gamma_{\mathrm{AR}}} f_{\gamma_{\mathrm{AB}}} \,\mathrm{d}\gamma_{\mathrm{E}}\,\mathrm{d}\gamma_{\mathrm{B}}\,\mathrm{d}\gamma_{\mathrm{AR}}\,\mathrm{d}\gamma_{\mathrm{AB}},
\end{aligned} \tag{132}$$

onde, já que assumimos canais com desvanecimento Rayleigh, γ_{ij} são variáveis aleatórias exponencialmente distribuídas, cujas funções densidade de probabilidade são dadas por (4). Já a PDF das SNRs equivalentes de Bob e Eve ($\gamma_j = \gamma_{\mathrm{A}j} + \gamma_{\mathrm{R}j}$, com $j \in \{\mathrm{B},\mathrm{E}\}$), segundo (PAPOULIS, 1991) são dadas por

$$f_{\gamma_j} = \frac{1}{\bar{\gamma}_{\mathrm{R}j} - \bar{\gamma}_{\mathrm{A}j}} \left(e^{-\gamma_{\mathrm{R}j}/\bar{\gamma}_{\mathrm{R}j}} - e^{-\gamma_{\mathrm{A}j}/\bar{\gamma}_{\mathrm{A}j}} \right). \tag{133}$$

Com relação ao caso γ'_{AB} e γ'_{AE}, tendo em vista que as mesmas estatísticas do canal são assumidas para ambas transmissões de Alice, podemos definir $\bar{\gamma}'_{\mathrm{AB}} = 2\bar{\gamma}_{\mathrm{AB}}$ e $\bar{\gamma}'_{\mathrm{AE}} = 2\bar{\gamma}_{\mathrm{AE}}$.

Já A_2 pode ser escrito como $A_{2\mathrm{a}} - A_{2\mathrm{b}}$, com $A_{2\mathrm{a}} = \Pr\{C_\mathrm{L} - C_\mathrm{E} < 2\theta\mathcal{R} \bigcap C_\mathrm{L} - 2\mathcal{R} < C_\mathrm{E}\}$ e $A_{2\mathrm{b}} = \Pr\{C_\mathrm{L} - C_\mathrm{E} < 2\theta\mathcal{R} \bigcap C_\mathrm{E} \geq C_\mathrm{L}\}$, de modo que

$$\begin{aligned}
A_{2\mathrm{a}} &= \Pr\left\{C_\mathrm{L} - C_\mathrm{E} < 2\theta\mathcal{R} \bigcap C_\mathrm{L} - 2\mathcal{R} < C_\mathrm{E} \bigcap \mathcal{E}_1\right\} \\
&\quad + \Pr\left\{C_\mathrm{L} - C_\mathrm{E} < 2\theta\mathcal{R} \bigcap C_\mathrm{L} - 2\mathcal{R} < C_\mathrm{E} \bigcap \mathcal{E}_2\right\} \\
&\quad + \Pr\left\{C_\mathrm{L} - C_\mathrm{E} < 2\theta\mathcal{R} \bigcap C_\mathrm{L} - 2\mathcal{R} < C_\mathrm{E} \bigcap \mathcal{E}_3\right\} \\
&= \int_0^\infty \int_{\gamma_{\mathrm{AR}}}^\infty \int_{\rho}^\infty f_{\gamma_{\mathrm{AE}}} f_{\gamma_{\mathrm{AB}}} f_{\gamma_{\mathrm{AR}}} \,\mathrm{d}\gamma_{\mathrm{AE}}\,\mathrm{d}\gamma_{\mathrm{AB}}\,\mathrm{d}\gamma_{\mathrm{AR}} \\
&\quad + \int_0^\infty \int_{\gamma_{\mathrm{AB}}}^\infty \int_{\gamma_{\mathrm{AR}}}^\infty \int_{\psi(\gamma_{\mathrm{AR}})}^\infty f_{\gamma_\mathrm{E}} f_{\gamma_\mathrm{B}} f_{\gamma_{\mathrm{AB}}} f_{\gamma_{\mathrm{AR}}} \,\mathrm{d}\gamma_\mathrm{E}\,\mathrm{d}\gamma_\mathrm{B}\,\mathrm{d}\gamma_{\mathrm{AR}}\,\mathrm{d}\gamma_{\mathrm{AB}} \\
&\quad + \int_0^\infty \int_{\gamma_{\mathrm{AB}}}^\infty \int_0^{\gamma_{\mathrm{AR}}} \int_{\psi(\gamma_\mathrm{B})}^\infty f_{\gamma_\mathrm{E}} f_{\gamma_\mathrm{B}} f_{\gamma_{\mathrm{AB}}} f_{\gamma_{\mathrm{AR}}} \,\mathrm{d}\gamma_\mathrm{E}\,\mathrm{d}\gamma_\mathrm{B}\,\mathrm{d}\gamma_{\mathrm{AR}}\,\mathrm{d}\gamma_{\mathrm{AB}},
\end{aligned} \tag{134}$$

onde $\rho = \frac{2^{-2\theta\mathcal{R}}(1+\gamma'_{\mathrm{AB}})-1}{2}$, $\psi(x) = 2^{-2\theta\mathcal{R}}(1+x) - 1$ e

