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

JAMIL DE ARAUJO FARHAT

EFICIÊNCIA ENERGÉTICA E THROUGHPUT SEGUROS EM DECODE-AND-FORWARD SELETIVO COM ALOCAÇÃO DE POTÊNCIA DISTRIBUÍDA

DISSERTAÇÃO

CURITIBA
2015

JAMIL DE ARAUJO FARHAT

EFICIÊNCIA ENERGÉTICA E THROUGHPUT SEGUROS EM DECODE-AND-FORWARD SELETIVO COM ALOCAÇÃO DE POTÊNCIA DISTRIBUÍDA

Dissertação apresentada ao Programa de Pós-graduação em Engenharia Elétrica e Informática Industrial da Universidade Tecnológica Federal do Paraná como requisito parcial para obtenção do grau de "Mestre em Ciências" – Área de Concentração: Telecomunicações e Redes.

Orientador: Prof. Dr. Glauber Gomes de Oliveira Brante

Coorientador: Prof. Dr. Richard Demo Souza

CURITIBA
2015

Dados Internacionais de Catalogação na Publicação

F223e 2015

Farhat, Jamil de Araújo
Eficiência energética e *throughput* seguros em *decode-and-forward* seletivo com alocação de potência distribuída / Jamil de Araújo Farhat.-- 2015.
47 f.: il.; 30 cm

Texto em português, com resumo em inglês.
Dissertação (Mestrado) - Universidade Tecnológica Federal do Paraná. Programa de Pós-graduação em Engenharia Elétrica e Informática Industrial, Curitiba, 2015.
Bibliografia: f. 45-47.

1. Sistemas de comunicação sem fio - Conservação de energia 2. Sistemas de transmissão de dados - Medidas de segurança. 3. Sistemas MIMO. 4. Processamento de sinais - Técnicas digitais. 5. Algoritmos. 6. Redes de computação - Protocolos. 7. Otimização matemática. 8. Métodos de simulação. 9. Engenharia elétrica - Dissertações. 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 22 -- 621.3

Biblioteca Central da UTFPR, Câmpus Curitiba

Título da Dissertação Nº. 689

Eficiência Energética e Throughput Seguros em Decode-and-Forward Seletivo com Alocação de Potência Distribuída.

por

Jamil de Araujo Farhat

Orientador: Prof. Dr. Glauber Gomes de Oliveira Brante
Coorientador: Prof Dr. Richard Demo Souza

Esta dissertação foi apresentada como requisito parcial à obtenção do grau de MESTRE EM CIÊNCIAS – Área de Concentração: **Telecomunicações e Redes** do Programa de Pós-Graduação em Engenharia Elétrica e Informática Industrial – CPGEI – da Universidade Tecnológica Federal do Paraná – UTFPR, às **9**:**30h** do dia **19 de junho de 2015**. O trabalho foi aprovado pela Banca Examinadora, composta pelos professores doutores:

Prof. Dr. Glauber Gomes de Oliveira Brante
(Presidente – UTFPR)

Prof. Dr. Evelio Martin Garcia Fernandez
(UFPR)

Prof. Dr. Ohara Kerusauskas Rayel
(UTFPR)

Visto da coordenação:

Prof. Emilio Carlos Gomes Wille, Dr.
(Coordenador do CPGEI)

A Folha de Aprovação assinada encontra-se na Coordenação do Programa de Pós-Graduação em Engenharia Elétrica e Informática Industrial.

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 demais familiares por todo amor e confiança. Também ao meu irmão, Nader de Araujo Farhat, que sempre me apoiou.

À minha namorada, Rayta Paim Horta, que sempre esteve disposta a me apoiar, orientar sobre dúvidas ortográficas e dar palpites diversos sobre a escrita deste trabalho;

Aos meus orientadores, Glauber Brante e Richard Souza, que sempre estiveram dispostos a me motivar, dar novas ideias e orientar sobre o caminho a ser tomado para realização deste trabalho;

Aos meus gerentes do Banco do Brasil, Flavio Puperi e Iana Marchioro, e demais colegas pela compreensão, paciência e apoio;

Aos meus amigos por toda paciência e apoio.

RESUMO

Farhat, Jamil. EFICIÊNCIA ENERGÉTICA E THROUGHPUT SEGUROS EM DECODE-AND-FORWARD SELETIVO COM ALOCAÇÃO DE POTÊNCIA DISTRIBUÍDA. 47 f. Dissertação – Programa de Pós-graduação em Engenharia Elétrica e Informática Industrial, Universidade Tecnológica Federal do Paraná. Curitiba, 2015.

Investiga-se a eficiência energética e o *throughput* seguros em sistemas de comunicações sem fio cooperativos, em que um par de usuários legítimos (Alice e Bob) são auxiliados por um nó *relay* e em que a comunicação ocorre na presença de um espião passivo (Eve). Diversos protocolos cooperativos são comparados em relação a estas medidas e se utiliza um algoritmo iterativo e distribuído, baseado no algoritmo Dinkelbach, para alocação de potência entre Alice e o *relay*. A alocação de potência é utilizada visando maximizar a eficiência energética segura, medida em bits seguros/J/Hz, ou o *throughput* seguro, medido em bits seguros/s/Hz. Em relação aos protocolos, consideramos o caso onde Alice tem conhecimento perfeito do estado instantâneo do canal apenas em relação aos usuários legítimos. Desta forma, empregamos o protocolo *Decode-and-Forward* Seletivo (SDF), que realiza a escolha entre o melhor tipo de comunicação entre Alice e Bob (comunicação direta ou cooperativa) de forma a aumentar a segurança do sistema. Para comparação, consideramos outros esquemas clássicos de cooperação como o *Amplify-and-Forward* (AF), *Decode-and-Forward* Fixo (DF) e o *Cooperative Jamming* (CJ). Nossos resultados demostram que o SDF supera o AF, o DF e o CJ em grande parte das situações. Contudo, quando a taxa de transmissão aumenta ou quando Eve está muito próxima aos nós legítimos, o CJ apresenta um melhor desempenho.

Palavras-chave: Segurança na Camada Física, Eficiência Energética, Comunicação Cooperativa, Alocação de Potência, Algoritmo Dinkelbach.

ABSTRACT

Farhat, Jamil. SECURE ENERGY EFFICIENCY AND THROUGHPUT IN SELECTIVE DECODE-AND-FORWARD WITH DISTRIBUTED POWER ALLOCATION. 47 f. Dissertação – Programa de Pós-graduação em Engenharia Elétrica e Informática Industrial, Universidade Tecnológica Federal do Paraná. Curitiba, 2015.

We investigate the secure energy efficiency and throughput in cooperative wireless communications systems, in which a pair of legitimate users (Alice and Bob) are assisted by a relay node and the communication occurs in the presence of a passive eavesdropper (Eve). Several cooperative protocols are compared with respect to these measures and we use an iterative and distributed algorithm, based on Dinkelbach algorithm, to allocate power between Alice and the relay. The power allocation is performed in order to increase the secure energy efficiency, measured in secure bits/J/Hz, or secure throughput, measured in secure bits/s/Hz. About the protocols, we consider the case where Alice has perfect knowledge only about the instantaneous channel state of the legitimate channel. So, we employ a Selective Decode-and-Forward (SDF) protocol, which chooses the best type of communication between Alice and Bob (direct or cooperative communication) in order to improve security. For comparison, we consider other classical cooperative schemes such as the Amplify-and-Forward (AF), the Fixed Decode-and-Forward (DF) and the Cooperative Jamming (CJ). Our results show that SDF outperforms AF, DF and CJ in most situations. However, when the transmit rate increases or when Eve is close to the legitimate nodes, CJ has a better performance.

Keywords: Physical Layer Security, Energy Efficiency, Cooperative Communication, Power Allocation, Dinkelbach Algorithm.

LISTA DE FIGURAS

LISTA DE SIGLAS

AF	do inglês, *Amplify-and-Forward*
AWGN	do inglês, *Additive White Gaussian Noise*
CJ	do inglês, *Cooperative Jamming*
CSI	do inglês, *Channel State Information*
DF	*Decode-and-Forward* Fixo, do inglês *Fixed Decode-and-Forward*
MIMO	do inglês, *Multiple Input Multiple Output*
MRC	do inglês, *Maximal Ratio Combining*
NLOS	do inglês, *Non Line-of-Sight*
PDF	do inglês, *Probability Density Function*
SDF	*Decode-and-Forward* Seletivo, do inglês *Selective Decode-and-Forward*
SNR	do inglês, *Signal-to-Noise Ratio*

LISTA DE SÍMBOLOS

κ_{ij}	Perda de percurso entre os nós i e j
P_i	Potência de transmissão
$\mathbf{x}_i$	Vetor de dados transmitido
$\mathbf{w}_{ij}$	Ruído aditivo Gaussiano branco
N_0	Densidade espectral de potência unilateral do ruído térmico
h_{ij}	Coeficiente de desvanecimento no enlace i-j
G	Ganho total das antenas de transmissão e recepção
λ	Comprimento de onda
f_c	Frequência de portadora
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
$\overline{\gamma}_{ij}$	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
$\mathscr{R}_s$	Taxa de *secrecy*
$\mathscr{R}_e$	Taxa de equívoco
τ	*Throughput* seguro
η	Eficiência energética segura
P_{TX}	Potência gasta no circuito de transmissão
P_{RX}	Potência gasta no circuito de recepção
P_{DAC}	Potência consumida pelo conversor digital-analógico
P_{mix}	Potência consumida pelo *mixer*
$P_{\mathrm{filter_{TX}}}$	Potência consumida pelos filtros de transmissão
P_{sync}	Potência consumida pelo sintetizador de frequência
P_{LNA}	Potência consumida pelo amplificador de baixo ruído
P_{IFA}	Potência consumida pelo amplificador intermediário de potência
$P_{\mathrm{filter_{RX}}}$	Potência consumida pelos filtros de recepção
P_{ADC}	Potência consumida pelo conversor analógico-digital
$\mathscr{P}_{\mathrm{Total}}$	Potência total

SUMÁRIO

1 INTRODUÇÃO

A crescente demanda por sistemas de comunicações sem fio tornou a segurança da informação transmitida um item fundamental no desenvolvimento destes sistemas. A comunicação segura foi abordada primeiramente por Shannon em (SHANNON, 1949), na qual a transmissão da mensagem entre um par de usuários legítimos deve evitar a decodificação por parte de uma eventual escuta. Recorrendo à nomenclatura usual no contexto de segurança, neste trabalho iremos denominar o par de usuários legítimos por Alice e Bob, com os respectivos papéis de transmissor e receptor, que se comunicam na presença de Eve, que é uma escuta passiva, ou seja, que apenas tenta obter algum tipo de informação da rede sem tentar interferir na transmissão entre Alice e Bob. A segurança na transmissão da informação recebeu um renovado interesse com o decorrer dos anos e, atualmente, é possível encontrar na literatura dois métodos principais para obtenção da segurança: a criptografia e a segurança na camada física. Estas abordagens não são mutuamente exclusivas e podem ser combinadas para aumentar a segurança já que são implementadas em diferentes camadas da rede. A criptografia utiliza pesadas operações matemáticas para proporcionar segurança à informação transmitida (BLOCH; BARROS, 2011). Desta forma, a confidencialidade da informação transmitida está limitada à capacidade computacional de Eve. Já a segurança na camada física, que será avaliada neste trabalho, utiliza a aleatoriedade da canal sem fio, baseada na flutuação da potência instantânea recebida, para transmitir a informação de maneira segura. Desta forma, 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).

O princípio básico sobre a segurança na camada física foi introduzido por (WYNER, 1975) com o modelo do canal de escuta (do inglês, *wiretap channel*), no qual é considerado que Eve recebe uma versão degradada da informação transmitida entre os pares legítimos, Alice e Bob, o que acaba tornando a comunicação segura possível. Uma grandeza fundamental para determinação da confidencialidade destes sistemas é a capacidade de confidencialidade (do inglês, *secrecy capacity*), que representa a máxima taxa a qual a escuta não pode decodificar nenhuma informação transmitida entre os nós legítimos. A quantificação da confidencialidade

da transmissão da informação está relacionada ao nível de disponibilidade da informação do estado do canal (CSI, do inglês *channel state information*). Considerando conhecimento global da CSI disponível a Alice, a confidencialidade perfeita é obtida adaptando a taxa de equívoco da informação em relação a Eve, 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*). Este cenário, contudo, apresenta a forte suposição que a CSI do canal de Eve também está disponível. Outro cenário possível está relacionado a suposição que a CSI dos canais legítimos são conhecidas e a CSI do canal de Eve é desconhecida, desta forma não é possível definir diretamente a capacidade de confidencialidade do sistema. Neste caso é necessário realizar uma análise probabilística da confidencialidade da informação, definindo a probabilidade de que a taxa de confidencialidade escolhida seja maior que a capacidade de confidencialidade do sistema. Esta análise é denominada como probabilidade de *outage* de segurança (do inglês, *secrecy outage probability*). Além destes, também pode ser considerado um terceiro cenário, no qual Alice não tem conhecimento da CSI de canal algum. Desta forma, além de realizar a análise probabilística da informação estar disponível à Eve, também é necessário determinar a probabilidade de ocorrer uma transmissão confiável entre Alice e Bob. Portanto, a probabilidade de *outage* de segurança torna-se a união de dois eventos independentes: Bob não decodificar a mensagem transmitida e a capacidade instantânea do canal de Eve estar acima da taxa de equívoco do código de escuta em uso. Este cenário sem CSI é considerado, por exemplo, em (TANG et al., 2009; BRANTE et al., 2015a; 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. 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. Alguns protocolos cooperativos clássicos, como o *Amplify-and-Forward* (AF) e o *Decode-and-Forward* Fixo (DF) são 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.

