UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Câmpus de São João da Boa Vista - SP

EDSON NOBUYUKI EGASHIRA

ANÁLISE DE DESEMPENHO DE SIGILO DE REDES COOPERATIVAS COM RETRANSMISSOR NÃO CONFIÁVEL USANDO JAMMING E ESTRATÉGIAS DE TRANSFERÊNCIA DE ENERGIA SEM FIO

São João da Boa Vista - SP
2020

EDSON NOBUYUKI EGASHIRA

ANÁLISE DE DESEMPENHO DE SIGILO DE REDES COOPERATIVAS COM RETRANSMISSOR NÃO CONFIÁVEL USANDO JAMMING E ESTRATÉGIAS DE TRANSFERÊNCIA DE ENERGIA SEM FIO

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia Elétrica -ICTS/SJBV, Câmpus de São João da Boa Vista, da Universidade Estadual Paulista "Júlio de Mesquita Filho", como parte dos requisitos para obtenção do título de Mestre em Engenharia Elétrica.

Financiadora: CAPES

Prof. Dr. Edgar Eduardo Benitez Olivo
Orientador

São João da Boa Vista - SP
2020

E28a

Egashira, Edson Nobuyuki

Análise de desempenho de sigilo de redes cooperativas com retransmissor não confiável usando jamming e estratégias de transferência de energia sem fio / Edson Nobuyuki Egashira. -- São João da Boa Vista, 2020

67 p. : il.

Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Câmpus Experimental de São João da Boa Vista, São João da Boa Vista

Orientador: Edgar Eduardo Benitez Olivo

1. Telecomunicações. 2. Sistemas de comunicação sem fio. 3. Probabilidades. 4. Sistemas de segurança. 5. Energia Transferência. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca do Câmpus Experimental de São João da Boa Vista. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

UNIVERSIDADE ESTADUAL PAULISTA

Câmpus de Sorocaba

CERTIFICADO DE APROVAÇÃO

TÍTULO DA DISSERTAÇÃO: **Análise de desempenho de sigilo de redes cooperativas com retransmissor não confiável usando jamming e estratégias de transferência de energia sem fio.**

AUTOR: EDSON NOBUYUKI EGASHIRA
ORIENTADOR: EDGAR EDUARDO BENITEZ OLIVO

Aprovado como parte das exigências para obtenção do Título de Mestre em ENGENHARIA ELÉTRICA, área: Sistemas Eletrônicos pela Comissão Examinadora:

Prof. Dr. EDGAR EDUARDO BENITEZ OLIVO
Coordenadoria de Curso de Engenharia Eletrônica e de Telecomunicações / Câmpus de São João da Boa Vista

Prof. Dr. CARLOS RAFAEL NOGUEIRA DA SILVA
Departamento de Engenharia Elétrica / Universidade Federal do Triângulo Mineiro (UFTM)

Prof. Dr. HENRY RAMIRO CARVAJAL MORA
Faculdade de Engenharia e Ciências Aplicadas, Engenharia em Telecomunicações / Universidad de Las Américas (UDLA)

Sorocaba, 29 de outubro de 2020

À minha família, em especial aos meus pais Nelson e Nelly, à minha irmã Erika e aos meus amigos de longa data por todo apoio, confiança e incentivo em todos os momentos.

AGRADECIMENTOS

Primeiramente agradeço a Deus, por ter me dado força e saúde para chegar até aqui.

Aos meus pais e minha irmã, Nelson, Nelly e Erika, por todo amor e incentivo.

Ao meu orientador, Prof. Dr. Edgar, pelos valiosos ensinamentos e orientações dadas até o momento. Não conseguiria chegar tão longe sem a orientação devida.

Minha sincera gratidão à Profa. Dra. Diana, pelo apoio e incentivo desde a orientação do TCC até os dias de hoje e por acreditar no meu potencial de crescimento.

Aos professores membros da banca examinadora, Dr. Carlos Rafael Nogueira da Silva e Dr. Henry Ramiro Carvajal Mora, pela disponibilidade e pelas sugestões para a melhoria deste trabalho.

Meus agradecimentos a todos os familiares, amigos, professores e funcionários da UNESP de São João da Boa Vista, pela contribuição direta ou indireta para a realização deste trabalho.

Por fim, à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001, pela oportunidade e suporte financeiro.