$$\begin{aligned}
A_{2\mathrm{b}} &= \Pr\left\{C_\mathrm{L} - C_\mathrm{E} < 2\theta\mathcal{R} \bigcap C_\mathrm{E} \geq C_\mathrm{L} \bigcap \mathcal{E}_1\right\} \\
&\quad + \Pr\left\{C_\mathrm{L} - C_\mathrm{E} < 2\theta\mathcal{R} \bigcap C_\mathrm{E} \geq C_\mathrm{L} \bigcap \mathcal{E}_2\right\} \\
&\quad + \Pr\left\{C_\mathrm{L} - C_\mathrm{E} < 2\theta\mathcal{R} \bigcap C_\mathrm{E} \geq C_\mathrm{L} \bigcap \mathcal{E}_3\right\} \\
&= \int_0^\infty \int_{\gamma_{\mathrm{AR}}}^\infty \int_{\gamma_{\mathrm{AB}}}^\infty f_{\gamma_{\mathrm{AE}}} f_{\gamma_{\mathrm{AB}}} f_{\gamma_{\mathrm{AR}}} \,\mathrm{d}\gamma_{\mathrm{AE}}\,\mathrm{d}\gamma_{\mathrm{AB}}\,\mathrm{d}\gamma_{\mathrm{AR}} \\
&\quad + \int_0^\infty \int_{\gamma_{\mathrm{AB}}}^\infty \int_{\gamma_{\mathrm{AR}}}^\infty \int_{\gamma_{\mathrm{AR}}}^\infty f_{\gamma_\mathrm{E}} f_{\gamma_\mathrm{B}} f_{\gamma_{\mathrm{AB}}} f_{\gamma_{\mathrm{AR}}} \,\mathrm{d}\gamma_\mathrm{E}\,\mathrm{d}\gamma_\mathrm{B}\,\mathrm{d}\gamma_{\mathrm{AR}}\,\mathrm{d}\gamma_{\mathrm{AB}} \\
&\quad + \int_0^\infty \int_{\gamma_{\mathrm{AB}}}^\infty \int_0^{\gamma_{\mathrm{AR}}} \int_{\gamma_\mathrm{B}}^\infty f_{\gamma_\mathrm{E}} f_{\gamma_\mathrm{B}} f_{\gamma_{\mathrm{AB}}} f_{\gamma_{\mathrm{AR}}} \,\mathrm{d}\gamma_\mathrm{E}\,\mathrm{d}\gamma_\mathrm{B}\,\mathrm{d}\gamma_{\mathrm{AR}}\,\mathrm{d}\gamma_{\mathrm{AB}}.
\end{aligned} \tag{135}$$

Finalmente, após algumas manipulações algébricas com $A_1 + A_{2\mathrm{a}} - A_{2\mathrm{b}}$ obtém-se que

$$\begin{aligned} p_{\mathrm{gso}}^{(\text{CSI-RC})} \approx & \int_0^\infty \int_{\gamma_{\mathrm{AR}}}^\infty \int_\rho^\infty f_{\gamma_{\mathrm{AE}}} f_{\gamma_{\mathrm{AB}}} f_{\gamma_{\mathrm{AR}}} \,\mathrm{d}\gamma_{\mathrm{AE}} \,\mathrm{d}\gamma_{\mathrm{AB}} \,\mathrm{d}\gamma_{\mathrm{AR}} \\ & + \int_0^\infty \int_{\gamma_{\mathrm{AB}}}^\infty \int_{\gamma_{\mathrm{AR}}}^\infty \int_{\psi(\gamma_{\mathrm{AR}})}^\infty f_{\gamma_{\mathrm{E}}} f_{\gamma_{\mathrm{B}}} f_{\gamma_{\mathrm{AB}}} f_{\gamma_{\mathrm{AR}}} \,\mathrm{d}\gamma_{\mathrm{E}} \,\mathrm{d}\gamma_{\mathrm{B}} \,\mathrm{d}\gamma_{\mathrm{AR}} \,\mathrm{d}\gamma_{\mathrm{AB}} \\ & + \int_0^\infty \int_{\gamma_{\mathrm{AB}}}^\infty \int_0^{\gamma_{\mathrm{AR}}} \int_{\psi(\gamma_{\mathrm{B}})}^\infty f_{\gamma_{\mathrm{E}}} f_{\gamma_{\mathrm{B}}} f_{\gamma_{\mathrm{AB}}} f_{\gamma_{\mathrm{AR}}} \,\mathrm{d}\gamma_{\mathrm{E}} \,\mathrm{d}\gamma_{\mathrm{B}} \,\mathrm{d}\gamma_{\mathrm{AR}} \,\mathrm{d}\gamma_{\mathrm{AB}}, \end{aligned} \tag{136}$$

cuja solução é (16). Além do mais, salientamos que apesar da solução ser uma aproximação assumindo que o *relay* está em uma posição intermediária entre Alice e Bob, o impacto nos resultados da probabilidade de *outage* de segurança são mínimos independentemente da posição do *relay*, conforme mostrado em (FARHAT et al., 2015) para o caso com $\theta = 1$.

APÊNDICE B – PROVA DO LEMA 1

Inicialmente reescrevemos $\Phi_j = \gamma_{\mathrm{A}j} + \gamma_{\mathrm{R}j} + \gamma_{\mathrm{A}j}\gamma_{\mathrm{R}j}$ como

$$\Phi_j = X + Y + \underbrace{XY}_{Z}. \tag{137}$$

Porém, é difícil obter uma expressão exata para a PDF de Φ_j visto que nesta expressão existe a soma e o produto de duas VAs, X e Y, independentes e não identicamente distribuídas, cuja distribuições exponenciais são dadas por $X \sim \mathrm{Exp}\left(\frac{1}{\bar{\gamma}_{\mathrm{A}j}}\right)$ e $Y \sim \mathrm{Exp}\left(\frac{1}{\bar{\gamma}_{\mathrm{R}j}}\right)$. Para obtenção da PDF, nós consideramos uma aproximação realizada em dois passos, na qual a primeira parte realiza a aproximação do produto $Z = XY$ por uma única VA com distribuição Gamma, enquanto aproximamos a soma $X + Y + Z$ novamente por outra VA com distribuição Gamma.