Em relação à confidencialidade em comunicações cooperativas, um estudo inicial é apresentado em (LAI; GAMAL, 2008), no qual o canal de escuta e o canal *relay* são generalizados, de forma que a comunicação entre Alice e Bob tem auxílio do *relay* e ocorre na presença

de Eve. Naquele trabalho, limites para taxa de equívoco de diversas estratégias cooperativas são derivadas, em particular, para a estratégia de encaminhamento de ruído, na qual o *relay* envia palavras-código independentes de Alice com o propósito de confundir Eve. Em (DONG et al., 2010), o cenário cooperativo é investigado na presença de múltiplas Eves, tendo como conclusão que a comunicação cooperativa pode melhorar significativamente a segurança. Sob o ponto de vista de probabilidade de *outage* de segurança, que caracteriza a probabilidade da informação estar disponível a Eve, em (GABRY et al., 2011a) são investigados diferentes protocolos cooperativos para diferentes cenários e configurações da posição de Eve. Esquemas cooperativos tais como AF, DF e *Cooperative Jamming* (CJ) são comparados e os resultados concluem que o AF supera todos os outros esquemas cooperativos em termos de probabilidade de *outage* de segurança, exceto quando Eve está muito próxima ao *relay*, sendo que neste caso o CJ apresenta um melhor desempenho.

Quando utiliza-se a comunicação cooperativa, uma escolha que pode ser realizada para melhorar o desempenho do sistema é quanto à potência alocada em Alice e no *relay*. A alocação de potência consiste na escolha da potência ótima que permite maximizar uma função de interesse. Sobre alocação de potência, uma extensão de (GABRY et al., 2011a) é dada em (GABRY et al., 2011b), que considera um esquema ótimo de alocação com o intuito de minimizar a probabilidade de *outage* de segurança dos esquemas DF e CJ. No entanto, o esquema proposto é bastante complexo, já que é realizada uma busca exaustiva para obter os valores ótimos de potência.

Com o intuito de realizar alocação de potência, um método possível de ser utilizado é o algoritmo Dinkelbach, que apresenta uma busca distribuída e iterativa. Este algoritmo foi desenvolvido para otimização de razões entre funções de mesma variável (DINKELBACH, 1967; ISHEDEN et al., 2012), como é o caso da eficiência energética segura e do *throughput* seguro que serão empregados neste trabalho. O algoritmo Dinkelbach é utilizado, por exemplo, em (BRANTE et al., 2013) para melhorar a eficiência energética de esquemas MIMO cooperativos, com múltiplas antenas no transmissor e receptor. Naquele trabalho, a conclusão foi que o esquema com este algoritmo apresenta um desempenho muito similar ao método de busca exaustiva de alocação de potência. Recentemente, os autores em (WANG et al., 2015a) analisam um cenário com múltiplos *relays* sob a perspectiva da eficiência energética segura, que é definida pela razão entre a taxa de confidencialidade e a potência total, medida em bits seguros/J/Hz. No esquema proposto por estes autores, Alice realiza radiodifusão no primeiro intervalo de tempo, enquanto um subconjunto de *relays* decodificam a mensagem e retransmitem utilizando um *beamforming* distribuído no segundo intervalo. O algoritmo Dinkelbach é utilizado para alocação de potência em Alice e no subconjunto dos *relays*, contudo, apenas o

esquema DF é considerado na análise.

1.1 OBJETIVOS

Este trabalho tem como objetivo realizar uma investigação sobre o *throughput* seguro e a eficiência energética segura em um sistema cooperativo com a presença de dois usuários legítimos, Alice e Bob, comunicando-se com auxílio de um nó *relay*, na presença de um espião passivo. Para realização da alocação de potência visando otimização dos protocolos, diferentemente de (GABRY et al., 2011b), estamos interessados em um cenário com baixa complexidade, no qual a alocação de potência pode ser realizada de uma maneira iterativa e distribuída. Além disto, nosso objetivo é maximizar o sistema com relação ao *throughput* seguro, medido em bits seguros/s/Hz, ou com relação à eficiência energética segura, medida em bits seguros/J/Hz.

Diferentemente de (WANG et al., 2015a), diversos protocolos cooperativos são comparados em termos de eficiência energética segura e *throughput* seguro. Além do mais, estamos particularmente interessados no caso onde Alice tem CSI perfeito apenas do canal legítimo. Como temos conhecimento do canal legítimo, empregamos o protocolo *Decode-and-Forward* Seletivo (SDF), que realiza a escolha pelo melhor tipo de comunicação entre Alice e Bob (comunicação direta ou cooperativa) de forma a aumentar a segurança do sistema. Em outras palavras, como Alice tem CSI do canal legítimo, é possível escolher (e informar ao *relay*), se a cooperação deve ocorrer ou não, o que implica em um impacto positivo no aumento do *throughput* seguro e redução do consumo de potência, consequentemente, aumentando a eficiência energética segura. Nossos resultados demostram que o SDF supera os protocolos AF, DF e CJ em grande parte das situações nas duas métricas citadas anteriormente, exceto quando a taxa de transmissão é grande ou quando Eve está muito próxima aos nós legítimos, quando CJ se destaca.

1.2 ESTRUTURA DO DOCUMENTO

O restante do documento está organizado da seguinte forma. O Capítulo 2 apresentará uma fundamentação teórica de diversos conceitos relacionados à comunicação cooperativa e à confidencialidade na camada física. No Capítulo 3 serão apresentadas as equações relacionadas à probabilidade de *outage* de segurança, à eficiência energética segura e ao *throughput* seguro de cada esquema cooperativo. Além disto, serão demonstrados os métodos de alocação de potência utilizados, dentre eles o algoritmo Dinkelbach. Já o Capítulo 4 apresentará os resultados numéricos e, por fim, o Capítulo 5 concluirá o documento com comentários e considerações

finais.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo apresentamos os conceitos básicos relacionados à transmissão digital no canal sem fio, à confidencialidade e aos protocolos de comunicação cooperativa. O objetivo principal é abordar de maneira sucinta os fundamentos que serão empregados no Capítulo 3. O modelo de sistema relacionado ao canal sem fio é apresentado na Seção 2.1. Já na Seção 2.2 são apresentados os conceitos relacionados à confidencialidade da informação transmitida e medidas que visam quantificar a confidencialidade do sistema. Finalmente, os protocolos de comunicação cooperativa e as análises das capacidades de cada protocolo são apresentados na Seção 2.3.

2.1 TRANSMISSÃO DIGITAL NO CANAL SEM FIO

Consideraremos três usuários legítimos: Alice (A), *relay* (R) e Bob (B) se comunicando na presença de uma escuta, Eve (E). O bloco de informação recebido por qualquer 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

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

onde κ_{ij} representa a perda de percurso entre i e j, P_i é a potência de transmissão e $\mathbf{x}_i$ é o bloco de dados transmitido com energia unitária. Além disto, $\mathbf{w}_{ij}$ é a variável de 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 o ganho do canal, cujo envelope do sinal recebido, $|h_{ij}|^2$, é descrito estatisticamente por uma função densidade de probabilidade (PDF do inglês, *Probability Density Function*) Rayleigh com média nula e variância unitária.

A perda de percurso entre dois nós i e j, de acordo com (GOLDSMITH, 2005), pode ser representada por

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

onde G é o ganho total das antenas transmissoras e receptoras, λ é o comprimento de onda,

definido como $\lambda = \frac{3\times10^8}{f_c}$, f_c é a frequência de portadora, 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.

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 escrita como

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

onde $\overline{\gamma}_{ij} = \frac{\kappa_{ij} P}{N}$ 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.

O modelo utilizado para descrever o comportamento da variável aleatória que representa o módulo do desvanecimento do canal sem fio neste documento é a distribuição de Rayleigh. Esta distribuição representa sistemas em que não há linha de visada (NLOS, do inglês *Non Line-of-Sight*) entre os nós de transmissão e recepção. Portanto, 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:

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

2.2 CONFIDENCIALIDADE NA CAMADA FÍSICA

A confidencialidade refere-se à capacidade de um canal permitir a transmissão de informações de Alice até Bob sem que esta informação seja decodificada por Eve. O princípio básico sobre a segurança da informação na camada física foi introduzido em (WYNER, 1975), a partir do modelo do canal de escuta, representado na Figura 1.

A partir desta figura, vemos que Alice codifica a mensagem w em um bloco de dados de transmissão x_{A}, que é enviado através de um canal com ruído. Desta forma, Eve observa uma versão ruidosa, determinada por y_{AE}, do sinal y_{AB} disponível a Bob. Aqui duas medidas podem ser caracterizadas: a confidencialidade e a confiabilidade. A confidencialidade caracteriza o nível de confusão de Eve sobre a mensagem w, dada a observação do sinal y_{AE}. Já a confiabilidade está relacionada a probabilidade da mensagem decodificada pelo Bob, $\hat{w}$, ser diferente da mensagem original w.

Uma grandeza fundamental para determinação da confidencialidade de um canal é a

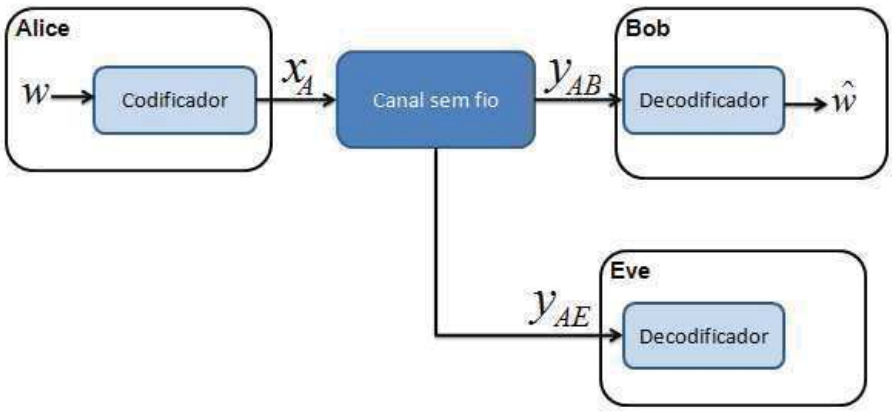


Figura 1: Representação do modelo do canal de escuta.

Fonte: Autoria Própria

capacidade de confidencialidade. Esta medida determina a máxima taxa a partir da qual Eve não pode decodificar nenhuma informação transmitida por Alice, além de garantir uma transmissão confiável entre Alice e Bob. A capacidade de confidencialidade, C_s, é determinada pela diferença entre as capacidades do canal legítimo, C_L, e do canal da escuta, C_E. Assim, conforme (BLOCH; BARROS, 2011; CSISZAR; KORNER, 1978), a capacidade de confidencialidade é dada por

$$C_s = C_L - C_E. \tag{5}$$

As capacidades C_L e C_E podem ser definidas, a partir de (SHANNON, 1948), considerando canais Gaussianos, por

$$\begin{aligned} C_L &= B \cdot \log_2(1+\gamma_L) \\ C_E &= B \cdot \log_2(1+\gamma_E) \end{aligned} \tag{6}$$

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

Considerando canais AWGN, em (LEUNG-YAN-CHEONG; HELLMAN, 1978) é mostrado que a confidencialidade nestes canais apenas é possível se a capacidade do canal legítimo for maior que a capacidade do canal espião. Recentemente, (BARROS; RODRIGUES, 2006) renovaram o interesse na confidencialidade de sistemas sem fio considerando canais com desvanecimentos quase-estáticos. Nestes sistemas conclui-se que comunicações perfeitamente seguras são possíveis mesmo que Eve tenha uma SNR média maior que Bob. Isto ocorre pois, devido ao desvanecimento do canal, existe uma probabilidade, mesmo que pequena, da SNR

instantânea do canal legítimo ser superior à SNR instantânea do canal da escuta, de modo que uma comunicação segura ainda é possível em algumas ocasiões.

A capacidade de confidencialidade está relacionada com o conhecimento global da CSI. Se assumimos que o comportamento dos canais legítimo e da 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 seria dada por $\mathscr{R}_s = C_L - C_E$, de modo que seria possível atingir a confidencialidade perfeita apenas adaptando a taxa do código de escuta (BLOCH et al., 2008). Caso 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 onde $\mathscr{R}$ seja igual à capacidade do canal legítimo, C_L, e $\mathscr{R}_e$ seja uma taxa de equívoco estimada para Eve. A taxa de comunicação segura neste caso seria $\mathscr{R}_s = C_L - \mathscr{R}_e$. Desta forma, um evento de falha é definido como a capacidade do canal de Eve, C_E, exceder a taxa $\mathscr{R}_e$ ou a capacidade de confidencialidade do canal ser menor que a taxa $\mathscr{R}_s$. A probabilidade deste evento é denominada de probabilidade de *outage* de segurança e é definida, em (BLOCH; BARROS, 2011), por

$$P_{\text{out}} = \Pr\{C_s < \mathscr{R}_s\}. \tag{7}$$

Outro caso possível, considerado em (TANG et al., 2007, 2009; BRANTE et al., 2015a), 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 não é conhecida, deve ser escolhida uma taxa $\mathscr{R}$ para o canal legítimo e uma taxa $\mathscr{R}_e$ para o canal de Eve. A taxa de comunicação segura é fixa e dada por $\mathscr{R}_s = \mathscr{R} - \mathscr{R}_e$ e uma falha ocorre quando $\mathscr{R}$ supera C_L ou quando C_E supera $\mathscr{R}_e$. 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 COMUNICAÇÃO COOPERATIVA

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 2, o *relay* auxilia Alice a encaminhar a informação até Bob. Nesta seção apresentaremos alguns protocolos cooperativos clássicos como o AF e o DF. Este último faz uso consistente do *relay*, já que a informação recebida por Alice deverá ser decodificada e o resultado deverá ser encaminhado ao Bob. Além destes, apresentaremos o protocolo CJ, no qual o *relay* não reencaminha a informação de Alice para Bob, ao invés disto, este tenta confundir Eve de modo esta não possa decodificar a informação transmitida por Alice.

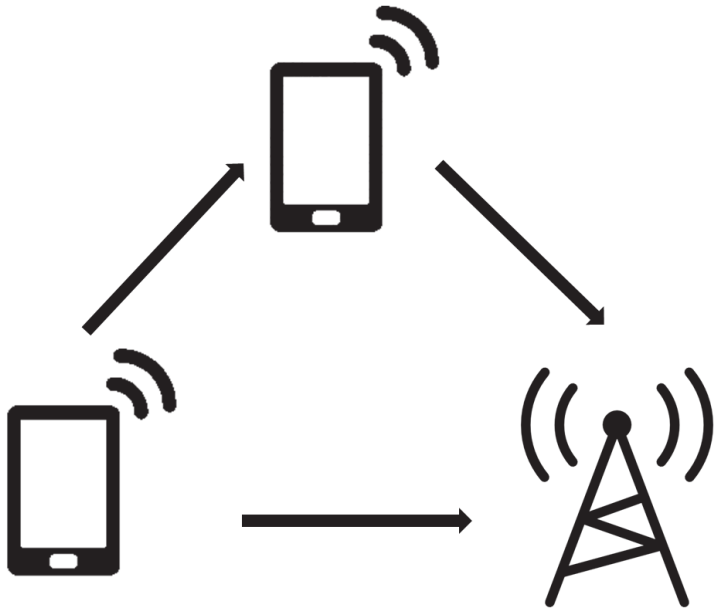


Figura 2: Representação da comunicação cooperativa com o *relay* auxiliando Alice a reencaminhar a informação até Bob.