”A persistência é o menor caminho do êxito”

Charles Chaplin

RESUMO

Neste trabalho, o desempenho em termos da probabilidade de *outage* de sigilo para uma rede cooperativa de dois saltos, em que o retransmissor é considerado ser não confiável, possuir energia restrita e operar sob o protocolo amplifica-e-encaminha, é investigado. A técnica de *jamming* baseado no destino é adotada para prevenir que o retransmissor obtenha informação a partir da mensagem da fonte. Adicionalmente, a fim de fornecer uma fonte de alimentação de energia para o retransmissor, três estratégias de transferência de energia sem fio são consideradas: alimentação a partir da fonte, alimentação a partir do destino, e alimentação conjunta a partir da fonte e destino. Para este propósito, em todas as estratégias de transferência de energia sem fio, o protocolo de comutação no tempo é usado, o qual se baseia na utilização de intervalos de tempo alternados para as fases de transferência de energia e transmissão de informação. Para os esquemas propostos, expressões assintóticas em forma fechada para a probabilidade de *outage* de sigilo são obtidas no regime de alta relação sinal-ruído. A acurácia dessas expressões é verificada por meio de simulações de Monte Carlo em diversos casos ilustrativos. O efeito de vários parâmetros chave do sistema sobre o desempenho de sigilo é investigado, incluindo o fator de alocação de tempo entre as fases de transferência de energia e transmissão de informação, o fator de alocação de potência entre a fonte e destino para a transmissão do sinal de informação e do sinal de *jamming*, respectivamente, e a posição relativa do retransmissor entre fonte e destino. Resultados numéricos mostram que a estratégia de alimentação conjunta a partir da fonte e destino supera as outras estratégias de transferência de energia sem fio, considerando um regime de média-a-alta relação sinal-ruído. Ao avaliar o impacto da posição do retransmissor, os resultados mostram que, conforme o retransmissor se aproxima da fonte, a melhor estratégia para garantir sigilo no processo de comunicação é obtida quando a estratégia de alimentação a partir da fonte é considerada.

Palavras-chave: *Jamming* cooperativo, probabilidade de *outage* de sigilo, retransmissor não confiável, segurança na camada física, transferência de energia sem fio.

ABSTRACT

In this work, the performance in terms of the secrecy outage probability for a dual-hop cooperative network, in which the relay is considered to be untrustworthy, to have constrained energy and to operate under the amplify-and-forward protocol, is investigated. A destination based jamming technique is adopted in order to prevent the relay from obtaining information from the source's message. Additionally, with the aim of providing power supply to the relay node, three wireless energy transfer strategies are considered: wireless energy transfer from the source, wireless energy transfer from the destination and wireless energy transfer from both source and destination. For this purpose, for all strategies, a time-switching protocol is used, which is based on the use of alternating time intervals for the energy harvesting and information transmission phases. For the proposed schemes, closed-form asymptotic expressions for the secrecy outage probability are derived at the high signal-to-noise ratio regime. The accuracy of these expressions is verified through Monte Carlo simulations for different illustrative cases. The effect of key system parameters on the secrecy performance is investigated, including the time allocation factor between the energy harvesting and information transmission phases, power allocation factor between source and destination for the transmission of information and jamming signals, respectively, and the relay's relative position between source and destination. Numerical results show that, in general, the strategy of wireless energy transfer from both source and destination outperforms the others strategies, considering a medium-to-high signal-to-noise ratio regime. When assessing the impact of the relay's position, results show that, as the relay approaches the source, the best strategy to ensure secrecy in the communication process is attained when the source-based wireless energy transfer strategy is considered.

Keywords: Cooperative jamming, physical layer security, secrecy outage probability, untrustworthy relay, wireless energy transfer.

LISTA DE FIGURAS

LISTA DE ABREVIAÇÕES E SIGLAS

5G	quinta geração
AF	amplifica-e-encaminha (*amplify-and-forward*)
AWGN	ruído aditivo branco e gaussiano (*additive white Gaussian noise*)
CDF	função de distribuição acumulada (*cumulative distribution function*)
CJ	interferência intencionada cooperativa (*cooperative jamming*)
CSI	informação de estado de canal (*channel state information*)
D-WET	transferência de energia sem fio a partir do destino (*destination wireless energy transfer*)
DBJ	*jamming* baseado no destino (*destination-based jamming*)
DF	decodifica-e-encaminha (*decode-and-forward*)
EH	colheita de energia (*energy harvesting*)
eMBB	banda larga móvel aprimorada (*enhanced mobilie broadband*)
HD	*half duplex*
IMT	Telecomunicações Móveis Internacionais (*International Mobile Telecommunications*)
IoT	Internet das coisas (*Internet of Things*)
IT	transmissão de informação (*information transmission*)
mMTC	comunicação massiva do tipo máquina (*massive machine-type communication*)
PDF	função densidade de probabilidade (*probability density function*)
PLS	segurança na camada física (*physical layer security*)
RF	radiofrequência (*radio frequency*)
S-WET	transferência de energia sem fio a partir da fonte (*source wireless energy transfer*)
SBJ	*jamming* baseado na fonte (*source-based jamming*)
SD-WET	transferência de energia sem fio a partir da fonte e do destino (*source and destination wireless energy transfer*)
SNR	relação sinal-ruído (*signal-to-noise ratio*)
SRT	compromisso entre confiabilidade e segurança (*security-reliability tradeoff*)
SWIPT	transferência simultânea de informação e potência sem fio (*simultaneous wireless information and power transfer*)
TDMA	acesso múltiplo por divisão de tempo (*time division multiple access*)
URLLC	comunicação ultra confiável e de baixa latência (*ultra-reliable and low-latency communication*)
WET	transferência de energia sem fio (*wireless energy transfer*)