Começando pelo produto $Z = XY$, utilizamos o fato que uma VA exponencial com parâmetro β pode ser representada por uma VA Gamma com parâmetros $k = 1$ e $\Theta = \frac{1}{\beta}$. Portanto, $X \sim \mathrm{Gamma}\left(k = 1, \bar{\gamma}_{\mathrm{A}j}\right)$ e $Y \sim \mathrm{Gamma}\left(k = 1, \bar{\gamma}_{\mathrm{R}j}\right)$.

Então, seguimos um procedimento similar à (KARAGIANNIDIS et al., 2005; ALVES et al., 2013), no qual os autores aproximam o produto de duas VAs com distribuição Nakagami-m por uma única VA também com distribuição Nakagami-m utilizando o método dos momentos. No caso deste documento, o objetivo é realizar a aproximação de Z por uma distribuição Gamma, de forma que $Z \sim \mathrm{Gamma}\left(\xi, \varrho\right)$. Porém, a aplicação direta do método dos momentos assim como em (ALVES et al., 2013) produz uma aproximação com diversidade diferente no caso da distribuição Gamma. Portanto já que o parâmetro de forma da curva (do inglês, *shape parameter*), ξ, está relacionado à inclinação da curva e já que ambos X e Y apresentam o parâmetro de forma da curva igual a um, observamos que uma aproximação mais precisa pode ser obtida a partir da consideração de $\xi = 1$ e calculando ϱ de acordo com o segundo momento da distribuição Gamma.

O n-ésimo momento de Z é dado por

$$\mathbb{E}\left[Z^n\right] = \frac{\Gamma[\xi+n]\varrho^n}{\Gamma[\xi]}, \tag{138}$$

enquanto o n-ésimo momento conjunto de XY é (Papoulis; Pillai, 2002)

$$\mathbb{E}\left[(XY)^n\right] = \frac{\Gamma[k+n](\bar{\gamma}_{\mathrm{A}j})^n}{\Gamma[k]} \times \frac{\Gamma[k+n](\bar{\gamma}_{\mathrm{R}j})^n}{\Gamma[k]}. \tag{139}$$

Desta forma, coincidindo os segundos momentos de (138) com (139) obtemos $\varrho = \sqrt{2}\bar{\gamma}_{\mathrm{A}j}\bar{\gamma}_{\mathrm{R}j}$, de forma que $Z \sim \mathrm{Gamma}\left(1, \sqrt{2}\bar{\gamma}_{\mathrm{A}j}\bar{\gamma}_{\mathrm{R}j}\right)$.

Para realizar a aproximação da soma $X+Y+Z$ por uma única VA Gamma Φ_j, baseando-se em (FILHO; YACOUB, 2004), consideramos $\Phi_j \sim \mathrm{Gamma}(m_j, \frac{\Omega_j}{m})$, com $\Omega_j = \mathbb{E}[\Phi_j]$ e $m_j = \frac{\Omega_j^2}{\mathrm{E}[\Phi_j^2]-\Omega_j^2}$, onde o n-ésimo momento de Φ_j pode ser obtido utilizando uma expansão multinomial representada por (Papoulis; Pillai, 2002)

$$\mathbb{E}\left[\Phi_j^n\right] = \sum_{n_1=0}^{n}\sum_{n_2=0}^{n_1}\binom{n}{n_1}\binom{n_1}{n_2}\mathbb{E}\left[X^{(n-n_1)}\right]\mathbb{E}\left[Y^{(n_1-n_2)}\right]\mathbb{E}\left[Z^{n_2}\right], \tag{140}$$

em que obtém-se $m_j = \frac{{\Omega_j}^2}{\bar{\gamma}_{\mathrm{R}j}^2+\bar{\gamma}_{\mathrm{A}j}^2+\left(\sqrt{2}\,\bar{\gamma}_{\mathrm{A}j}\,\bar{\gamma}_{\mathrm{R}j}\right)^2}$ e $\Omega_j = \bar{\gamma}_{\mathrm{R}j} + \bar{\gamma}_{\mathrm{A}j} + \left(\sqrt{2}\,\bar{\gamma}_{\mathrm{A}j}\,\bar{\gamma}_{\mathrm{R}j}\right)$.

Finalmente, a PDF de Φ_j leva a (21), concluindo a prova.

APÊNDICE C – PROVA DO TEOREMA 2

Como no caso do CSI-RC, a mesma aproximação é considerada para escolha de Alice entre transmissão direta ou cooperativa, na qual a transmissão direta ocorre sempre que $\gamma_{\mathrm{AB}} \geq \gamma_{\mathrm{AR}}$ e a transmissão cooperativa ocorre quando $\gamma_{\mathrm{AR}} > \gamma_{\mathrm{AB}}$. Redefinindo os três possíveis sub-casos, nós obtemos:

- $\mathcal{E}_1 = \{\gamma_{\mathrm{AB}} \geq \gamma_{\mathrm{AR}}\}$, indicando transmissão direta – a mesma que da CSI-RC;
- $\mathcal{E}_2' = \{\gamma_{\mathrm{AB}} < \gamma_{\mathrm{AR}} \bigcap \gamma_{\mathrm{AR}} < \Phi_{\mathrm{B}}\}$, indicando cooperação com a capacidade limitada pelo canal A-R;
- $\mathcal{E}_3' = \{\gamma_{\mathrm{AB}} < \gamma_{\mathrm{AR}} \bigcap \gamma_{\mathrm{AR}} \geq \Phi_{\mathrm{B}}\}$, indicando cooperação com a capacidade limitada por Bob,