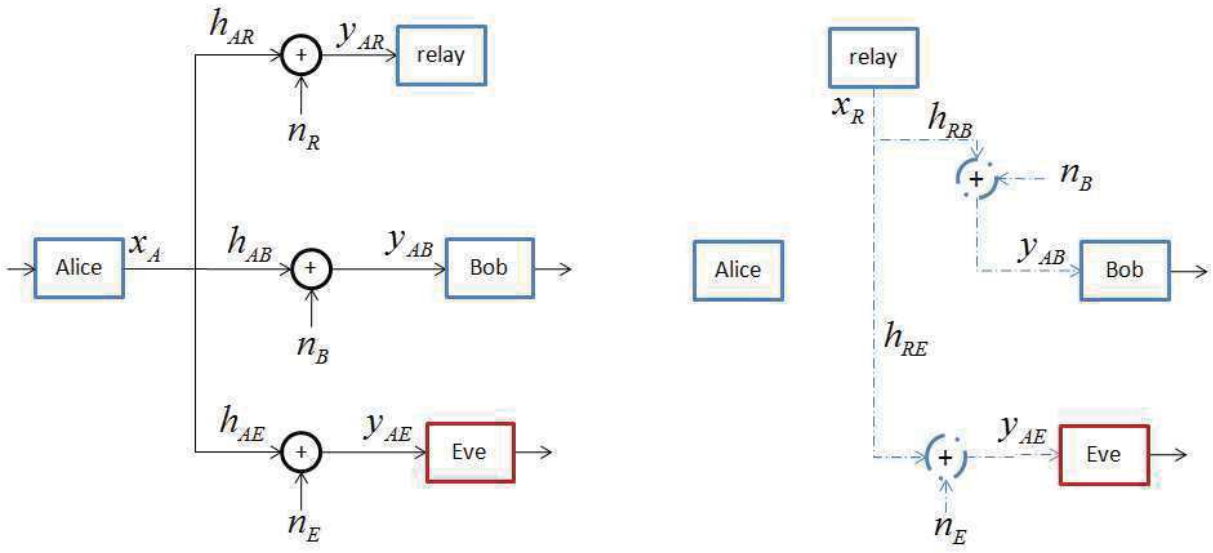
Fonte: Autoria Própria

Considerando CSI do canal legítimo, Alice pode utilizar este conhecimento para decidir sobre a utilização, ou não, da cooperação com o intuito de melhorar a transmissão da informação. Este protocolo será denominado *Decode-and-Forward* Seletivo (SDF) e será apresentado no decorrer deste capítulo com mais detalhes.

Nas próximas subseções serão apresentados estes protocolos cooperativos sob o ponto de vista de segurança. Nesta seção já incluiremos a presença da escuta que tenta decodificar as informações da fonte. 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.

2.3.1 AMPLIFY-AND-FORWARD (AF)

O protocolo AF é o mais simples entre os protocolos de cooperação. Neste esquema, Alice primeiramente envia a informação para Bob e esta informação acaba sendo recebida simultaneamente pelo *relay*. O *relay*, após receber o sinal com os efeitos de atenuação e ruído, aplica um ganho de potência no sinal recebido e reencaminha a informação até Bob. O ganho de potência no sinal recebido é variável e está relacionado com a potência instantânea do sinal recebido, conforme (LANEMAN et al., 2004). A comunicação em cada instante de tempo pode ser verificada na Figura 3, com Alice transmitindo no primeiro intervalo de tempo (Figura 3a) e o *relay* no segundo instante (Figura 3b).



(a) Comunicação no primeiro intervalo de tempo. (b) Comunicação no segundo intervalo de tempo.

Figura 3: Representação dos protocolos cooperativos na presença de Eve.
Fonte: Autoria Própria

Salientamos que neste protocolo cooperativo, e nos próximos que serão apresentados, consideramos que a transmissão é *half-duplex* e ortogonal ao tempo. Além disto, por se tratar do método que proporciona o melhor desempenho, consideramos que Bob combina os sinais recebidos pelos caminhos independentes, Alice-Bob e *relay*-Bob, por combinação por máxima razão (MRC, do inglês *Maximal Ratio Combining*) (GOLDSMITH, 2005).

Desta forma, podemos definir a capacidade do canal legítimo empregando o AF, $C_{\mathrm{L}}^{(\mathrm{AF})}$, e do canal de Eve, $C_{\mathrm{E}}^{(\mathrm{AF})}$, que serão utilizadas no próximo capítulo para definição da probabilidade de *outage* de segurança. Conforme (DONG et al., 2010), as capacidades podem ser

representadas por

$$C_{\mathrm{L}}^{(\mathrm{AF})} = \log_2\left(1+\gamma_{\mathrm{AB}}+\frac{\gamma_{\mathrm{AR}}\,\gamma_{\mathrm{RB}}}{1+\gamma_{\mathrm{AR}}+\gamma_{\mathrm{RB}}}\right) \tag{8}$$

e

$$C_{\mathrm{E}}^{(\mathrm{AF})} = \log_2\left(1+\gamma_{\mathrm{AE}}+\frac{\gamma_{\mathrm{AR}}\,\gamma_{\mathrm{RE}}}{1+\gamma_{\mathrm{AR}}+\gamma_{\mathrm{RE}}}\right). \tag{9}$$

2.3.2 DECODE-AND-FORWARD FIXO (DF)

No protocolo DF, semelhantemente ao AF, a transmissão ocorre por Alice no primeiro intervalo de tempo e pelo *relay* no segundo instante, conforme Figuras 3a e 3b, respectivamente. A principal diferença é que no DF o sinal é decodificado pelo *relay* enquanto no AF o sinal é apenas amplificado. Portanto, no segundo intervalo de tempo, o *relay* realiza uma decisão sobre a informação recebida por Alice, com o intuito de tentar anular os efeitos de ruído e atenuação do canal, para que possa, no segundo intervalo, reencaminhar a informação a Bob. Em relação a este esquema, conforme (DONG et al., 2010), as capacidades dos canais legítimo e de Eve podem ser representadas por

$$C_{\mathrm{L}}^{(\mathrm{DF})} = \min\left(\log_2(1+\gamma_{\mathrm{AR}}), \log_2(1+\gamma_{\mathrm{AB}}+\gamma_{\mathrm{RB}})\right) \tag{10}$$

e

$$C_{\mathrm{E}}^{(\mathrm{DF})} = \log_2\left(1+\gamma_{\mathrm{AE}}+\gamma_{\mathrm{RE}}\right). \tag{11}$$

2.3.3 COOPERATIVE JAMMING (CJ)

O protocolo CJ está associado à noção de confidencialidade na transmissão de informações. Neste esquema, ao invés de retransmitir a informação recebida por Alice, o *relay* cria uma interferência enquanto Alice está transmitindo sua informação de modo a confundir Eve, conforme é mostrado na Figura 4. Nesta figura, a linha contínua representa a transmissão de informação entre Alice e Bob e a linha tracejada representa a transmissão do ruído pelo *relay*. Pode-se notar que ambas transmissões ocorrem simultaneamente e interferem tanto em Bob quanto em Eve. Para esta estratégia consideramos que o *relay* transmite ruído Gaussiano, n_R. Pelo fato desta estratégia não utilizar dois intervalos de tempo para transmissão, consideraremos que Alice encaminhará a informação a uma taxa de transmissão $\mathscr{R}_s$ de modo que seja possível efetuar uma comparação justa com os outros esquemas de cooperação.

Neste método, temos que as capacidades dos canais legítimo e da escuta, conforme (VI-

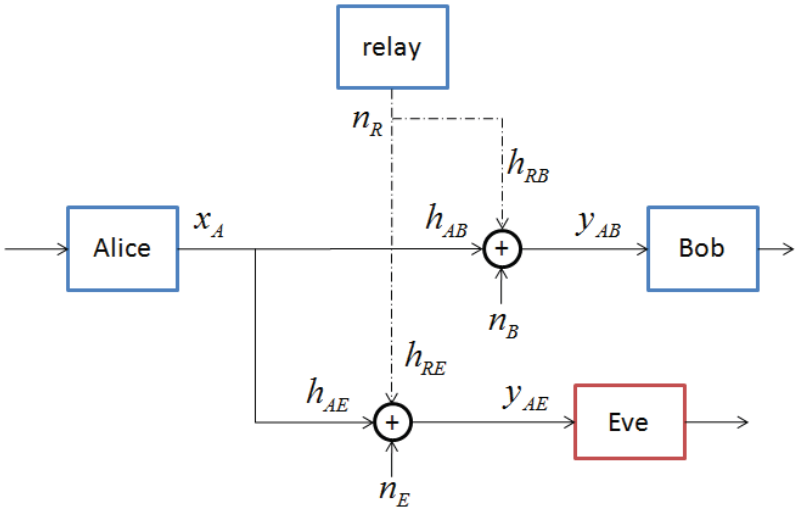


Figura 4: Representação do protocolo *Cooperative Jamming*.

Fonte: Autoria Própria

LELA et al., 2011), podem ser representados por

$$C_{\mathrm{L}}^{(\mathrm{CJ})} = \log_2\left(1+\frac{\gamma_{\mathrm{AB}}}{1+\gamma_{\mathrm{RB}}}\right) \tag{12}$$

e

$$C_{\mathrm{E}}^{(\mathrm{CJ})} = \log_2\left(1+\frac{\gamma_{\mathrm{AE}}}{1+\gamma_{\mathrm{RE}}}\right). \tag{13}$$

2.3.4 DECODE-AND-FORWARD SELETIVO (SDF)

No esquema de transmissão SDF, como estamos considerando CSI completa do canal legítimo, Alice realiza uma decisão sobre a utilização ou não da cooperação, informando o *relay* sobre sua participação. Assim, Alice envia sua informação no primeiro instante de tempo por radiodifusão e, caso a cooperação não tenha um desempenho melhor que a transmissão direta, a própria Alice retransmite sua informação no segundo intervalo de tempo. Caso contrário, o *relay* participa da comunicação, realiza uma decodificação com o intuito de tentar anular os efeitos de ruído e atenuação do canal, e reencaminha a informação para Bob durante o segundo intervalo. A possibilidade desta escolha por Alice implica em uma vantagem deste protocolo em relação ao DF, já que a taxa de transmissão não precisa sempre ser suportada pelo canal Alice-*relay*.

Dessa forma, Alice faz uma escolha entre a transmissão direta ou cooperativa, escolhendo a capacidade do canal legítimo mais vantajosa, podendo esta ser a direta, dada por $C_{\mathrm{L_{dir}}}$,

ou cooperativa, representada por $C_{\mathrm{L_{coop}}}$. Desta forma, as capacidades podem ser representadas por

$$C_{\mathrm{L}}^{(\mathrm{SDF})} = \max\left\{C_{\mathrm{L_{dir}}}, C_{\mathrm{L_{coop}}}\right\}. \tag{14}$$

Assim, quando ocorre apenas a transmissão direta com retransmissão por parte de Alice, temos

$$C_{\mathrm{L_{dir}}}^{(\mathrm{SDF})} = \log_2(1+2\,\gamma_{\mathrm{AB}}) \tag{15}$$

e

$$C_{\mathrm{E_{dir}}}^{(\mathrm{SDF})} = \log_2(1+2\,\gamma_{\mathrm{AE}}). \tag{16}$$

Já para o caso cooperativo, consideraremos que as capacidades são calculadas por

$$C_{\mathrm{L_{coop}}}^{(\mathrm{SDF})} = \min\left\{\log_2\left(1+\gamma_{\mathrm{AR}}\right), \log_2\left(1+\gamma_{\mathrm{AB}}+\gamma_{\mathrm{RB}}\right)\right\} \tag{17}$$

e

$$C_{\mathrm{E_{coop}}}^{(\mathrm{SDF})} = \log_2(1+\gamma_{\mathrm{AE}}+\gamma_{\mathrm{RE}}). \tag{18}$$

Em relação a capacidade de Eve para o caso cooperativo consideramos uma aproximação pessimista para simplificar as equações, na qual Eve sempre receberá as informações retransmitidas pelo *relay*.

A partir do conhecimento das capacidades dos canais dos diferentes esquemas cooperativos é possível realizar o cálculo da probabilidade de *outage* de segurança. Este cálculo será apresentado com mais detalhes no próximo capítulo.

3 ESQUEMAS DE TRANSMISSÃO COOPERATIVOS COM ALOCAÇÃO DE POTÊNCIA

Neste capítulo derivamos a equação fechada para a probabilidade de *outage* de segurança do esquema SDF e apresentamos as expressões já existentes para os esquemas DF, AF e CJ para efeito de comparação. Conforme citado anteriormente, utilizamos a abordagem probabilística para o cálculo da confidencialidade já que a falta de conhecimento do comportamento do canal de Eve impede que possamos atingir confidencialidade perfeita. Também definimos, na Seção 3.5, as equações de *throughput* seguro e eficiência energética segura para cada esquema cooperativo.

Além disso, na Seção 3.6 apresentamos os esquemas de alocação de potência utilizados para maximização do *throughput* seguro e eficiência energética segura. A alocação de potência neste trabalho consiste na escolha de potência em Alice e no *relay* que permitem maximizar as variáveis desejadas. Em especial, na subseção 3.6.3, apresentamos uma fundamentação teórica do algoritmo Dinkelbach.

3.1 DECODE-AND-FORWARD SELETIVO

Para o cálculo da probabilidade de *outage* de segurança deste esquema iremos utilizar a equação (7), que representa a probabilidade de que uma determinada taxa de confidencialidade escolhida seja superior à capacidade de confidencialidade do sistema. Para cálculo da capacidade de confidencialidade será necessário utilizar as capacidades dos canais legítimos e da escuta, representadas por (15) e (16) quando ocorre apenas a transmissão direta, ou por (17) e (18) quando a transmissão é cooperativa.