LISTA DE SÍMBOLOS

C_e	Capacidade do enlace de escuta
C_ℓ	Capacidade do enlace legítimo
C_s	Capacidade de sigilo
$F_A(\cdot)$	CDF de uma variável aleatória A
h_{SR}	Coeficiente do canal do enlace fonte-retransmissor
h_{RD}	Coeficiente do canal do enlace retransmissor-destino
$n_{\mathrm{R}}(t)$	Componente do ruído no receptor do retransmissor
$n_{\mathrm{D}}(t)$	Componente do ruído no receptor do destino
d_{SD}	Distância entre fonte e destino
d_{SR}	Distância entre fonte e retransmissor
d_{RD}	Distância entre retransmissor e destino
E_{S}	Energia armazenada no retransmissor proveniente de sinais RF vindos da fonte
E_{SD}	Energia armazenada no retransmissor proveniente de sinais RF vindos da fonte e destino
E_{D}	Energia armazenada no retransmissor proveniente de sinais RF vindos do destino
$\mathrm{E}\{\cdot\}$	Esperança matemática
β	Expoente de perda de percurso
μ	Fator de alocação de potência entre fonte e destino durante a fase de EH
δ	Fator de alocação de potência entre fonte e destino durante o primeiro subintervalo da fase de transmissão de informação
α	Fator de alocação de tempo entre as fases de EH e transmissão de informação
G	Fator de amplificação relativo ao protocolo de retransmissão AF
η	Fator de eficiência de conversão de energia
$\Gamma(\cdot)$	Função Gama
g_{SR}	Ganho instantâneo de canal do enlace fonte-retransmissor
g_{RD}	Ganho instantâneo de canal do enlace retransmissor-destino
Ω_{SR}	Ganho médio de canal do enlace fonte-retransmissor
Ω_{RD}	Ganho médio de canal do enlace retransmissor-destino
T	Intervalo de tempo total referente à transmissão do quadro
$f_A(\cdot)$	PDF de uma variável aleatória A
N	Potência do ruído AWGN
P	Potência transmitida total do sistema
P_{D}	Potência transmitida no destino
P_{R}	Potência transmitida no retransmissor

P_{S}	Potência transmitida na fonte
P_{sout}	Probabilidade de *outage* de sigilo
$s_{\mathrm{I}}(t)$	Sinal de informação
$s_{\mathrm{J}}(t)$	Sinal de interferência intencionada (*jamming*)
$y_{\mathrm{D}}(t)$	Sinal recebido no destino
$y_{\mathrm{R}}(t)$	Sinal recebido no retransmissor
Γ_{ℓ}	SNR fim-a-fim recebida no enlace legítimo
Γ_{e}	SNR recebida no enlace de escuta
γ_{P}	SNR transmitida total do sistema
γ_{D}	SNR transmitida no destino
γ_{R}	SNR transmitida no retransmissor
γ_{S}	SNR transmitida na fonte
R	Taxa de sigilo alvo
τ	Limiar de sigilo alvo
θ	Variável auxiliar para a alimentação do retransmissor durante a fase de EH

TRABALHOS PUBLICADOS PELO AUTOR

- E. N. Egashira, E. E. Benitez Olivo, D. P. Moya Osorio, e H. Alves, "*Secrecy performance of untrustworthy AF relay networks using cooperative jamming and SWIPT*", em Proc. *IEEE 30th Annual International Symposium on Personal Indoor and Mobile Radio Communications* (PIMRC), Istambul, Turquia, Setembro, 2019.
- E. N. Egashira, E. E. Benitez Olivo, e D. P. Moya Osorio,"*Desempenho de outage de sigilo para redes AF com relay não confiável usando WET e jamming baseados no destino*", em Proc. XXXVII Simpósio Brasileiro de Telecomunicações (SBrT), Petrópolis, Brasil, Outubro, 2019.