e seguindo o mesmo procedimento do Apêndice A, obtêm-se

$$\begin{aligned} p_{\mathrm{gso}}^{(\text{CSI-PC})} \approx & \int_0^\infty \int_{\gamma_{\mathrm{AR}}}^\infty \int_{\rho'}^\infty f_{\gamma_{\mathrm{AE}}} f_{\gamma_{\mathrm{AB}}} f_{\gamma_{\mathrm{AR}}} \,\mathrm{d}\gamma_{\mathrm{AE}} \,\mathrm{d}\gamma_{\mathrm{AB}} \,\mathrm{d}\gamma_{\mathrm{AR}} \\ & + \int_0^\infty \int_{\gamma_{\mathrm{AB}}}^\infty \int_{\gamma_{\mathrm{AR}}}^\infty \int_{\psi'(\gamma_{\mathrm{AR}})}^\infty f_{\Phi_{\mathrm{E}}} f_{\Phi_{\mathrm{B}}} f_{\gamma_{\mathrm{AB}}} f_{\gamma_{\mathrm{AR}}} \,\mathrm{d}\Phi_{\mathrm{E}} \,\mathrm{d}\Phi_{\mathrm{B}} \,\mathrm{d}\gamma_{\mathrm{AR}} \,\mathrm{d}\gamma_{\mathrm{AB}} \\ & + \int_0^\infty \int_{\gamma_{\mathrm{AB}}}^\infty \int_0^{\gamma_{\mathrm{AR}}} \int_{\psi'(\Phi_{\mathrm{B}})}^\infty f_{\Phi_{\mathrm{E}}} f_{\Phi_{\mathrm{B}}} f_{\gamma_{\mathrm{AB}}} f_{\gamma_{\mathrm{AR}}} \,\mathrm{d}\Phi_{\mathrm{E}} \,\mathrm{d}\Phi_{\mathrm{B}} \,\mathrm{d}\gamma_{\mathrm{AR}} \,\mathrm{d}\gamma_{\mathrm{AB}}, \end{aligned} \tag{141}$$

onde $\rho' = 2^{-\theta\mathcal{R}}(1+\gamma_{\mathrm{AB}}) - 1$. Para simplificar a análise relembramos que assumimos $\log_2(1+x) \approx \log_2(x)$, de forma que $\psi'(x) = 2^{-2\theta\mathcal{R}}x$ é empregado em (141). Esta aproximação foi validada por diversas simulações em que é mostrado uma boa concordância entre o caso real e a aproximação em todo intervalo de SNR considerado nos resultados numéricos.

Finalmente, para resolução de (141) é necessário recorrer a (GRADSHTEYN; RYZHIK, 2007, Eq. (3.351.1)) e (GRADSHTEYN; RYZHIK, 2007, Eq. (6.455.2)), na qual, após algumas manipulações algébricas, chega-se ao resultado mostrado em (22).

APÊNDICE D – PROVA DA PROPOSIÇÃO 1

Similarmente ao Apêndice A, reescrevemos $p_{\text{gso}}^{(\text{DF})}$ como uma soma de dois termos e tratamos cada intersecção individualmente. Além do mais, destacamos que a solução para DF é semelhante a um sub-caso da solução do CSI-RC, já que o CSI-RC envolve a escolha entre o DF tradicional e a transmissão direta. De forma que $p_{\text{gso}}^{(\text{DF})}$ se reduz a

$$p_{\text{gso}}^{(\text{DF})} = \int_0^\infty \int_{\gamma_{\text{AR}}}^\infty \int_{\psi(\gamma_{\text{AR}})}^\infty f_{\gamma_{\text{B}}} f_{\gamma_{\text{E}}} f_{\gamma_{\text{AR}}} \, \mathrm{d}\gamma_{\text{E}} \, \mathrm{d}\gamma_{\text{B}} \, \mathrm{d}\gamma_{\text{AR}} + \int_0^\infty \int_0^{\gamma_{\text{AR}}} \int_{\psi(\gamma_{\text{B}})}^\infty f_{\gamma_{\text{B}}} f_{\gamma_{\text{E}}} f_{\gamma_{\text{AR}}} \, \mathrm{d}\gamma_{\text{E}} \, \mathrm{d}\gamma_{\text{B}} \, \mathrm{d}\gamma_{\text{AR}}, \tag{142}$$

cuja solução é dada por (26).

APÊNDICE E – PROVA DA PROPOSIÇÃO 2

Primeiramente, reescrevemos $p_{\text{gso}}^{(\text{AF})}$ como uma soma de B_1 e B_2. Porém, como em (GABRY et al., 2013), nós precisamos considerar uma aproximação em alta SNR para definir $\gamma_{\text{B}'} = \gamma_{\text{AB}} + \frac{\gamma_{\text{AR}}\gamma_{\text{RB}}}{\gamma_{\text{AR}}+\gamma_{\text{RB}}}$ e $\gamma_{\text{E}'} = \gamma_{\text{AE}} + \frac{\gamma_{\text{AR}}\gamma_{\text{RE}}}{\gamma_{\text{AR}}+\gamma_{\text{RE}}}$, de forma que B_1 pode ser aproximada por

$$B_1 \approx \Pr\left\{\gamma_{\text{B}'} < \gamma_{\text{E}'}\right\}, \tag{143}$$

enquanto

$$B_2 = \Pr\left\{C_{\text{L}} - C_{\text{E}} < 2\theta\mathcal{R} \bigcap C_{\text{L}} - 2\mathcal{R} < C_{\text{E}}\right\} - \Pr\left\{C_{\text{L}} - C_{\text{E}} < 2\theta\mathcal{R} \bigcap C_{\text{E}} \geq C_{\text{L}}\right\}. \tag{144}$$

Simplificando as intersecções, obtemos

$$p_{\text{gso}}^{(\text{AF})} \approx \int_0^{\infty} \int_0^{2^{2\theta\mathcal{R}}(1+\gamma_{\text{E}'})-1} f_{\gamma_{\text{B}'}} f_{\gamma_{\text{E}'}} \, \text{d}\gamma_{\text{B}'} \text{d}\gamma_{\text{E}'}, \tag{145}$$

cuja solução é dada por (30).