Pelo fato de considerarmos dois intervalos de tempo para transmissão da informação entre Alice e Bob, utilizamos uma taxa de confidencialidade igual a $2\mathscr{R}_s$ para cálculo da probabilidade de *outage* de segurança, a fim de se realizar uma comparação justa com a transmissão direta.

A solução exata deste esquema, a partir da relação mostrada em (14), é equivalente a

resolver o seguinte sistema

$$\begin{aligned} p_{\text{out}}^{(\text{SDF})} = &\Pr\left\{C_{\text{L}_{\text{dir}}}^{(\text{SDF})} - C_{\text{E}_{\text{dir}}}^{(\text{SDF})} < 2\mathscr{R}_s \bigcap C_{\text{L}_{\text{dir}}} \geq C_{\text{L}_{\text{coop}}}\right\} \\ &+ \Pr\left\{C_{\text{L}_{\text{coop}}}^{(\text{SDF})} - C_{\text{E}_{\text{coop}}}^{(\text{SDF})} < 2\mathscr{R}_s \bigcap C_{\text{L}_{\text{coop}}} > C_{\text{L}_{\text{dir}}}\right\}. \end{aligned} \tag{19}$$

Porém esta resolução matemática torna-se bastante complicada devido ao termo $C_{\text{L}_{\text{coop}}}$, que relaciona o mínimo entre duas variáveis aleatórias. Desta forma, como usualmente o *relay* está localizado em uma posição intermediária entre Alice e Bob, utilizaremos uma aproximação ao considerar que a transmissão direta, dada por p_{dir}, ocorre sempre que $\gamma_{\text{AB}} \geq \gamma_{\text{AR}}$ ao passo que a cooperação, representada por p_{coop}, ocorre somente quando $\gamma_{\text{AB}} < \gamma_{\text{AR}}$, de forma que a probabilidade de *outage* de segurança se torna

$$\begin{aligned} p_{\text{out}}^{(\text{SDF})} \simeq &\overbrace{\Pr\left\{C_{\text{L}_{\text{dir}}}^{(\text{SDF})} - C_{\text{E}_{\text{dir}}}^{(\text{SDF})} < 2\mathscr{R}_s \bigcap \gamma_{\text{AB}} \geq \gamma_{\text{AR}}\right\}}^{p_{\text{dir}}} \\ &\underbrace{+ \Pr\left\{C_{\text{L}_{\text{coop}}}^{(\text{SDF})} - C_{\text{E}_{\text{coop}}}^{(\text{SDF})} < 2\mathscr{R}_s \bigcap \gamma_{\text{AR}} > \gamma_{\text{AB}}\right\}}_{p_{\text{coop}}}. \end{aligned} \tag{20}$$

Primeiramente calculamos a probabilidade de *outage* de segurança considerando o caso mais simples, no qual a transmissão é feita totalmente por Alice. Neste caso p_{dir} é dado por

$$\begin{aligned} p_{\text{dir}} &= \Pr\left\{\log_2(1+2\,\gamma_{\text{AB}}) - \log_2(1+2\,\gamma_{\text{AE}}) < 2\mathscr{R}_s \bigcap \gamma_{\text{AB}} \geq \gamma_{\text{AR}}\right\} \\ &= \Pr\left\{\left(\frac{1+2\,\gamma_{\text{AB}}}{1+2\,\gamma_{\text{AE}}}\right) < 2^{2\mathscr{R}_s} \bigcap \gamma_{\text{AB}} \geq \gamma_{\text{AR}}\right\} \\ &= \Pr\left\{\gamma_{\text{AE}} > \frac{(2^{-2\mathscr{R}_s}(1+2\,\gamma_{\text{AB}}) - 1)}{2} \bigcap \gamma_{\text{AB}} \geq \gamma_{\text{AR}}\right\}. \end{aligned} \tag{21}$$

Considerando que $f_{\gamma_{\text{AB}}}(\gamma_{\text{AB}})$, $f_{\gamma_{\text{AE}}}(\gamma_{\text{AE}})$ e $f_{\gamma_{\text{AR}}}(\gamma_{\text{AR}})$ são PDFs de variáveis aleatórias que seguem a distribuição exponencial, a probabilidade p_{dir}, utilizando os limites da relação entre γ_{AB}, γ_{AE} e γ_{AR} obtidos a partir de (21), pode ser representada por

$$p_{\text{dir}} = \int_0^{\infty} \int_0^{\gamma_{\text{AB}}} \int_{\frac{2^{-2\mathscr{R}_s}(1+2\gamma_{\text{AB}})-1}{2}}^{\infty} f_{\gamma_{\text{AB}}} f_{\gamma_{\text{AR}}} f_{\gamma_{\text{AE}}} \, \text{d}\gamma_{\text{AE}} \text{d}\gamma_{\text{AR}} \text{d}\gamma_{\text{AB}}, \tag{22}$$

onde

$$f_{\gamma_{\text{A}j}}(\gamma_{\text{A}j}) = \frac{1}{\overline{\gamma}_{\text{A}j}} e^{-\frac{\gamma_{\text{A}j}}{\overline{\gamma}_{\text{A}j}}}, \tag{23}$$

com $j \in \{\mathrm{B},\mathrm{R},\mathrm{E}\}$. Resolvendo a integral, chegamos a

$$p_{\mathrm{dir}} = \frac{2^{4\mathscr{R}_\mathrm{s}}\overline{\gamma}_{\mathrm{AB}}\overline{\gamma}_{\mathrm{AE}}{}^2 e^{\frac{2^{-(2\mathscr{R}_\mathrm{s}+1)}(2^{2\mathscr{R}_\mathrm{s}}-1)}{\overline{\gamma}_{\mathrm{AE}}}}}{(\overline{\gamma}_{\mathrm{AB}}+2^{2\mathscr{R}_\mathrm{s}}\overline{\gamma}_{\mathrm{AE}})(\overline{\gamma}_{\mathrm{AB}}\overline{\gamma}_{\mathrm{AR}}+2^{2\mathscr{R}_\mathrm{s}}\overline{\gamma}_{\mathrm{AE}}(\overline{\gamma}_{\mathrm{AB}}+\overline{\gamma}_{\mathrm{AR}}))}. \tag{24}$$

Já para a transmissão cooperativa, denominada anteriormente como p_{coop}, temos que a SNR equivalente dos canais legítimos e da escuta são representados por γ_B e γ_E, onde $\gamma_B = \gamma_{\mathrm{AB}} + \gamma_{\mathrm{RB}}$ e $\gamma_E = \gamma_{\mathrm{AE}} + \gamma_{\mathrm{RE}}$. A soma de duas variáveis aleatórias exponenciais pode ser calculada pelo teorema da convolução. Conforme (PAPOULIS, 1991), considerando γ_1 e γ_2 duas variáveis aleatórias exponenciais identicamente distribuídas com médias μ_1 e μ_2, temos que a PDF resultante da soma destas variáveis é dada pela convolução das PDF individuais. Assim,

$$g_\mu(\mu) = \frac{1}{\mu_1\mu_2}\int_0^\mu e^{-\frac{x}{\mu_1}} e^{-\frac{(\mu-x)}{\mu_2}}\,\mathrm{d}x = \frac{1}{\mu_1-\mu_2}\left(e^{-\frac{\mu}{\mu_1}} - e^{-\frac{\mu}{\mu_2}}\right). \tag{25}$$

De forma que a soma das variáveis aleatórias é representada por

$$g_{\gamma_k}(\gamma_k) = \frac{1}{\overline{\gamma}_{\mathrm{R}k}-\overline{\gamma}_{\mathrm{A}k}}\left(e^{-\frac{\gamma_k}{\overline{\gamma}_{\mathrm{R}k}}} - e^{-\frac{\gamma_k}{\overline{\gamma}_{\mathrm{A}k}}}\right), \tag{26}$$

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

Considerando os mesmos passos utilizados para cálculo da probabilidade do caso direto, temos que a probabilidade do caso cooperativo é dada por

$$\begin{aligned} p_{\mathrm{coop}} = {} & \overbrace{\Pr\left\{\frac{(1+\gamma_{\mathrm{AR}})}{(1+\gamma_{\mathrm{E}})} < 2^{2\mathscr{R}_\mathrm{s}} \bigcap \gamma_{\mathrm{AR}} > \gamma_{\mathrm{AB}} \bigcap \gamma_{\mathrm{AR}} < \gamma_{\mathrm{B}}\right\}}^{p_1} \\ & + \underbrace{\Pr\left\{\frac{(1+\gamma_{\mathrm{B}})}{(1+\gamma_{\mathrm{E}})} < 2^{2\mathscr{R}_\mathrm{s}} \bigcap \gamma_{\mathrm{AR}} > \gamma_{\mathrm{AB}} \bigcap \gamma_{\mathrm{AR}} \geq \gamma_{\mathrm{B}}\right\}}_{p_2}. \end{aligned} \tag{27}$$

Para resolução de p_1, isolamos γ_{E} e consideramos a resolução das integrais a seguir. A solução é dividida em duas partes para facilitar a integração pelos limites dados pelas intersecções. Assim,

$$\begin{aligned} p_1 = {} & \int_0^\infty \int_0^{\gamma_{\mathrm{B}}} \int_{(2^{-2\mathscr{R}_\mathrm{s}}(1+\gamma_{\mathrm{AR}})-1)}^\infty g_{\gamma_{\mathrm{B}}} f_{\gamma_{\mathrm{AR}}} g_{\gamma_{\mathrm{E}}}\,\mathrm{d}\gamma_{\mathrm{E}}\mathrm{d}\gamma_{\mathrm{AR}}\mathrm{d}\gamma_{\mathrm{B}} \\ & - \int_0^\infty \int_0^{\gamma_{\mathrm{AB}}} \int_{(2^{-2\mathscr{R}_\mathrm{s}}(1+\gamma_{\mathrm{AR}})-1)}^\infty f_{\gamma_{\mathrm{AB}}} f_{\gamma_{\mathrm{AR}}} g_{\gamma_{\mathrm{E}}}\,\mathrm{d}\gamma_{\mathrm{E}}\mathrm{d}\gamma_{\mathrm{AR}}\mathrm{d}\gamma_{\mathrm{AB}}. \end{aligned} \tag{28}$$

Para resolução de p_2, ressalta-se que ambas intersecções, $\gamma_{\mathrm{AR}} > \gamma_{\mathrm{AB}}$ e $\gamma_{\mathrm{AR}} \geq \gamma_{\mathrm{B}}$, não

precisam ser consideradas, já que a última intersecção envolve a região da primeira. Desta forma, p_2 é resolvido por

$$p_2 = \int_0^{\infty} \int_{\gamma_B}^{\infty} \int_{(2^{-2\mathscr{R}_s}(1+\gamma_B)-1)}^{\infty} g_{\gamma_B} f_{\gamma_{AR}} g_{\gamma_E} \, \mathrm{d}\gamma_E \mathrm{d}\gamma_{AR} \mathrm{d}\gamma_B. \tag{29}$$

Após a resolução de (28) e (29) e substituição destes termos em (27), obtemos a probabilidade de *outage* de segurança do termo cooperativo, que é dado por

$$p_{\text{coop}} = \frac{2^{4\mathscr{R}_s}\overline{\gamma}_{AR}(\overline{\gamma}_{RB}+\overline{\gamma}_{AR})}{\overline{\gamma}_{RE}-\overline{\gamma}_{AE}} \left(\mathscr{B}(\overline{\gamma}_{RE}) - \mathscr{B}(\overline{\gamma}_{AE})\right), \tag{30}$$

onde

$$\mathscr{B}(x) = \frac{e^{\frac{-(2^{2\mathscr{R}_s}-1)}{x}} x^3 \left(\overline{\gamma}_{AB}\overline{\gamma}_{AR} + 2^{2\mathscr{R}_s} x(\overline{\gamma}_{AB}+\overline{\gamma}_{AR})\right)^{-1}}{(\overline{\gamma}_{RB}\overline{\gamma}_{AR} + 2^{2\mathscr{R}_s} x(\overline{\gamma}_{RB}+\overline{\gamma}_{AR}))}. \tag{31}$$

Finalmente, a probabilidade de *outage* de segurança completa do SDF é obtida a partir da substituição dos termos (24) e (30) em (20), resultando na seguinte expressão final

$$\begin{aligned} p_{\text{out}}^{(\text{SDF})} \simeq & \frac{2^{4\mathscr{R}_s}\overline{\gamma}_{AB}\overline{\gamma}_{AE}{}^2 e^{\frac{2^{-(2\mathscr{R}_s+1)}(2^{2\mathscr{R}_s}-1)}{\overline{\gamma}_{AE}}}}{(\overline{\gamma}_{AB}+2^{2\mathscr{R}_s}\overline{\gamma}_{AE})(\overline{\gamma}_{AB}\overline{\gamma}_{AR}+2^{2\mathscr{R}_s}\overline{\gamma}_{AE}(\overline{\gamma}_{AB}+\overline{\gamma}_{AR}))} \\ & + \frac{2^{4\mathscr{R}_s}\overline{\gamma}_{AR}(\overline{\gamma}_{RB}+\overline{\gamma}_{AR})}{\overline{\gamma}_{RE}-\overline{\gamma}_{AE}} \left(\mathscr{B}(\overline{\gamma}_{RE}) - \mathscr{B}(\overline{\gamma}_{AE})\right). \end{aligned} \tag{32}$$

De forma a validar a expressão obtida, comparamos na Figura 5 a probabilidade de *outage* de segurança do SDF considerando o caso exato, obtido por simulação de Monte Carlo, a partir de (19), e a expressão aproximada dada por (32), a partir da variação da SNR do canal legítimo. Na figura, consideramos três casos para a posição do *relay*, estando este posicionado em $d_{AR} = 0,2\,d_{AB}$, $d_{AR} = 0,5\,d_{AB}$ e $d_{AR} = 0,8\,d_{AB}$. A partir da figura, podemos observar que a simplificação considerada apresenta uma boa aproximação para o caso exato. Além disso, é importante ressaltar que a aproximação é pessimista, ou seja, tem desempenho levemente pior que a curva exata.