SUMÁRIO

1 INTRODUÇÃO

1.1 Contexto

O conjunto de especificações IMT-2020 (*International Mobile Telecommunications*-2020) define os requerimentos para a quinta geração (5G) de sistemas móveis celulares. As principais especificações consistem em alcançar maiores taxas de dados, fazendo parte dos serviços de eMBB (*enhanced mobile broadband*); fornecer suporte a um número massivo de dispositivos em uma área limitada, fazendo parte dos serviços de mMTC (*massive machine-type communications*); e atender serviços que requerem uma comunicação ultra confiável de baixíssima latência, fazendo parte dos serviços de URLLC (*ultra-reliable and low-latency communications*) [1, 2]. Considerando as três principais vertentes, as redes 5G são essenciais para atender as demandas de novos paradigmas, tais como a Internet das Coisas (IoT, *Internet of Things*), que consiste em uma infraestrutura de rede dinâmica e global com capacidades autoconfiguráveis, na qual os mais diversos dispositivos do mundo físico estarão conectados à Internet, coletando e compartilhando informação de forma inteligente [3, 4, 5].

A devida implementação das redes 5G em IoT permitirá concretizar diversas aplicações, promovendo uma evolução tecnológica para sociedades e economias atuais. Algumas das aplicações incluem o suporte ao uso de dados criados por veículos conectados, fazendo parte da Internet dos Veículos (IoV, *Internet of Vehicles*), assim como *smart homes*, cidades inteligentes, veículos aéreos não tripulados (VANTs). Todas as aplicações mencionadas precisarão de maior segurança para serem devidamente implementadas [1, 2]. Por outro lado, apesar de todas as vantagens que as novas aplicações podem trazer, estes dispositivos conectados à Internet possuem tanto limitações computacionais quanto em tempo de duração de bateria. Para tanto, estratégias baseadas em segurança na camada física (PLS, *physical layer security*) e de transferência de energia sem fio (WET, *wireless energy transfer*), por meio de sinais de radiofrequência (RF), podem ser exploradas de forma a contornar tais limitações, promovendo melhores cenários que aproveitam melhor as propriedades físicas dos canais sem fio.

A seguir, objetiva-se descrever os principais fundamentos básicos utilizados nesta dissertação. Para tanto, são descritos os principais conceitos relativos a comunicações cooperativas, técnicas de PLS e estratégias WET.

1.2 Fundamentos Básicos

1.2.1 Segurança na Camada Física

No contexto das redes 5G, uma das principais preocupações está diretamente relacionada à segurança de informações confidenciais a serem transmitidas em redes sem fio, tais como dados de cartão de crédito, mensagens de controle de sensores críticos, ou até mesmo dados de saúde (*e-health data*), que são dados de todos os registros de medicamentos tomados, doenças, histórico de lesões e até resultados de exames. Nessas aplicações de redes do tipo mMTC, técnicas tradicionais de criptografia e protocolos de autenticação consolidados podem ser inviáveis para implementar em um número massivo de dispositivos [6], os quais possuem limitações computacionais, de potência e armazenamento de dados, aumentando drasticamente a complexidade da implementação de protocolos de encriptação e decriptação [7, 8]. Recentemente, uma nova abordagem para complementar a segurança das redes de nova geração tem emergido a partir dos fundamentos da teoria da informação [6, 9]. Essa abordagem é referida como PLS, que consiste em explorar as propriedades físicas do canal sem fio, tais como os fenômenos de desvanecimento e interferência, para oferecer um nível adicional de proteção além dos esquemas de segurança existentes.

Inicialmente, PLS foi introduzido por C. E. Shannon em 1949, na qual foi definida a noção de sigilo perfeito na perspectiva da camada física [10]. Para isso, um modelo de sistema baseado em uma chave compartilhada entre dois usuários legítimos foi proposto, na qual foi assumido que a mensagem encriptada é transmitida através de um canal sem ruído e que o espião possui capacidade computacional ilimitada. Como conclusão, foi determinado que o sigilo perfeito é garantido se a chave secreta tem um comprimento maior ou igual a mensagem encriptada.

Posteriormente, com base nas noções abordadas por C. E. Shannon, em [11] foi proposto um modelo que assume canais sem memória, em que a fonte legítima (Alice) poderia enviar um sinal de *broadcast* com a mensagem encriptada para o destino legítimo (Bob), de forma que o espião (Eve) não consiga obter nenhuma informação sobre a mensagem enviada. Nesse modelo, foi mostrado que se o sinal obtido pelo espião for uma versão degradada do sinal recebido pelo destino legítimo, é possível atingir uma capacidade de sigilo não nula. A taxa de sigilo referida é determinada como a taxa de transmissão máxima alcançável com sigilo perfeito sem o uso de compartilhamento de chaves secretas. Adicionalmente, o modelo de canal Gaussiano é investigado sob a presença de um espião em [12], no qual foi definida a capacidade de sigilo como a diferença entre as capacidades do canal legítimo e do canal de escuta, dada por

$$\begin{aligned} C_s &= [C_\ell - C_e]^+ \\ &= \frac{1}{2}\left[\log_2(1+\Gamma_\ell) - \log_2(1+\Gamma_e)\right]^+ \end{aligned}$$