APÊNDICE F – PROVA DA PROPOSIÇÃO 3

Considerando a mesma abordagem do Apêndice E, dividindo a solução em subcasos, mostra-se que

$$p_{\text{gso}}^{(\text{CJ})} = \int_0^{\infty}\int_0^{\infty}\int_0^{\infty}\int_0^{\sigma} f_{\gamma_{\text{AB}}} f_{\gamma_{\text{RB}}} f_{\gamma_{\text{AE}}} f_{\gamma_{\text{RE}}} \, \mathrm{d}\gamma_{\text{AB}} \mathrm{d}\gamma_{\text{RB}} \mathrm{d}\gamma_{\text{AE}} \mathrm{d}\gamma_{\text{RE}}, \tag{146}$$

onde $\sigma = \left[\left(1 + \frac{\gamma_{\text{AE}}}{1+\gamma_{\text{RE}}}\right) 2^{\theta\mathcal{R}} - 1\right](1+\gamma_{\text{RB}})$, e cuja solução é dada por (35), concluindo a prova.

REFERÊNCIAS

ALVES, H.; COSTA, D. B. da; SOUZA, R. D.; LATVA-AHO, M. Performance of block-markov full duplex relaying with self interference in nakagami-m fading. **IEEE Wireless Commun. Letters**, v. 2, n. 3, p. 311–314, Jun 2013. ISSN 2162-2337.

ALVES, H.; SOUZA, R.; DEBBAH, M.; BENNIS, M. Performance of transmit antenna selection physical layer security schemes. **IEEE Signal Process. Lett.**, v. 19, n. 6, p. 372–375, June 2012. ISSN 1070-9908.

ALVES, H.; TOME, M. D. C.; NARDELLI, P. H. J.; LIMA, C. H. M. D.; LATVA-AHO, M. Enhanced transmit antenna selection scheme for secure throughput maximization without csi at the transmitter. **IEEE Access**, v. 4, p. 4861–4873, 2016. ISSN 2169-3536.

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 Trans. Inf. Theory**, v. 54, n. 6, p. 2515–2534, Jun. 2008. ISSN 0018-9448.

BRANTE, G.; ALVES, H.; SOUZA, R.; LATVA-AHO, M. Secrecy analysis of transmit antenna selection cooperative schemes with no channel state information at the transmitter. **IEEE Trans. Commun.**, v. 63, n. 4, p. 1330–1342, Apr. 2015. ISSN 0090-6778.

BRANTE, G.; STUPIA, I.; SOUZA, R. D.; VANDENDORPE, L. Outage probability and energy efficiency of cooperative MIMO with antenna selection. **IEEE Trans. Wireless Commun.**, v. 12, n. 11, p. 5896–5907, Nov. 2013. ISSN 1536-1276.

BURICH, M. E.; SOUZA, R. D.; BRANTE, G.; ONIRETI, O.; IMRAN, M. A. On the impact of HARQ on the throughput and energy efficiency using cross-layer analysis. In: **2017 Wireless Days**. 2017. p. 146–151.

CAO, C.; LI, H.; HU, Z.; LIU, W.; ZHANG, X. Physical-layer secrecy performance in finite blocklength case. In: **IEEE Global Commun. Conf.** 2015. p. 1–6.

CHEN, J.; YANG, L.; ALOUINI, M. S. Physical layer security for cooperative NOMA systems. **IEEE Trans. Vehicular Technol.**, p. 1–1, 2018. ISSN 0018-9545.

CHEN, X.; LEI, L.; ZHANG, H.; YUEN, C. Large-scale MIMO relaying techniques for physical layer security: AF or DF? **IEEE Trans. Wireless Commun.**, v. 14, n. 9, p. 5135–5146, Sep 2015. ISSN 1536-1276.

CHOI, S.; KO, Y.-C.; POWERS, E. J. Performance analysis of maximal-ratio combining with transmit antenna selection for generalized selection criterion. In: **IEEE Vehicular Technol. Conf.** 2005. p. 2039–2042. ISSN 1090-3038.

CHORTI, A.; PAPADAKI, K.; POOR, H. Optimal power allocation in block fading channels with confidential messages. **IEEE Trans. Wireless Commun.**, v. 14, n. 9, p. 4708–4719, Sep 2015. ISSN 1536-1276.

COSTA, D. B.; FERDINAND, N. S.; DIAS, U. S.; JUNIOR, R. T. de S.; LATVA-AHO, M. Secrecy outage performance of MIMO wiretap channels with multiple jamming signals. **J. Commun. Inf. Systems**, 2016.

CSISZAR, I.; KORNER, J. Broadcast channels with confidential messages. **IEEE Trans. Inf. Theory**, v. 24, n. 3, p. 339–348, May 1978. ISSN 0018-9448.

CUI, S.; GOLDSMITH, A.; BAHAI, A. Energy-efficiency of MIMO and cooperative MIMO techniques in sensor networks. **IEEE J. Sel. Areas Commun.**, v. 22, n. 6, p. 1089–1098, Aug. 2004. ISSN 0733-8716.

DENG, H.; WANG, H. M.; GUO, W.; WANG, W. Secrecy transmission with a helper: To relay or to jam. **IEEE Trans. Inf. Forensics and Security**, v. 10, n. 2, p. 293–307, Feb 2015. ISSN 1556-6013.

DING, Z.; LEUNG, K.; GOECKEL, D.; TOWSLEY, D. On the application of cooperative transmission to secrecy communications. **IEEE J. Sel. Areas Commun.**, v. 30, n. 2, p. 359–368, Feb 2012. ISSN 0733-8716.