3.2 AMPLIFY-AND-FORWARD

Para definir a probabilidade de *outage* de segurança para o esquema AF, é necessário realizar uma aproximação para alta SNR. Esta aproximação é necessária devido a relação das variáveis aleatórias no denominador da expressão da capacidade do canal legítimo, mostrada em (8), que acaba por impedir a resolução direta da equação. Considerando que as SNRs equivalentes em Bob e Eve podem ser aproximadas em alta SNR conforme (LANEMAN et al.,

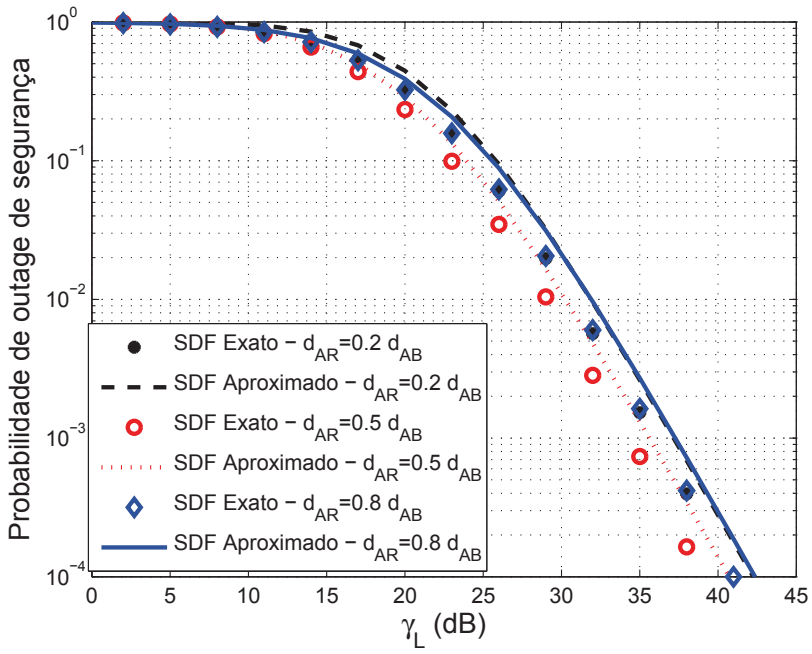


Figura 5: Probabilidade de *outage* de segurança aproximada para o esquema SDF em comparação com a simulação de Monte Carlo para a expressão exata.

Fonte: Autoria Própria

2004)

$$\overline{\gamma}_j \approx \frac{\overline{\gamma}_{\mathrm{AR}} \cdot \overline{\gamma}_{\mathrm{R}j}}{\overline{\gamma}_{\mathrm{AR}} + \overline{\gamma}_{\mathrm{R}j}}, \tag{33}$$

com $j \in \{\mathrm{B}, \mathrm{E}\}$, temos que a probabilidade de *outage* de segurança, encontrada em (GABRY et al., 2013), é definida por

$$p_{\mathrm{out}}^{(\mathrm{AF})} = \frac{\overline{\gamma}_{\mathrm{B}} \left(\mathscr{A}(\overline{\gamma}_{\mathrm{B}}, \overline{\gamma}_{\mathrm{E}}) - \mathscr{A}(\overline{\gamma}_{\mathrm{B}}, \overline{\gamma}_{\mathrm{AE}})\right)}{(\overline{\gamma}_{\mathrm{E}} - \overline{\gamma}_{\mathrm{AE}})(\overline{\gamma}_{\mathrm{B}} - \overline{\gamma}_{\mathrm{AB}})} - \frac{\overline{\gamma}_{\mathrm{AB}} \left(\mathscr{A}(\overline{\gamma}_{\mathrm{AB}}, \overline{\gamma}_{\mathrm{E}}) - \mathscr{A}(\overline{\gamma}_{\mathrm{AB}}, \overline{\gamma}_{\mathrm{AE}})\right)}{(\overline{\gamma}_{\mathrm{E}} - \overline{\gamma}_{\mathrm{AE}})(\overline{\gamma}_{\mathrm{B}} - \overline{\gamma}_{\mathrm{AB}})}, \tag{34}$$

onde $\mathscr{A}(x,y) = \frac{y^2}{2^{-2\mathscr{R}_{\mathrm{s}}} x + y} e^{-\frac{(2^{-2\mathscr{R}_{\mathrm{s}}} - 1)}{y}}$.

3.3 DECODE-AND-FORWARD FIXO

A probabilidade de *outage* de segurança do esquema DF, utilizando as capacidades definidas anteriormente, conforme (GABRY et al., 2011a), pode ser representada por

$$\begin{aligned} p_{\text{out}}^{(\text{DF})} = & \frac{\mathscr{A}(\overline{\gamma}_{\text{AR}},\overline{\gamma}_{\text{RE}}) - \mathscr{A}(\overline{\gamma}_{\text{AR}},\overline{\gamma}_{\text{AE}})}{(\overline{\gamma}_{\text{RE}} - \overline{\gamma}_{\text{AE}})} \\ & + \frac{\overline{\gamma}_{\text{AR}}\,\mathscr{A}(\overline{\gamma}_{\text{AR}},\overline{\gamma}_{\text{AE}})\,[\mathscr{D}(\overline{\gamma}_{\text{AE}},\overline{\gamma}_{\text{AB}}) - \mathscr{D}(\overline{\gamma}_{\text{AE}},\overline{\gamma}_{\text{RB}})]}{2^{2R_{\text{s}}}(\overline{\gamma}_{\text{RE}} - \overline{\gamma}_{\text{AE}})(\overline{\gamma}_{\text{RB}} - \overline{\gamma}_{\text{AB}})} \\ & - \frac{\overline{\gamma}_{\text{AR}}\,\mathscr{A}(\overline{\gamma}_{\text{AR}},\overline{\gamma}_{\text{RE}})\,[\mathscr{D}(\overline{\gamma}_{\text{RE}},\overline{\gamma}_{\text{AB}}) - \mathscr{D}(\overline{\gamma}_{\text{RE}},\overline{\gamma}_{\text{RB}})]}{2^{2R_{\text{s}}}(\overline{\gamma}_{\text{RE}} - \overline{\gamma}_{\text{AE}})(\overline{\gamma}_{\text{RB}} - \overline{\gamma}_{\text{AB}})}, \end{aligned} \tag{36}$$

onde $\mathscr{D}(x,y) \triangleq \frac{y\overline{\gamma}_{\text{AR}}}{x(y+\overline{\gamma}_{\text{AR}})+y\overline{\gamma}_{\text{AR}}\,2^{-2\mathscr{R}_{\text{s}}}}$.

3.4 COOPERATIVE JAMMING

Salientamos que neste esquema consideraremos que Alice está transmitindo a uma taxa $\mathscr{R}_s$ de forma que o mesmo intervalo total de tempo é utilizado em comparação com os demais esquemas cooperativos. Lembramos que no esquema CJ, Alice e *relay* transmitem simultaneamente. Esta consideração possibilita realizar uma comparação justa entre os diversos esquemas cooperativos. Desta forma, temos que a equação de probabilidade de *outage* de segurança, segundo (GABRY et al., 2011a), é definida como

$$p_{\text{out}}^{(\text{CJ})} = 1 + \frac{e^{-b}}{\overline{\gamma}_{\text{RE}}\overline{\gamma}_{\text{RB}}\,ck}\left[\left(1 - \frac{1}{klc}\right)\mathscr{F}(c+ck) + \left(\frac{1}{klc} + \frac{1}{k}\right)\mathscr{F}\left(\frac{1+k}{k\overline{\gamma}_{\text{RE}}}\right) - \overline{\gamma}_{\text{RE}}\right], \tag{37}$$

onde $b \triangleq \frac{2^{\mathscr{R}_{\text{s}}}-1}{\overline{\gamma}_{\text{AB}}}$, $c \triangleq \frac{1+\overline{\gamma}_{\text{RB}}\,b}{\overline{\gamma}_{\text{RB}}}$, $k \triangleq \frac{\overline{\gamma}_{\text{AB}}}{\overline{\gamma}_{\text{AE}}(1+\overline{\gamma}_{\text{AB}}\,b)}$, $l \triangleq 1 - \frac{1}{\overline{\gamma}_{\text{RE}}\,ck}$, $\mathscr{F}(x) = e^x E_1(x)$, em que $E_1(x) = \int_x^\infty \frac{e^{-t}}{t}dt$ é a exponencial integral (GRADSHTEYN; RYZHIK, 2007).

3.5 ANÁLISE DE EFICIÊNCIA ENERGÉTICA E THROUGHPUT SEGUROS

A partir das equações da probabilidade de *outage* de segurança para cada esquema cooperativo, podemos determinar as equações de *throughput* seguro e eficiência energética segura. O *throughput* seguro, τ, representa a máxima taxa que pode ser utilizada no sistema sem ocorrer falha de confidencialidade. Esta métrica pode ser representada por

$$\tau^{(\text{esq})} = \mathscr{R}_{\text{s}}\left(1 - p_{\text{out}}^{(\text{esq})}\right), \tag{38}$$

com esq $\in \{\text{SDF}, \text{AF}, \text{DF}, \text{CJ}\}$.

Já a eficiência energética segura, η, que é a relação entre o *throughput* seguro e o gasto total de potência, é representada matematicamente por

$$\eta^{(\mathrm{esq})} = \frac{\mathscr{R}_{\mathrm{s}}}{\mathscr{P}_{\mathrm{Total}}^{(\mathrm{esq})}} \left(1 - p_{\mathrm{out}}^{(\mathrm{esq})}\right). \tag{39}$$

O $\mathscr{P}_{\mathrm{Total}}$ representa o gasto total de potência de cada esquema cooperativo. Este valor é obtido a partir de P_{TX} que representa a potência gasta no circuito de transmissão, P_{RX} que representa a potência gasta no circuito de recepção e P_{A} e P_{R} que são as potências alocadas em Alice e no *relay*, respectivamente. Em relação ao consumo de potência em Eve, este é negligenciado, já que o objetivo é maximizar a eficiência energética segura apenas do canal legítimo.

O circuito RF é o mesmo apresentado em (CUI et al., 2004; CHEN et al., 2010), o qual inclui os blocos do conversor digital-analógico, filtros de transmissão, *mixer* e sintetizador de frequência. Os consumos de potência são representados, respectivamente, por P_{DAC}, P_{mix}, $P_{\mathrm{filter_{TX}}}$ e P_{sync}. Desta forma, na transmissão o consumo de potência do *hardware* é dado por

$$P_{\mathrm{TX}} = P_{\mathrm{DAC}} + P_{\mathrm{mix}} + P_{\mathrm{filter_{TX}}} + P_{\mathrm{sync}}. \tag{40}$$

No receptor, os blocos considerados são: sintetizador de frequência, amplificador de baixo-ruído, *mixer*, amplificador de frequências intermediárias, filtros de recepção e conversores analógicos-digitais. Os consumos de potência são, respectivamente, P_{sync}, P_{LNA}, P_{mix}, P_{IFA}, $P_{\mathrm{filter_{RX}}}$ e P_{ADC}. A potência total de *hardware* utilizada na recepção é dada por

$$P_{\mathrm{RX}} = P_{\mathrm{sync}} + P_{\mathrm{LNA}} + P_{\mathrm{mix}} + P_{\mathrm{IFA}} + P_{\mathrm{filter_{RX}}} + P_{\mathrm{ADC}}. \tag{41}$$

Para o esquema SDF, temos que a potência total consumida, $\mathscr{P}_{\mathrm{Total}}$, é definida por

$$\begin{aligned} \mathscr{P}_{\mathrm{Total}}^{(\mathrm{SDF})} \simeq{}& \left(2P_{\mathrm{A}}^{(\mathrm{SDF})} + 2P_{\mathrm{TX}} + 2P_{\mathrm{RX}}\right) \cdot \Pr\{\gamma_{\mathrm{AB}} \geq \gamma_{\mathrm{AR}}\} \\ &+ \left(P_{\mathrm{A}}^{(\mathrm{SDF})} + P_{\mathrm{R}}^{(\mathrm{SDF})} + 2P_{\mathrm{TX}} + 3P_{\mathrm{RX}}\right) \cdot \Pr\{\gamma_{\mathrm{AR}} > \gamma_{\mathrm{AB}}\}, \end{aligned} \tag{43}$$

onde

$$\Pr\{\gamma_{\mathrm{AR}} > \gamma_{\mathrm{AB}}\} = \int_0^{\infty} f_{\gamma_{\mathrm{AB}}}(z) \Pr\{\gamma_{\mathrm{AR}} > z\}\, dz = \frac{\overline{\gamma}_{\mathrm{AR}}}{\overline{\gamma}_{\mathrm{AR}} + \overline{\gamma}_{\mathrm{AB}}}. \tag{44}$$

Assim, caso a cooperação seja utilizada, cuja probabilidade é dada por $\Pr\{\gamma_{\mathrm{AR}} > \gamma_{\mathrm{AB}}\}$, o gasto total de potência será composto pela potência alocada em Alice e no *relay*, mais o gasto do circuito de transmissão de Alice e dos circuitos de recepção do *relay* e Bob no primeiro intervalo de tempo. Além destes, ainda teremos o gasto do circuito de transmissão do *relay* e do

circuito de recepção de Bob no segundo intervalo de tempo. Caso a comunicação direta seja mais vantajosa, cuja probabilidade é dada por $\Pr\{\gamma_{\mathrm{AB}} \geq \gamma_{\mathrm{AR}}\}$, o gasto total de potência será dado pela potência alocada em Alice nos dois intervalos de tempo, além do gasto do circuito de transmissão de Alice e de recepção do Bob nos dois intervalos de tempo. Nota-se que a equação da potência total consumida também é uma aproximação, já que utiliza-se a mesma aproximação do cálculo da probabilidade de *outage* de segurança para definição do uso ou não da cooperação.