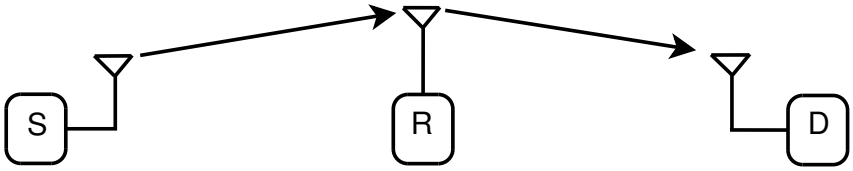

Figura 1 - Rede cooperativa de três nós, composta por uma fonte (S), retransmissor (R) e destino (D). Fonte: Elaborada pelo autor.

$$= \frac{1}{2}\log_2\left(\frac{1+\Gamma_\ell}{1+\Gamma_e}\right), \tag{1}$$

em que, Γ_ℓ e Γ_e são as relações sinal-ruído recebidas no enlace direto e no enlace de escuta, respectivamente, e o operador $[c]^+ \triangleq \max\{0,c\}$. Desta forma, a capacidade de sigilo é um valor positivo ou nulo. Por outro lado, em [13], foram introduzidos os conceitos de capacidade de sigilo em termos da probabilidade de *outage* de sigilo para redes com canais com desvanecimento quase-estático do tipo Rayleigh. A probabilidade de *outage* de sigilo é definida como a probabilidade de que a capacidade de sigilo em (1) seja menor que uma taxa de sigilo alvo R. Assim, ela é dada por

$$P_{\text{sout}} = \Pr\left(C_s < R\right), \tag{2}$$

ou seja, é a probabilidade da capacidade de sigilo instantânea ser menor que a taxa de sigilo alvo, de tal forma que $R > 0$.

A seguir, são apresentados conceitos de comunicações cooperativas, incluindo os principais protocolos de retransmissão utilizados.

1.2.2 Comunicações Cooperativas

Em um sistema de comunicação sem fio típico, o processo de comunicação acontece entre usuários de forma direta, como por exemplo, uma comunicação entre a fonte e destino. Comunicações cooperativas consistem na existência de um nó intermediário denominado retransmissor (R), cujo intuito é auxiliar na comunicação entre fonte (S) e destino (D), melhorando o desempenho do sistema em termos de confiabilidade e extensão de cobertura. Na Fig.1 mostra o modelo do sistema com um retransmissor. Em [14, 15] são mostradas as vantagens que as comunicações cooperativas podem oferecer, tais como o desempenho em termos da confiabilidade na transmissão de informação a partir da fonte e a extensão de cobertura. Em [15], os principais protocolos relacionados à comunicação cooperativa para a retransmissão de mensagens são propostos, sendo eles: o amplifica-e-encaminha (AF, *amplify-and-forward*) e decodifica-e-encaminha (DF, *decode-and-foward*). No protocolo AF, primeiramente o retransmissor amplifica o sinal recebido e em seguida envia este sinal amplificado para o destino, enquanto no protocolo DF, o retransmissor decodifica a mensagem recebida em uma primeira instância, re-

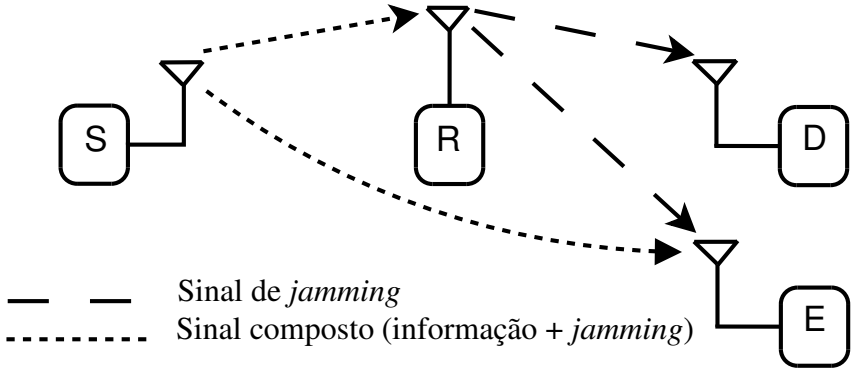

Figura 2 - Rede cooperativa utilizando a técnica SBJ. Fonte: Elaborada pelo autor.

genera e recodifica o sinal antes de enviá-lo para o destino.

Na próxima seção, a técnica de interferência intencionada cooperativa (CJ, *cooperative jamming*), considerando uma rede cooperativa com a presença de um espião é apresentada. Para tanto, são apresentadas as técnicas de *jamming* baseado na fonte e *jamming* baseado no destino.