DINKELBACH, W. On nonlinear fractional programming. **Manag. Sci.**, v. 13, n. 7, p. 492–498, Mar. 1967.

DONG, L.; HAN, Z.; PETROPULU, A.; POOR, H. Improving wireless physical layer security via cooperating relays. **IEEE Trans. Signal Process**, v. 58, n. 3, p. 1875–1888, Mar. 2010. ISSN 1053-587X.

DU, F.; HU, Y.; QIU, L.; SCHMEINK, A. Finite blocklength performance of multi-hop relaying networks. In: **IEEE Int. Symp. on Wireless Commun Systems**. 2016. p. 466–470.

DURISI, G.; KOCH, T.; POPOVSKI, P. Toward massive, ultrareliable, and low-latency wireless communication with short packets. **Proc. IEEE**, v. 104, n. 9, p. 1711–1726, Sept 2016. ISSN 0018-9219.

FARHAT, J.; BRANTE, G.; SOUZA, R.; REBELATTO, J. Energy efficiency of repetition coding and parallel coding relaying under partial secrecy regime. **IEEE Access**, PP, n. 99, p. 1–1, 2016. ISSN 2169-3536.

FARHAT, J. A.; BRANTE, G.; SOUZA, R. D.; REBELATTO, J. L. Secure energy efficiency of selective decode and forward with distributed power allocation. **IEEE 12th Int. Symp. Wireless Commun. Systems**, 2015.

FILHO, J. C. S. S.; YACOUB, M. D. Nakagami-m approximation to the sum of m non-identical independent nakagami-m variates. **Electronics Letters**, v. 40, n. 15, p. 951–952, Jul 2004. ISSN 0013-5194.

GABRY, F.; SALIMI, S.; THOBABEN, R.; SKOGLUND, M. High SNR performance of amplify-and-forward relaying in Rayleigh fading wiretap channels. In: **Iran Workshop Commun. Inf. Theory (IWCIT)**. 2013. p. 1–5.

GABRY, F.; THOBABEN, R.; SKOGLUND, M. Outage performance and power allocation for decode-and-forward relaying and cooperative jamming for the wiretap channel. In: **IEEE Int. Conf. Commun.** 2011. p. 1–5.

GABRY, F.; THOBABEN, R.; SKOGLUND, M. Outage performances for amplify-and-forward, decode-and-forward and cooperative jamming strategies for the wiretap channel. In: **IEEE Wireless Commun. Netw. Conf. (WCNC)**. 2011. p. 1328–1333. ISSN 1525-3511.

GOLDSMITH, A. **Wireless Communications**. New York, NY, USA: Cambridge University Press, 2005. ISBN 0521837162.

GOPALA, P. K.; LAI, L.; GAMAL, H. E. On the secrecy capacity of fading channels. **IEEE Trans. Inf. Theory**, v. 54, n. 10, p. 4687–4698, Oct 2008. ISSN 0018-9448.

GRADSHTEYN, I. S.; RYZHIK, I. M. **Table of integrals, series, and products**. Seventh. Elsevier/Academic Press, Amsterdam, 2007. xlviii+1171 p. ISBN 978-0-12-373637-6; 0-12-373637-4.

HE, B. **Wireless Physical Layer Security: Towards Practical Assumptions and Requirements**. 2016. Tese (Doutorado) — Research School of Engineering, College of Engineering and Computer Science, The Australian National University, 2016.

HE, B.; LIU, A.; YANG, N.; LAU, V. K. N. On the design of secure non-orthogonal multiple access systems. **IEEE J. Sel. Areas Commun.**, v. 35, n. 10, p. 2196–2206, Oct 2017. ISSN 0733-8716.

HE, B.; ZHOU, X. New physical layer security measures for wireless transmissions over fading channels. In: **IEEE Global Commun. Conf.** 2014. p. 722–727.

HU, Y.; GROSS, J.; SCHMEINK, A. On the capacity of relaying with finite blocklength. **IEEE Trans. Vehicular Technol.**, v. 65, n. 3, p. 1790–1794, March 2016. ISSN 0018-9545.

HU, Y.; SCHMEINK, A.; GROSS, J. Blocklength-limited performance of relaying under quasi-static rayleigh channels. **IEEE Trans. Wireless Commun.**, v. 15, n. 7, p. 4548–4558, July 2016. ISSN 1536-1276.

HU, Y.; SCHMEINK, A.; GROSS, J. Relaying with finite blocklength: Challenge vs. opportunity. In: **IEEE Sensor Array and Multichannel Signal Process. Workshop**. 2016. p. 1–5.

HUI, H.; SWINDLEHURST, A. L.; LI, G.; LIANG, J. Secure relay and jammer selection for physical layer security. **IEEE Signal Process. Letters**, v. 22, n. 8, p. 1147–1151, Aug 2015. ISSN 1070-9908.

JU, Y.; WANG, H. M.; ZHENG, T. X.; YIN, Q. Secure transmissions in millimeter wave systems. **IEEE Trans. Commun.**, v. 65, n. 5, p. 2114–2127, May 2017. ISSN 0090-6778.

KARAGIANNIDIS, G. K.; SAGIAS, N. C.; MATHIOPOULOS, T. The N*Nakagami fading channel model. In: **Proc. IEEE 2nd Int. Symp. Wireless Commun. Systems**. 2005. p. 185–189. ISSN 2154-0217.

KHORMUJI, M. N.; LARSSON, E. G. Cooperative transmission based on decode-and-forward relaying with partial repetition coding. **IEEE Trans. on Wireless Commun.**, v. 8, n. 4, p. 1716–1725, Apr 2009. ISSN 1536-1276.