Já para o protocolo AF e DF temos que o gasto total de potência é definido por

$$\mathscr{P}_{\mathrm{Total}}^{(\mathrm{AF})} = P_{\mathrm{A}}^{(\mathrm{AF})} + P_{\mathrm{R}}^{(\mathrm{AF})} + 2P_{\mathrm{TX}} + 3P_{\mathrm{RX}} \tag{45}$$

e

$$\mathscr{P}_{\mathrm{Total}}^{(\mathrm{DF})} = P_{\mathrm{A}}^{(\mathrm{DF})} + P_{\mathrm{R}}^{(\mathrm{DF})} + 2P_{\mathrm{TX}} + 3P_{\mathrm{RX}}. \tag{46}$$

A potência total é dada pela potência alocada em Alice e no *relay*, o circuito de transmissão de Alice, bem como os circuitos de recepção do *relay* e Bob no primeiro intervalo de tempo, além do circuito de transmissão do *relay* e de recepção de Bob no segundo intervalo de tempo. Nota-se que a expressão da potência total dos esquemas AF e DF são semelhantes. Porém, cabe ressaltar que os valores de potência alocados em Alice e no *relay* podem ser diferentes para cada esquema dependendo do método de alocação de potência utilizado.

Finalmente, o gasto total de potência para o esquema CJ é definido por

$$\mathscr{P}_{\mathrm{Total}}^{(\mathrm{CJ})} = P_{\mathrm{A}}^{(\mathrm{CJ})} + P_{\mathrm{R}}^{(\mathrm{CJ})} + 2P_{\mathrm{TX}} + P_{\mathrm{RX}}. \tag{47}$$

Neste protocolo, a potência total é calculada pela potência alocada em Alice para transmitir a informação e no *relay* para geração do ruído Gaussiano, além dos circuitos de transmissão de Alice e do *relay* e pelo circuito de recepção de Bob.

3.6 MÉTODOS DE ALOCAÇÃO DE POTÊNCIA EM COMUNICAÇÃO COOPERATIVA SEGURA

Os três métodos utilizados neste trabalho para alocação de potência, que serão detalhados nas próximas seções, são: alocação de potências iguais, alocação de potência ótima aplicando uma abordagem de busca exaustiva e o método iterativo de alocação de potência aplicando o algoritmo Dinkelbach.

3.6.1 ALOCAÇÃO DE POTÊNCIAS IGUAIS

O esquema de alocação de potências iguais é o caso mais simples de alocação. Neste caso, a potência alocada no *relay* é igual a potência alocada em Alice. Os resultados deste método são importantes pois permitem mensurar o quão benéfico é a utilização da alocação de potência na maximização dos parâmetros analisados neste trabalho.

3.6.2 ALOCAÇÃO ÓTIMA POR BUSCA EXAUSTIVA

A alocação ótima de potência por busca exaustiva consiste em encontrar os valores de potência ótimos para Alice e para o *relay* que permitem maximizar as métricas de interesse em cada esquema cooperativo. Os problemas de alocação de potência ótima para o *throughput* seguro e eficiência energética segura podem ser definidos, respectivamente, como

$$\begin{aligned} &\max_{(P_A,P_R)} \ \tau^{(\mathrm{esq})} = \mathscr{R}_{\mathrm{s}} \left(1 - p_{\mathrm{out}}^{(\mathrm{esq})}\right) \\ &\text{dado } 0 \leq P_i \leq P_{\max}, \text{ com } i \in \{A,R\} \end{aligned} \tag{48}$$

e

$$\begin{aligned} &\max_{(P_A,P_R)} \ \eta^{(\mathrm{esq})} = \frac{\mathscr{R}_{\mathrm{s}}}{\mathscr{P}_{\mathrm{Total}}^{(\mathrm{esq})}} \left(1 - p_{\mathrm{out}}^{(\mathrm{esq})}\right) \\ &\text{dado } 0 \leq P_i \leq P_{\max}, \text{ com } i \in \{A,R\}, \end{aligned} \tag{49}$$

onde P_{max} representa a máxima potência que pode ser utilizada em cada nó operando com o esquema esq $\in \{\mathrm{SDF}, \mathrm{AF}, \mathrm{DF}, \mathrm{CJ}\}$.

Devido à complexidade das equações de probabilidade de *outage* de segurança de cada esquema cooperativo, a otimização das funções em (48) e (49) torna-se difícil de ser obtida analiticamente. Desta forma, realizamos uma busca computacional exaustiva das potências ótimas a serem alocadas, ou seja, verificamos no intervalo $0 \leq P_i \leq P_{\max}$, quais são os valores da potência do *relay* e de Alice que permitem maximizar o *throughput* seguro ou a eficiência energética segura.

3.6.3 ALOCAÇÃO ITERATIVA UTILIZANDO O ALGORITMO DINKELBACH

Como solução para a dificuldade de encontrar a solução analítica ótima de otimização das funções de *throughput* seguro e eficiência energética segura, utilizamos o algoritmo Dinkelbach. Este método, utilizado para alocação de potência de forma iterativa e distribuída, é um algoritmo que permite maximizar a razão entre duas funções de mesma variável. Note que a

equação de eficiência energética segura de cada esquema cooperativo é uma razão entre a probabilidade de *outage* de segurança de cada esquema e a potência total utilizada para transmissão da informação. Além disto, a própria equação de *throughput* seguro, que também é função da probabilidade de *outage* de segurança, também tem o numerador e denominador como funções da potência alocada no *relay*. Desta forma, como estas métricas são razões de funções de mesma variável, podem ser maximizadas a partir da utilização deste método de alocação de potência.

Esta classe de otimização de problemas é chamada de programação fracionária (do inglês, *fractional programs*), e, de forma geral, é representada por (DINKELBACH, 1967; ISHEDEN et al., 2012)

$$\max_{\mathbf{x}\in\mathbf{S}} q(x) = \frac{f_1(x)}{f_2(x)}, \tag{50}$$

onde $S \subseteq \mathbb{R}^n$, f_1, $f_2 : S \to \mathbb{R}$ e $f_2(x) > 0$.

Considerando um programa convexo paramétrico (DINKELBACH, 1967; ISHEDEN et al., 2012), é possível reescrever (50) como um programa fracionário equivalente a

$$\begin{aligned} &\max_{\mathbf{x}\in\mathbf{S},\theta\in\mathbb{R}} \theta \\ &\text{com } f_1(x) - \theta f_2(x) \geq 0. \end{aligned} \tag{51}$$

Conforme (ISHEDEN et al., 2012), podemos reescrever a equação anterior como

$$F(\theta) = \max_{\mathbf{x}\in\mathbf{S}} f_1(x) - \theta f_2(x), \tag{52}$$

em que o termo da direita pode ser visto como um problema de otimização no qual $f_1(x)$ é maximizado enquanto que $f_2(x)$ é minimizado, com o parâmetro θ determinando o peso relativo do denominador. Além do mais, a seguinte relação é mostrada

$$F(\theta) = 0 \iff \theta = q^\star, \tag{53}$$

onde $q^\star$ é o valor ótimo da função mostrada em (50). Portanto, resolver (50) é equivalente a encontrar a raiz de

$$F(\theta^\star) = \max_{\mathbf{x}\in\mathbf{S}} f_1(x) - \theta f_2(x) = 0. \tag{54}$$

Uma forma iterativa de encontrar a raiz de $F(\theta)$ é o algoritmo Dinkelbach (DINKELBACH, 1967; ISHEDEN et al., 2012). Este algoritmo baseia-se no método de Newton para encontrar o ótimo $x_n^\star$ para um dado valor de θ_n, conforme

$$\theta_{n+1} = \theta_n - \frac{F(\theta_n)}{F'(\theta_n)} = \frac{f_1(x_n^\star)}{f_2(x_n^\star)}. \tag{55}$$

A aplicação do algoritmo Dinkelbach é resumida no Algoritmo 1, podendo ser utilizado tanto para maximização do *throughput* seguro quanto da eficiência energética segura de cada esquema cooperativo apresentado anteriormente.

Algoritmo 1 O método Dinkelbach

Dados: θ_0 satisfazendo $F(\theta_0) \geq 0$, com tolerância Δ

$n = 0$;

enquanto $|F(\theta_n)| \geq \Delta$ **faça**

Utilize $\theta = \theta_n$ para obter P_{i_n}, $i \in \{\mathrm{A}, \mathrm{R}\}$;

$\theta_{n+1} = \frac{f_1(P_{i_n})}{f_2(P_{i_n})}$;

$n++$;

fim

4 RESULTADOS NUMÉRICOS

Neste capítulo é realizada uma comparação entre os métodos cooperativos SDF, AF, DF e CJ utilizando a alocação de potência. A alocação de potência visando a maximização de *throughput* seguro é mostrada na Seção 4.1, enquanto a maximização da eficiência energética segura é apresentada na Seção 4.2. Também é realizado um estudo comparativo do desempenho do algoritmo Dinkelbach em relação aos outros esquemas de alocação de potência. Salvo indicação contrária, considera-se $\mathscr{R}_{\mathrm{s}} = 2$ bits seguros/s/Hz, $d_{\mathrm{AB}} = 100$ m, $\upsilon = 3$, $B = 10$ kHz e $N_0 = -174$ dBm/Hz. Seguindo (CUI et al., 2004), temos que o consumo de cada bloco do circuito de transmissão e recepção é dado pela Tabela 1. Além do mais, considera-se uma margem de enlace de $M_l = 40$ 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.

Tabela 1: Parâmetros do sistema.

Conversor digital-analógico	$P_{\mathrm{DAC}} = 15$ mW
Mixer	$P_{\mathrm{mix}} = 30,3$ mW
Filtros de transmissão	$P_{\mathrm{filter_{TX}}} = 2,5$ mW
Sintetizador de frequência	$P_{\mathrm{sync}} = 50$ mW
Amplificador de baixo ruído	$P_{\mathrm{LNA}} = 20$ mW
Amplificador intermediário de potência	$P_{\mathrm{IFA}} = 3$ mW
Filtros de recepção	$P_{\mathrm{filter_{RX}}} = 2,5$ mW
Conversor analógico-digital	$P_{\mathrm{ADC}} = 7$ mW

Fonte: Autoria própria.

4.1 THROUGHPUT SEGURO

Inicialmente os resultados de *throughput* seguro para o SDF obtidos a partir dos diversos métodos de alocação de potência são comparados, conforme Figuras 6 e 7. Consideramos $\overline{\gamma}_{\mathrm{RE}} = 28$ dB e $\overline{\gamma}_{\mathrm{AE}} = 8$ dB, enquanto variamos a SNR do canal legítimo. A SNR do canal legítimo dita a potência associada com Alice e, para um valor específico de P_{A}, utilizamos os três algoritmos de alocação de potência da Seção 3.6 para encontrar a potência ótima para o

relay, P_{R}.

A partir da análise das Figuras 6 e 7, verificamos que a alocação de potência permite claramente melhorar o desempenho do sistema em comparação com o caso de alocação de potências iguais. Além disto, a alocação de potência proposta de forma iterativa e distribuída, com utilização do algoritmo Dinkelbach, apresenta um desempenho muito próximo à abordagem de busca exaustiva, com uma complexidade significativamente menor. Nestes exemplos, o esquema iterativo converge dentro de três iterações. Além do mais, verificamos que a proximidade do *relay* a Alice implica em maiores diferenças entre o esquema de alocação de potências iguais e os outros esquemas de alocação.

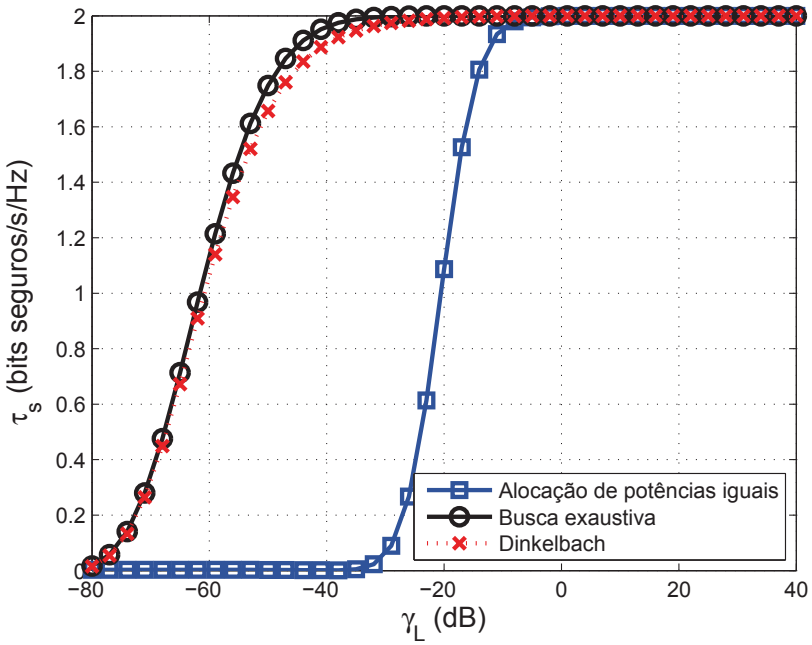


Figura 6: *Throughput* **seguro do esquema SDF a partir de três métodos de alocação de potência:** ***i.)*** **alocação de potências iguais;** ***ii.)*** **algoritmo Dinkelbach;** ***iii.)*** **busca exaustiva. A relação entre as distâncias entre Alice-***relay* **e Alice-Bob é dada por** $d_{\mathbf{AR}} = 0,2\,d_{\mathbf{AB}}$ **enquanto a SNR de Eve é fixa, com** $\overline{\gamma}_{\mathrm{RE}} = 28$ **dB e** $\overline{\gamma}_{\mathrm{AE}} = 8$ **dB.**

Fonte: Autoria Própria

A partir das simulações verificamos que, para diferentes posições do *relay*, a diferença entre os métodos de alocação de potência iterativa e de busca exaustiva tornavam-se maiores. Desta forma, visando mensurar a diferença entre a alocação de potência iterativa e a de busca exaustiva, definimos o erro entre os dois métodos como

$$\varepsilon_{\tau}(\%) = \left(\frac{\tau_{\mathrm{Busca\,Exaustiva}} - \tau_{\mathrm{Iterativo}}}{\tau_{\mathrm{Busca\,Exaustiva}}} \right) \cdot 100, \tag{56}$$

onde $\tau_{\mathrm{Busca\,Exaustiva}}$ representa o valor de *throughput* seguro obtido para uma dada SNR, γ_L,