1.2.3 *Jamming* Cooperativo

Em épocas passadas, especificamente em guerras, o termo referente ao sinal de interferência intencionada (*jamming*) se referia a uma interferência destrutiva, onde seu propósito era enganar o inimigo com o envio de sinais providos de falsas informações, de forma a garantir vantagens para tropas aliadas. As técnicas de *jamming* cooperativo consistem no envio de um sinal de interferência com o propósito de manter o sigilo da comunicação entre usuários legítimos. Para tanto, as principais técnicas relacionadas ao CJ são: *jamming* baseado na fonte (SBJ, *source-based jamming*) e *jamming* baseado no destino (DBJ, *destination-based jamming*).

- ***Jamming* Baseado na Fonte**

  Na Fig. 2 é mostrado um exemplo de uma rede cooperativa, composta por uma fonte (S), um retransmissor (R), um destino (D) e um espião (E), onde a técnica SBJ é usada. A fonte transmite um sinal de *jamming* durante a fase de transmissão de informação. Neste processo, a comunicação ocorre da seguinte forma: S envia um sinal composto (informação + *jamming*) para o retransmissor, que também é recebido pelo espião. Em seguida, o retransmissor recebe o sinal da fonte e retransmite para o destino, usando o protocolo AF (no protocolo DF, o retransmissor decodificaria o sinal recebido e retransmitiria o sinal já regenerado e sem o *jamming* para os nós D e E, inviabilizando a utilização deste protocolo). Ambos os nós D e E receberão o sinal composto de informação e *jamming*. Porém, utilizando a premissa que D tem conhecimento prévio do sinal de *jamming*, por

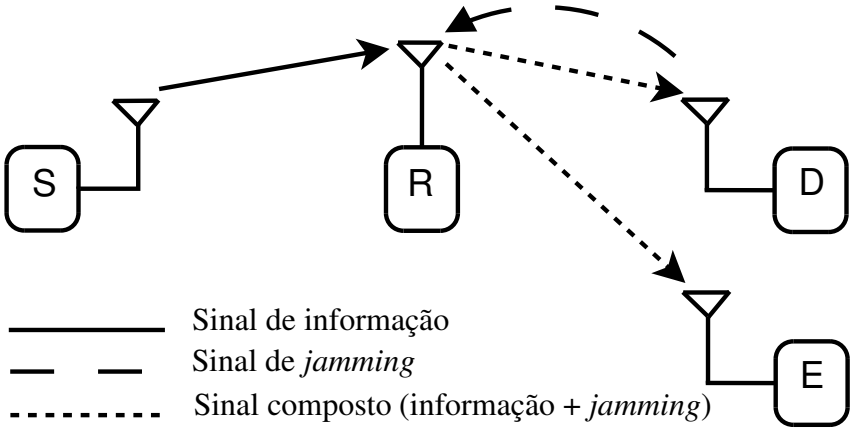

Figura 3 - Rede cooperativa utilizando a técnica DBJ. Fonte: Elaborada pelo autor.

meio da sinalização de rede, este nó consegue recuperar o sinal de informação a partir do sinal composto por meio de cancelamento.

- ***Jamming* Baseado no Destino**

  Na Fig. 3 é mostrado um exemplo de uma rede cooperativa, composta por uma fonte (S), um retransmissor (R), um destino (D) e um espião (E) em que a técnica DBJ é usada, ou seja, o destino é o encarregado de transmitir o sinal de *jamming* durante a fase de transmissão de informação. Neste caso, a comunicação ocorre da seguinte forma: enquanto a fonte envia o sinal de informação ao retransmissor, o destino envia também um sinal de *jamming*. Em seguida, utilizando o protocolo AF, o retransmissor transmite a versão amplificada dos sinais recebidos (informação + *jamming*) ao destino e espião. Dado que o destino é o responsável pela transmissão do sinal de *jamming*, este nó consegue recuperar o sinal de informação.

A seguir, apresenta-se a técnica de transferência simultânea de informação e potência sem fio (SWIPT, *simultaneous wireless and information power transfer*) e os principais protocolos que possibilitam a implementação desta técnica.

1.2.4 *Simultaneous Wireless and Information Power Transfer*

Junto aos requerimentos de segurança para redes 5G, os requerimentos como a demanda de altas taxas de dados e o suporte a um número massivo de dispositivos mostram a necessidade de adotar redes com alta eficiência energética [16]. Para isso, técnicas que dotam a sustentabilidade energética aplicadas a redes 5G têm sido propostas [17]. Nesse contexto, a técnica conhecida como captação de energia (EH, *energy harvesting*) tem-se mostrado promissora para atingir os requerimentos de eficiência energética para redes 5G. EH consiste na obtenção de energia elétrica a partir de outros tipos de fonte de energia, tais como energia térmica, eólica, cinética,