LAI, L.; GAMAL, H. E. The relay-eavesdropper channel: Cooperation for secrecy. **IEEE Trans. Inf. Theory**, v. 54, n. 9, p. 4005–4019, Sep. 2008. ISSN 0018-9448.

LANEMAN, J. N.; TSE, D. N. C.; WORNELL, G. W. Cooperative diversity in wireless networks: Efficient protocols and outage behavior. **IEEE Trans. Inf. Theory**, v. 50, n. 12, p. 3062–3080, Dec. 2004.

LI, J.; PETROPULU, A.; WEBER, S. On cooperative relaying schemes for wireless physical layer security. **IEEE Trans. Signal Process**, v. 59, n. 10, p. 4985–4997, Oct 2011. ISSN 1053-587X.

LI, L.; PETROPULU, A. P.; CHEN, Z. MIMO secret communications against an active eavesdropper. **IEEE Trans. Inf. Forensics and Security**, v. 12, n. 10, p. 2387–2401, Oct 2017. ISSN 1556-6013.

LIN, H.; ZHAO, R.; HE, Y.; HUANG, Y. Secrecy performance of transmit antenna selection with outdated csi for MIMO relay systems. In: **IEEE Int. Conf. Commun.** 2016. p. 272–277.

LIU, T.; MUKHERJEE, P.; ULUKUS, S.; LIN, S.; HONG, Y. P. Secure degrees of freedom of MIMO Rayleigh block fading wiretap channels with no CSI anywhere. **IEEE Trans. Wireless Commun.**, v. 14, n. 5, p. 2655–2669, May 2015. ISSN 1536-1276.

MAKKI, B.; SVENSSON, T.; ZORZI, M. Wireless energy and information transmission using feedback: Infinite and finite block-length analysis. **IEEE Trans. Commun.**, v. 64, n. 12, p. 5304–5318, Dec. 2016. ISSN 0090-6778.

MEULEN, E. C. van der. Three-terminal communication channels. **Adv. Appl. Probab.**, v. 3, p. 120–154, 1971.

MUCCHI, L.; RONGA, L.; HUANG, K.; CHEN, Y.; WANG, R. A new physical-layer security measure - secrecy pressure. In: **IEEE Global Commun. Conf.** 2017. p. 1–6.

PAPOULIS, A. **Probability, random variables, and stochastic processes**. New York: McGraw-Hill, 1991. ISBN 0-07-100870-5.

Papoulis, A.; Pillai, S. **Probability, Random Variables, and Stochastic Processes**. 4. ed. McGraw-Hill Higher Education, 2002.

POLYANSKIY, Y.; POOR, H. V.; VERDU, S. Channel coding rate in the finite blocklength regime. **IEEE Trans. Inf. Theory**, v. 56, n. 5, p. 2307–2359, May 2010. ISSN 0018-9448.

POPOVSKI, P. Ultra-reliable communication in 5g wireless systems. In: **Int. Conf. on 5G for Ubiquitous Connectivity**. 2014. p. 146–151.

PRESS, W. H.; TEUKOLSKY, S. A.; VETTERLING, W. T.; FLANNERY, B. P. **Numerical Recipes 3rd Edition: The Art of Scientific Computing**. 3. ed. New York, NY, USA: Cambridge University Press, 2007. ISBN 0521880688, 9780521880688.

PROAKIS, J.; SALEHI, M. **Digital Communications**. McGraw-Hill, 2008. (McGraw-Hill International Edition). ISBN 9780071263788.

QIN, Z.; LIU, Y.; DING, Z.; GAO, Y.; ELKASHLAN, M. Physical layer security for 5g non-orthogonal multiple access in large-scale networks. In: **IEEE Int. Conf. Commun.** 2016. p. 1–6.

SHANNON, C. Communication theory of secrecy systems. **Bell Syst. Tech. J.**, v. 28, n. 4, p. 656–715, Oct. 1949. ISSN 0005-8580.

SU, W.; LEE, S.; PADOS, D. A.; MATYJAS, J. D. Optimal power assignment for minimizing the average total transmission power in hybrid-ARQ rayleigh fading links. **IEEE Trans. Commun.**, v. 59, n. 7, p. 1867–1877, July 2011. ISSN 0090-6778.

SUN, L.; DU, Q. Physical layer security with its applications in 5g networks: A review. **China Communications**, v. 14, n. 12, p. 1–14, December 2017. ISSN 1673-5447.

TANG, X.; LIU, R.; SPASOJEVIC, P. On the achievable secrecy throughput of block fading channels with no channel state information at transmitter. In: **41st Annual Conf. Inf. Sciences Syst. (CISS)**. 2007. p. 917–922.

TANG, X.; LIU, R.; SPASOJEVIC, P.; POOR, H. On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels. **IEEE Trans. Inf. Theory**, v. 55, n. 4, p. 1575–1591, Apr. 2009. ISSN 0018-9448.

TANG, X.; REN, P.; WANG, Y.; HAN, Z. Combating full-duplex active eavesdropper: A hierarchical game perspective. **IEEE Trans. Commun.**, v. 65, n. 3, p. 1379–1395, March 2017. ISSN 0090-6778.

VILELA, J.; BLOCH, M.; BARROS, J.; MCLAUGHLIN, S. Wireless secrecy regions with friendly jamming. **IEEE Trans. Inf. Forensics Security**, v. 6, n. 2, p. 256–266, Jun. 2011. ISSN 1556-6013.

WANG, D.; BAI, B.; CHEN, W.; HAN, Z. Energy efficient secure communication over decode-and-forward relay channels. **IEEE Trans. Commun.**, v. 63, n. 3, p. 892–905, March 2015. ISSN 0090-6778.