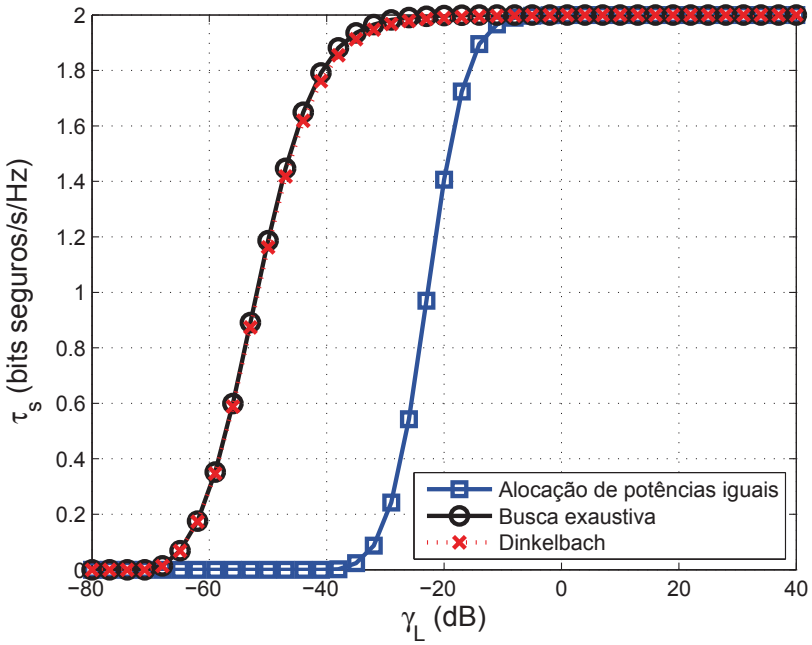


Figura 7: *Throughput* **seguro do esquema SDF a partir de três métodos de alocação de potência:** ***i.)*** **alocação de potências iguais;** ***ii.)*** **algoritmo Dinkelbach;** ***iii.)*** **busca exaustiva. A relação entre as distâncias entre Alice-***relay* **e Alice-Bob é dada por** $d_{\mathbf{AR}} = 0,5\,d_{\mathbf{AB}}$ **enquanto a SNR de Eve é fixa, com** $\overline{\gamma}_{\mathrm{RE}} = 28$ **dB e** $\overline{\gamma}_{\mathrm{AE}} = 8$ **dB.**

Fonte: Autoria Própria

considerando uma posição intermediária do *relay* entre Alice e Bob a partir da alocação de potência de busca exaustiva. Enquanto $\tau_{\mathrm{Iterativo}}$ representa o valor de *throughput* seguro obtido para a mesma SNR, γ_L, considerando também a mesma posição do *relay* pela alocação de potência iterativa. Para realização da simulação consideramos uma potência fixa de $\gamma_L = -40$ dB, a qual por simulação verificamos que maximizava a diferença entre os dois métodos de alocação. Além disto, variamos a distância do *relay* entre Alice e Bob e realizamos alocação de potência no *relay*. Analisando a Figura 8, verificamos que o erro entre os métodos é mais acentuado quando o *relay* encontra-se próximo à Alice. Além disso, o erro entre os métodos de alocação em todos os casos é inferior a 6%.

Também comparamos, conforme a Figura 9, os esquemas SDF, AF, DF e CJ para diferentes posições de Eve com relação ao *relay*. Incluímos nesta simulação também o esquema direto, sem a utilização da cooperação, para efeito de comparação. Neste esquema consideramos que a transmissão é realizada em dois intervalos de tempo com retransmissão por Alice, a fim de realizarmos uma comparação justa com o SDF. Somente o máximo *throughput* obtido através da alocação de potência é considerado. Quando Eve está próxima aos nós legítimos, o esquema CJ apresenta maior *throughput* seguro, porém, quando Eve move-se para longe dos

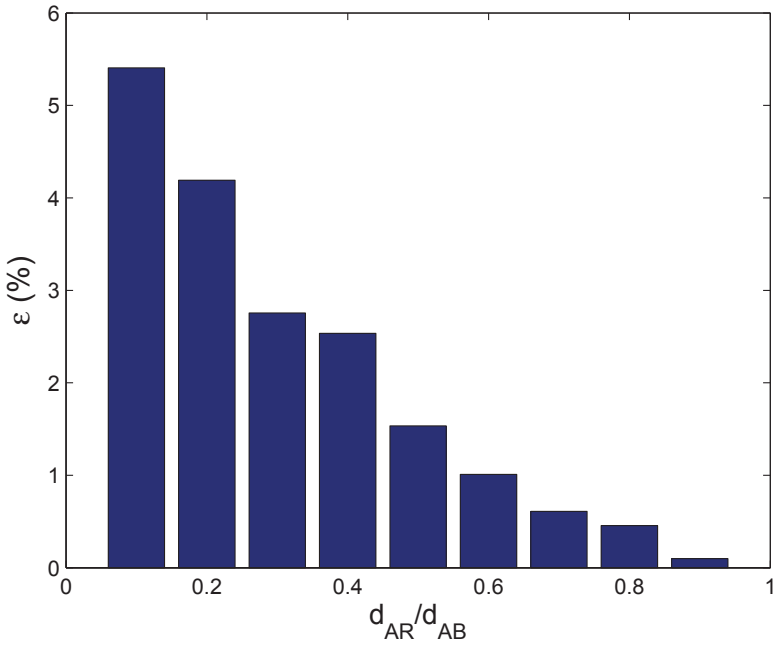


Figura 8: Erro do método iterativo em relação ao método exaustivo de alocação de potência do esquema SDF a partir da variação da distância intermediária do *relay* entre Alice e Bob.

Fonte: Autoria Própria

nós legítimos, o esquema SDF torna-se a melhor escolha para maximizar o *throughput* seguro. Uma comparação similar, mas em termos de probabilidade de *outage* de segurança, foi realizada em (GABRY et al., 2011a), na qual o AF tem a menor probabilidade de *outage* de segurança em comparação com o DF e CJ. Entretanto, somente o DF foi considerado, não explorando completamente a CSI disponível a Alice. Além do mais, é interessante notarmos que AF e DF só se tornam tão vantajosos quanto o SDF, quando Eve está muito distante dos nós legítimos. Em relação ao esquema direto, é interessante salientar que ele apresenta um desempenho subótimo em relação ao protocolo SDF em todo o intervalo, já que o SDF permite à Alice escolher entre a melhor comunicação, direta ou cooperativa.

4.2 EFICIÊNCIA ENERGÉTICA SEGURA

Similarmente à analise de *throughput* seguro, para a eficiência energética segura comparamos os esquemas de alocação de potência para o método cooperativo SDF para uma posição intermediária do *relay* entre Alice e Bob, conforme Figura 10. Novamente verificamos que o algoritmo Dinkelbach apresenta resultados semelhantes à alocação ótima visando a maximização da eficiência energética segura.

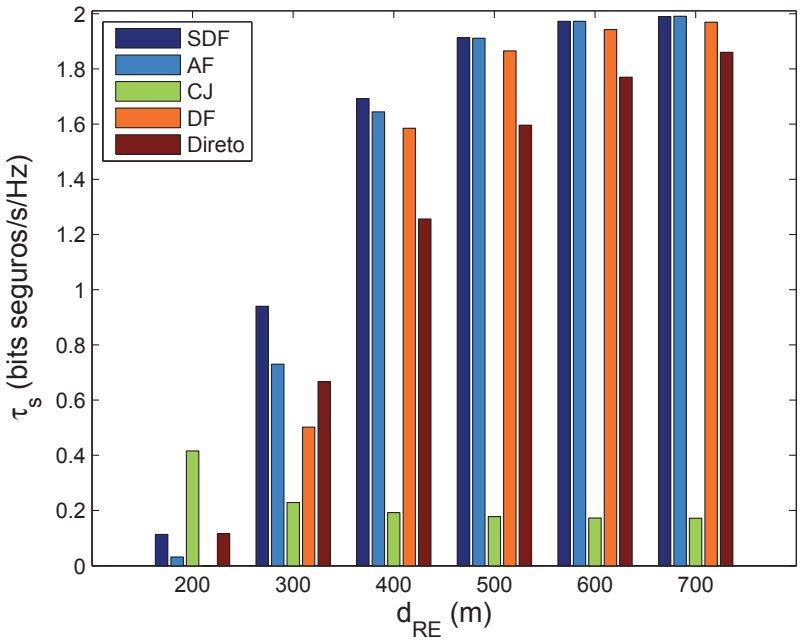


Figura 9: *Throughput* **seguro do SDF, AF, DF, CJ e direto em função da distância entre Eve e o** *relay* **(d_{RE}).**

Fonte: Autoria Própria

Buscando definir a proximidade de resultados entre o método iterativo de alocação de potência e o método de busca exaustiva, definimos também o erro percentual, semelhante à (56), entre os maiores valores de eficiência energética segura obtidas pelos dois métodos de alocação, a partir da variação da distância intermediária do *relay* entre Alice e Bob. Como resultado, obtemos valores semelhantes para todo intervalo de distância, com média de erro percentual igual a $1,42\%$.

De maneira semelhante à análise do *throughput* seguro, conforme a Figura 11, comparamos também a eficiência energética segura dos esquemas SDF, AF, DF, CJ e direto para diferentes posições de Eve com relação ao *relay*. Consideramos somente a máxima eficiência obtida através dos métodos de alocação de potência iterativa e de busca exaustiva. Como resultado, temos que quando Eve está próximo aos nós legítimos, o esquema CJ apresenta melhor desempenho. Porém, quando Eve move-se para longe dos nós legítimos, o esquema SDF torna-se a melhor escolha. Ao contrário da análise de *throughput* seguro, no qual os esquemas SDF, AF e DF apresentam um desempenho similar quando a distância de Eve em relação aos nós legítimos aumenta, na análise da eficiência energética segura, o SDF apresenta uma vantagem considerável em relação aos esquemas DF e AF, mesmo quando d_{RE} aumenta. Além disto, o melhor desempenho do esquema direto em relação aos esquemas DF e AF, com o aumento da

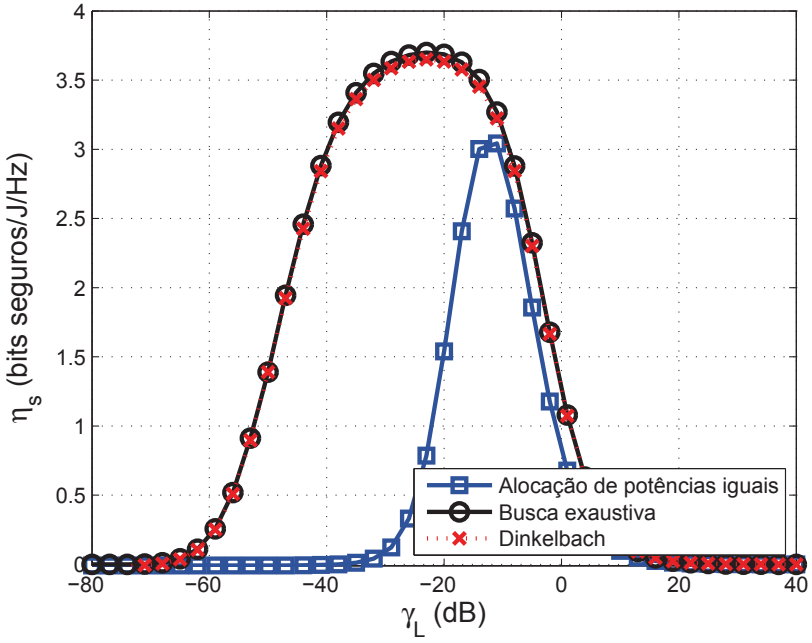


Figura 10: Eficiência energética segura do esquema SDF a partir de três esquemas de alocação de potência: *i.)* Alocação de potências iguais; *ii.)* algoritmo Dinkelbach; *iii.)* busca exaustiva. A relação entre as distâncias entre Alice-*relay* e Alice-Bob é dada por $d_{\mathbf{AR}} = 0,5\,d_{\mathbf{AB}}$ enquanto a SNR de Eve é fixa, com $\overline{\gamma}_{\mathrm{RE}} = 28$ dB e $\overline{\gamma}_{\mathrm{AE}} = 8$ dB.

Fonte: Autoria Própria

distância de Eve aos nós legítimos, demonstra a vantagem da possibilidade de escolha entre a cooperação ou comunicação direta no esquema SDF.

A comparação também é estendida para diferentes taxas de transmissão e posições do *relay*, com $d_{\mathrm{AR}} = 0,2d_{\mathrm{AB}}$ na Figura 12, $d_{\mathrm{AR}} = 0,5d_{\mathrm{AB}}$ na Figura 13 e $d_{\mathrm{AR}} = 0,8d_{\mathrm{AB}}$ na Figura 14. Para uma melhor visualização, somente os esquemas SDF e CJ são considerados já que todos os demais esquemas tem desempenho inferior a algum desses dois. Como podemos notar pelas figuras, o desempenho dos esquemas depende profundamente de $\mathscr{R}_{\mathrm{s}}$ e d_{AR}. De forma geral, observa-se que a taxa de transmissão tem uma forte influência no SDF, que apresenta um melhor desempenho em taxas baixas e moderadas, enquanto o CJ apresenta um melhor desempenho para altas $\mathscr{R}_{\mathrm{s}}$. Adicionalmente, a posição do *relay* tem forte efeito no CJ. A Figura 12 mostra que se o *relay* e Eve estão próximos a Alice, o CJ apresenta melhor desempenho do que quando o *relay* e Eve estão próximos a Bob. Isto ocorre porque no primeiro caso o ruído Gaussiano injetado pelo *relay* é considerado mais atenuado em Bob do que em Eve. No caso contrário, o *relay* move-se para próximo de Bob, como mostrado na Figura 14, de modo que o sinal interferente adicionado pelo *relay* afeta Bob com mais intensidade e, portanto, a eficiência energética segura do CJ diminui.