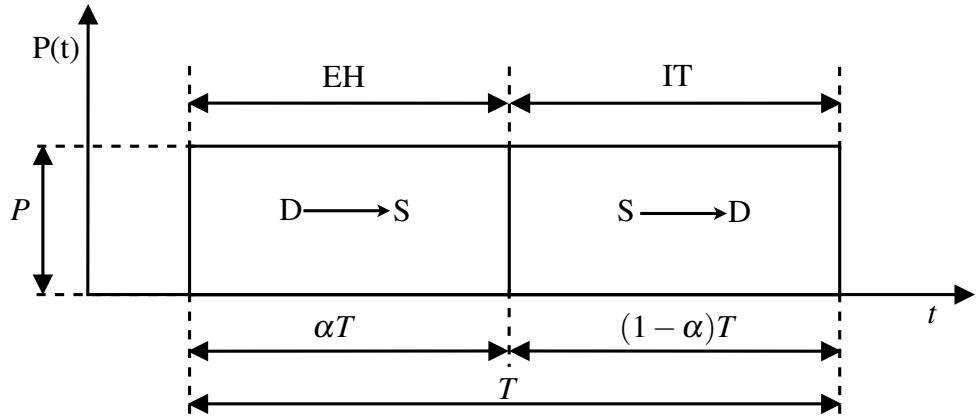

Figura 4 - Gráfico explicativo para o funcionamento da abordagem de SWIPT em uma rede ponto-a-ponto utilizando a comutação no tempo. Fonte: Elaborada pelo autor.

solar ou por sinais de RF [18, 19]. Dentre essas fontes externas, a captação de energia por sinais RF vindos de dispositivos remotos, conhecida como transferência de energia sem fio, pode ajudar a atender os requisitos de eficiência energética das redes do tipo mMTC. Adicionalmente, o SWIPT tem mostrado grande potencial, oferecendo ganhos de eficiência espectral e latência, além de eficiência energética [20]. A implementação de um sistema SWIPT implica na divisão da energia do sinal recebido em duas partes distintas: uma para o EH e outra para a transmissão de informação (IT, *information transmission*). Os principais protocolos SWIPT são: comutação no tempo (*time switching*) e divisão de potência (*power splitting*).

- **Comutação no Tempo**

  A Fig. 4 mostra um gráfico de potência em função do tempo, no qual é apresentado o processo de comunicação de uma rede ponto-a-ponto composta por dois nós, uma fonte (S) e um destino (D). Considera-se que a fonte é um dispositivo com limitações de energia, energizado pelo destino. Utilizando a abordagem de *time switching*, durante o intervalo de tempo αT, o destino energiza a fonte através de sinais RF e, posteriormente, durante o intervalo de tempo $(1-\alpha)T$, com a energia armazenada durante a fase de EH, ocorre o processo de transmissão do sinal de informação a partir da fonte. Note que α é um fator de alocação de tempo entre as fases de EH e IT, onde $0 < \alpha < 1$. Durante todo o processo, é adotado um mesmo nível de potência P.

  A Fig. 5 mostra um gráfico de potência em função do tempo para o processo de comunicação em uma rede cooperativa de três nós, fonte (S), retransmissor (R) e destino (D). Assume-se que apenas R é um dispositivo com restrições de energia e considera-se que S é o responsável pela energização deste dispositivo. Assim o processo de comunicação acontece da seguinte forma: durante o intervalo de tempo αT, S energiza R por sinais de RF e, posteriormente, ocorre o processo de transmissão de informação. O intervalo de tempo total alocado para tal processo é de $(1-\alpha)T$, sendo metade deste intervalo de

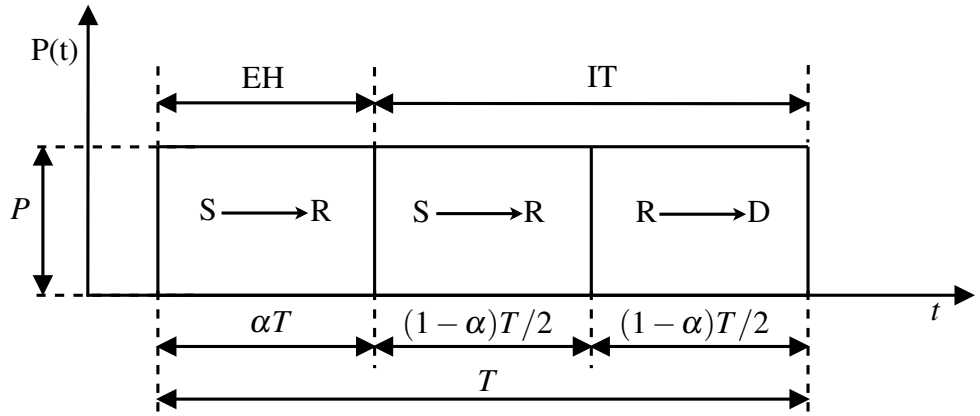

Figura 5 - Gráfico explicativo para o funcionamento da abordagem de SWIPT em uma rede cooperativa utilizando a comutação no tempo. Fonte: Elaborada pelo autor.