WANG, H. M.; LIU, F.; YANG, M. Joint cooperative beamforming, jamming, and power allocation to secure AF relay systems. **IEEE Trans. Vehicular Technol.**, v. 64, n. 10, p. 4893–4898, Oct. 2015. ISSN 0018-9545.

WANG, H. M.; ZHENG, T.; XIA, X. G. Secure miso wiretap channels with multiantenna passive eavesdropper: Artificial noise vs. artificial fast fading. **IEEE Trans. Wireless Commun.**, v. 14, n. 1, p. 94–106, Jan 2015. ISSN 1536-1276.

WANG, X.; TAO, M.; XU, Y. Outage analysis of cooperative secrecy multicast transmission. **IEEE Wireless Commun. Letters**, v. 3, n. 2, p. 161–164, Apr. 2014. ISSN 2162-2337.

WU, J.; WANG, G.; ZHENG, Y. R. Energy efficiency and spectral efficiency tradeoff in type-i ARQ systems. **IEEE J. Sel. Areas Commun.**, v. 32, n. 2, p. 356–366, February 2014. ISSN 0733-8716.

WYNER, A. The wire-tap channel. **Bell Syst. Tech. J.**, v. 54, n. 8, p. 1355–1387, Oct 1975. ISSN 0005-8580.

YANG, K.; YANG, N.; XING, C.; WU, J.; ZHANG, Z. Space-time network coding with transmit antenna selection and maximal-ratio combining. **IEEE Trans. Wireless Commun.**, v. 14, n. 4, p. 2106–2117, Apr. 2015. ISSN 1536-1276.

YANG, N.; SURAWEERA, H.; COLLINGS, I.; YUEN, C. Physical layer security of TAS/MRC with antenna correlation. **IEEE Trans. Inf. Forensics Security**, v. 8, n. 1, p. 254–259, Jan. 2013. ISSN 1556-6013.

YANG, N.; YEOH, P. L.; ELKASHLAN, M.; SCHOBER, R.; COLLINGS, I. B. Secure transmission via transmit antenna selection in MIMO wiretap channels. In: **IEEE Global Commun. Conf.** 2012. p. 789–794. ISSN 1930-529X.

YANG, N.; YEOH, P. L.; ELKASHLAN, M.; SCHOBER, R.; COLLINGS, I. B. Transmit antenna selection for security enhancement in MIMO wiretap channels. **IEEE Trans. Commun.**, v. 61, n. 1, p. 144–154, Jan. 2013. ISSN 0090-6778.

YANG, W.; DURISI, G.; KOCH, T.; POLYANSKIY, Y. Diversity versus channel knowledge at finite block-length. In: **IEEE Inf. Theory Workshop**. 2012. p. 572–576.

YANG, W.; DURISI, G.; KOCH, T.; POLYANSKIY, Y. Block-fading channels at finite blocklength. In: **IEEE 10th Int. Symp. Wireless Commun. Systems**. 2013. p. 1–4.

YANG, W.; SCHAEFER, R. F.; POOR, H. V. Finite-blocklength bounds for wiretap channels. In: **IEEE Int. Symp. Inf. Theory**. 2016. p. 3087–3091.

YOO, T.; JINDAL, N.; GOLDSMITH, A. Multi-antenna downlink channels with limited feedback and user selection. **IEEE J. Sel. Areas Commun.**, v. 25, n. 7, p. 1478–1491, Sep. 2007. ISSN 0733-8716.

ZAPPONE, A.; JORSWIECK, E. Energy efficiency in wireless networks via fractional programming theory. **Foundations and Trends in Communications and Information Theory**, v. 11, n. 3-4, p. 185–396, 2014. ISSN 1567-2190.

ZAPPONE, A.; LIN, P.-H.; JORSWIECK, E. Energy-efficient secure communications in MISO-SE systems. In: **48th Asilomar Conf. on Signals, Systems and Computers**. 2014. p. 1001–1005.

ZAPPONE, A.; LIN, P. H.; JORSWIECK, E. Optimal energy-efficient design of confidential multiple-antenna systems. **IEEE Trans. Inf. Forensics Security**, v. 13, n. 1, p. 237–252, Jan 2018. ISSN 1556-6013.

ZHANG, X.; MCKAY, M. R.; ZHOU, X.; HEATH, R. W. Artificial-noise-aided secure multi-antenna transmission with limited feedback. **IEEE Trans. Wireless Commun.**, v. 14, n. 5, p. 2742–2754, May 2015. ISSN 1536-1276.

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

ZHENG, T.-X.; WANG, H.-M.; LIU, F.; LEE, M. H. Outage constrained secrecy throughput maximization for df relay networks. **IEEE Trans. Commun.**, v. 63, n. 5, p. 1741–1755, May 2015. ISSN 0090-6778.

ZHU, Y.; WANG, L.; WONG, K. K.; HEATH, R. W. Secure communications in millimeter wave ad hoc networks. **IEEE Trans. on Wireless Commun.**, v. 16, n. 5, p. 3205–3217, May 2017. ISSN 1536-1276.

ZHU, Y.; ZHOU, Y.; PATEL, S.; CHEN, X.; PANG, L.; XUE, Z. Artificial noise generated in MIMO scenario: Optimal power design. **IEEE Signal Process. Letters**, v. 20, n. 10, p. 964–967, Oct 2013. ISSN 1070-9908.

ZOU, Y.; ZHU, J.; WANG, X.; LEUNG, V. C. M. Improving physical-layer security in wireless communications using diversity techniques. **IEEE Network**, v. 29, n. 1, p. 42–48, Jan. 2015. ISSN 0890-8044.

ZOU, Y.; ZHU, J.; WANG, X.; HANZO, L. A survey on wireless security: Technical challenges, recent advances, and future trends. **Proc. IEEE**, v. 104, n. 9, p. 1727–1765, Sept 2016. ISSN 0018-9219.