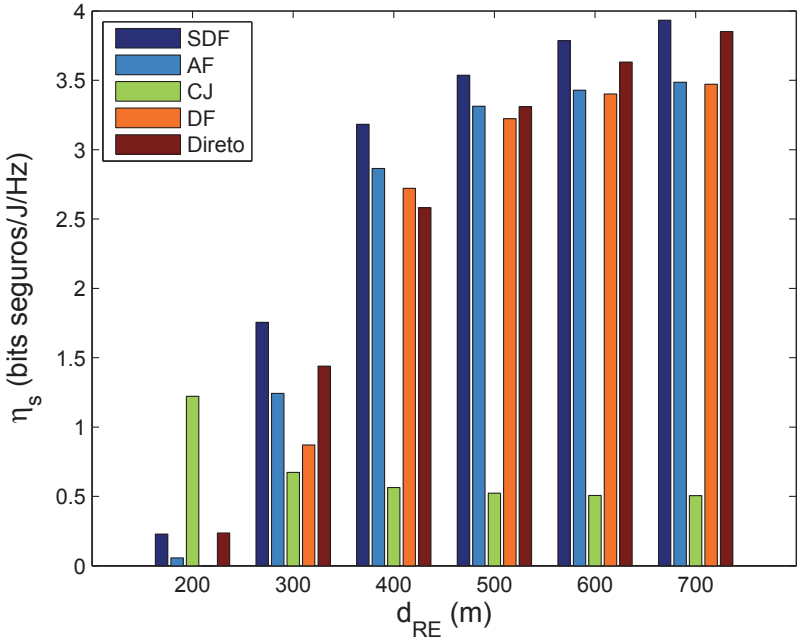


Figura 11: Eficiência energética segura do SDF, AF, DF, CJ e direto em função da distância entre Eve e o *relay* (d_{RE}).

Fonte: Autoria Própria

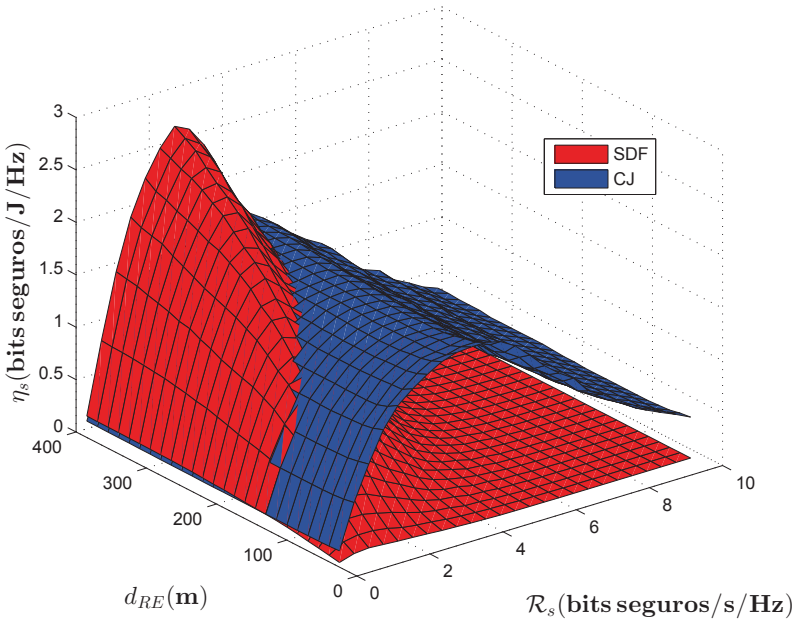


Figura 12: Eficiência energética segura do SDF e CJ em função de d_{RE} e $\mathscr{R}_s$ para $d_{\mathrm{AR}} = 0,2\,d_{\mathrm{AB}}$.

Fonte: Autoria Própria

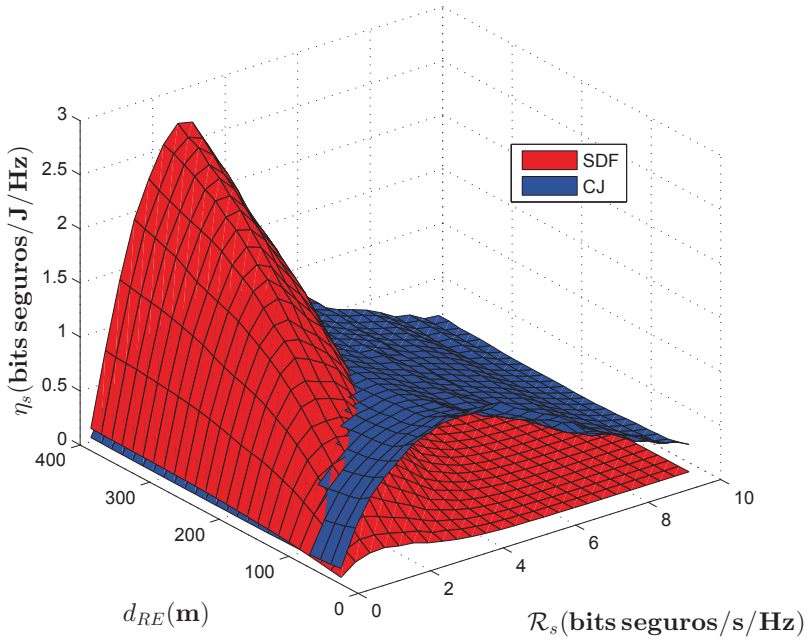


Figura 13: Eficiência energética segura do SDF e CJ em função de $d_{\mathbf{RE}}$ e $\mathscr{R}_s$ para $d_{\mathbf{AR}} = 0,5\,d_{\mathbf{AB}}$.

Fonte: Autoria Própria

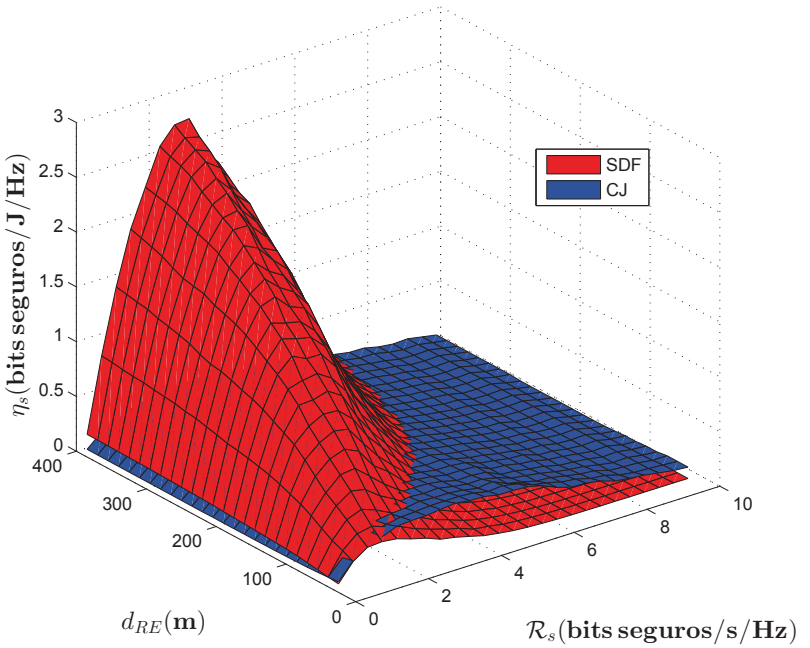


Figura 14: Eficiência energética segura do SDF e CJ em função de $d_{\mathbf{RE}}$ e $\mathscr{R}_s$ para $d_{\mathbf{AR}} = 0,8\,d_{\mathbf{AB}}$.

Fonte: Autoria Própria

5 CONCLUSÕES

Em um contexto no qual a segurança na transmissão sem fio de mensagens exerce grande impacto no desenvolvimento de novos sistemas, este trabalho propõe a análise de diferentes esquemas cooperativos utilizando um *relay* para auxiliar Alice a transmitir a informação de maneira segura a Bob, sem que Eve consiga decodificar a informação. Para isto derivamos uma equação fechada aproximada para o esquema SDF e realizamos a comparação deste esquema com outros esquemas de cooperação tais como o DF, o AF e o CJ. O esquema SDF é proposto visando explorar completamente a CSI disponível a Alice em relação ao canal legítimo. A CSI é explorada completamente ao possibilitar Alice escolher de antemão sobre qual caminho é mais vantajoso para a comunicação, seja a transmissão direta, realizada em dois instantes de tempo com retransmissão por parte da própria Alice, seja a transmissão cooperativa, realizada também em dois instantes de tempo, mas com o auxílio do *relay* no segundo instante.

A alocação de potência também é estudada visando a maximização do desempenho do *throughput* seguro ou da eficiência energética segura dos diferentes esquemas cooperativos. Para isto, diferentes métodos de alocação de potência são utilizados, considerando desde o caso mais simples, no qual a potência alocada em Alice é igual à potência alocada no *relay*, até o caso mais complexo, onde a potência alocada em Alice e no *relay* é escolhida a partir de uma busca exaustiva em todos os valores possíveis de serem alocados. Ademais, considerando uma estratégia com complexidade intermediária, tentando obter um desempenho semelhante à alocação ótima mas com menor complexidade, também consideramos o algoritmo Dinkelbach, desenvolvido para otimizações de razões de funções de uma mesma variável.

Em relação aos resultados numéricos, mostra-se que o protocolo SDF apresenta um desempenho superior aos dos outros esquemas cooperativos, como CJ, AF e DF na maior parte das situações. Esta análise é estendida para eficiência energética considerando também a taxa de transmissão. Conclui-se que quando a taxa de transmissão aumenta ou quando Eve está próximo aos nós legítimos, o esquema CJ apresenta maior *throughput* e eficiência energética. Caso contrário, o esquema SDF apresenta desempenho superior. Em termos de alocação de potência, o algoritmo Dinkelbach proposto apresenta um resultado muito próximo a abordagem

ótima de busca exaustiva, mas com menor complexidade.

Como trabalhos futuros, contempla-se a utilização de múltiplas antenas em Alice e/ou no *relay* de forma a obter um melhor desempenho na confidencialidade da troca de informações. Em (BRANTE et al., 2015b; ALVES et al., 2012) considera-se o caso com múltiplas antenas em Alice e no *relay* no qual escolhe-se a antena que apresenta melhor condição de transmissão em relação ao canal legítimo. Considerando que a CSI de nenhum dos canais é conhecida e que a antena de Alice é selecionada a partir do envio do índice da melhor antena por Bob, a utilização de múltiplas antenas em Alice apenas beneficia o canal legítimo, de forma que não existe ganho algum a Eve. Além do mais, outras estratégias envolvendo *jamming* podem ser exploradas, por exemplo, tentando realizar um *beamforming* com as antenas do *relay* de forma que ocorra interferência somente em Eve, com mínima interferência em Bob, conforme mostrado em (ZHANG et al., 2015). Outra forma de explorar múltiplas antenas no sistema é emulando um canal *fast-fading* para Eve de modo que a informação não possa ser decodificada. Em (WANG et al., 2015b), realiza-se uma comparação inicial entre a técnica do *beamforming* e do *fast-fading* citadas, caracterizando a taxa de confidencialidade para estes sistemas, considerando múltiplas antenas no transmissor. Uma futura extensão deste trabalho está relacionada ao uso da cooperação, por exemplo, considerando múltiplas antenas no *relay* ou até múltiplos *relays*.

Outra possível extensão está relacionada à consideração de outros cenários de disponibilidade da CSI. Por exemplo, realizando uma análise destes esquemas cooperativos considerando que Alice não tem conhecimento da CSI de nenhum dos canais, legítimo e de Eve. Dessa forma, seria necessário realizar uma abordagem probabilística de Bob não conseguir decodificar a mensagem transmitida por Alice e da probabilidade da capacidade instantânea do canal de Eve superar a taxa de equivoco do código de escuta utilizado. Este cenário ainda é pouco explorado na literatura, com algumas exceções (TANG et al., 2009; BRANTE et al., 2015a; LIU et al., 2015), porém é bastante prático em redes de sensores com um número de nós muito grande, no qual é difícil ao transmissor ter qualquer tipo de CSI.

REFERÊNCIAS

ALVES, H. et al. Performance of transmit antenna selection physical layer security schemes. **IEEE Signal Process. Lett**, v. 19, n. 6, p. 372–375, Jun. 2012. ISSN 1070-9908.

BARROS, J.; RODRIGUES, M. Secrecy capacity of wireless channels. In: **IEEE Int. Symp. on Inf. Theory**. 2006. p. 356–360.

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

BLOCH, M. et al. Wireless information-theoretic security. **IEEE Trans. Inf. Theory**, v. 54, n. 6, p. 2515–2534, Jun. 2008. ISSN 0018-9448.

BRANTE, G. et al. Secrecy analysis of transmit antenna selection cooperative schemes with no channel state information at the transmitter. **IEEE Trans. Commun.**, PP, n. 99, p. 1–1, Feb. 2015. ISSN 0090-6778.

BRANTE, G. et al. Secrecy analysis of transmit antenna selection cooperative schemes with no channel state information at the transmitter. **IEEE Trans. Com**, v. 63, n. 4, p. 1330–1342, Apr. 2015. ISSN 0090-6778.

BRANTE, G. et al. 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.

CHEN, G. et al. Circuit design advances for wireless sensing applications. **Proc. IEEE**, v. 98, n. 11, p. 1808–1827, Nov 2010. ISSN 0018-9219.

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.

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

DONG, L. et al. Improving wireless physical layer security via cooperating relays. **IEEE Trans. Signal Process**, v. 58, n. 3, p. 1875–1888, Mar. 2010. ISSN 1053-587X.

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

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. Workshops (ICC)**. 2011b. p. 1–5.

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

GRADSHTEYN, I. S.; RYZHIK, I. M. **Table of integrals, series, and products**. Seventh. Elsevier/Academic Press, Amsterdam, 2007. xlviii+1171 p.

ISHEDEN, C. et al. Framework for link-level energy efficiency optimization with informed transmitter. **IEEE Trans. Wireless Commun.**, v. 11, n. 8, p. 2946–2957, 2012.

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.

LEUNG-YAN-CHEONG, S.; HELLMAN, M. The Gaussian wire-tap channel. **IEEE Trans. I**, v. 24, n. 4, p. 451–456, Jul 1978. ISSN 0018-9448.

LIU, T. et al. 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.

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

PAPOULIS, A. **Probability, random variables, and stochastic processes**. New York: McGraw-Hill, 1991. (McGraw-Hill series in electrical engineering). ISBN 0-07-100870-5.

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

SHANNON, C. A mathematical theory of communication. **Bell Syst. Tech. J.**, v. 27, p. 379–423, 623–656, Oct. 1948.

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

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. et al. 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.

VILELA, J. et al. 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. et al. Energy efficient secure communication over decode-and-forward relay channels. **IEEE Trans. Commun.**, v. 63, n. 3, p. 892–905, Mar. 2015. ISSN 0090-6778.

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.

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

ZHANG, X. et al. 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.