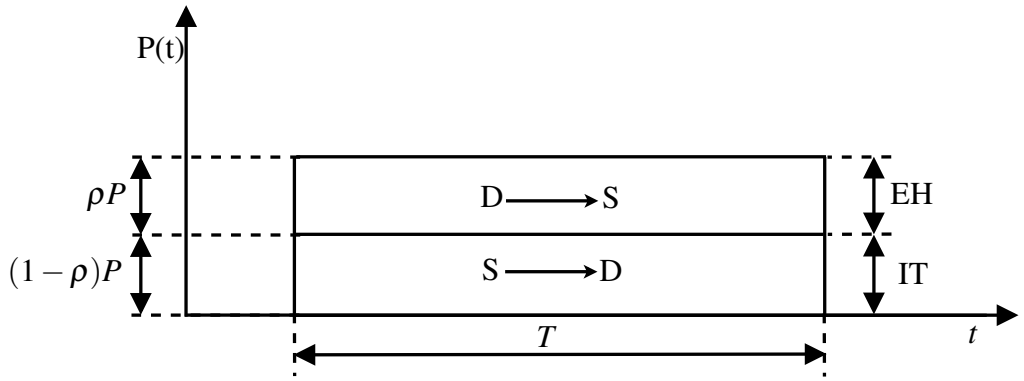

Figura 6 - Gráfico explicativo para o funcionamento da abordagem de SWIPT por divisão de potência. Fonte: Elaborada pelo autor.

tempo alocado para a transmissão de informação de S para R e a outra metade alocada para a transmissão de R para D.

- **Divisão de Potência**

  Na Fig. 6, ilustra-se um gráfico de potência em função do tempo para o processo de comunicação em uma rede ponto-a-ponto composta por uma fonte (S) e um destino (D). Assume-se que a fonte é um dispositivo com restrições de energia, sendo assim energizado pelo destino. Para a divisãode potência, percebe-se que no intervalo de tempo total de bloco, T, acontece a captação de energia em D e a transmissão de informação a partir de S ao mesmo tempo, porém com níveis de potência distintos. A potência total disponível é dividida em dois níveis de potência: ρP para EH, e $(1-\rho)P$ para IT, sendo ρ um fator de alocação de potência entre as fases de EH e IT , na qual $0 < \rho < 1$.

  Na Fig. 7, é mostrado um gráfico de potência em função do tempo, para fins de comparação do processo de comunicação que acontece com a abordagem *power splitting*, considerando uma rede cooperativa de dois saltos, composta por uma fonte (S), um retransmissor (R) e um destino (D). Assume-se que R é um dispositivo com restrições de

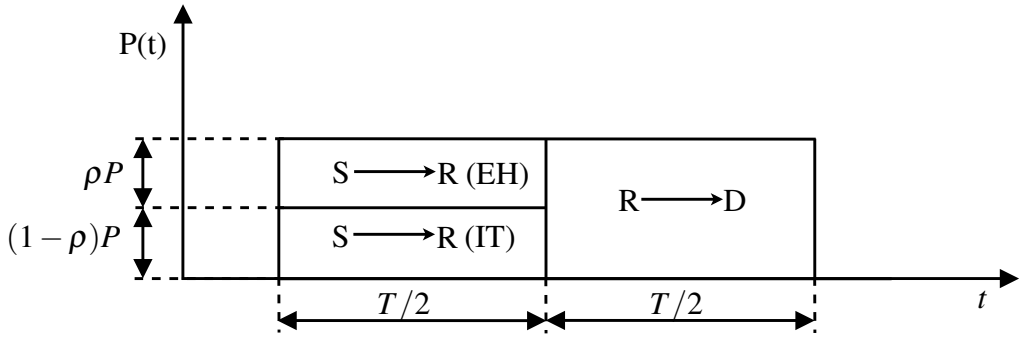

Figura 7 - Gráfico explicativo para o funcionamento da abordagem de SWIPT em uma rede cooperativa utilizando a divisão de potência. Fonte: Elaborada pelo autor.

energia e o nó S o energiza. O processo de comunicação ocorre da seguinte forma: durante o intervalo de tempo $T/2$, ocorre ao mesmo tempo a energização do retransmissor através de sinais RF vindos da fonte e a transmissão de informação de S para R, porém com níveis de potência distintos. Para EH, é alocado uma porção de potência ρP, e para IT é alocado uma porção $(1-\rho)P$. Por fim, no outro intervalo de tempo $T/2$ ocorre a transmissão de informação do retransmissor para o destino.

Na próxima seção, são apresentados alguns trabalhos relacionados aos cenários de rede sem fio que se aproveitam de uma ou mais das técnicas apresentadas anteriormente.

1.3 Trabalhos Relacionados

Diversas técnicas de comunicação cooperativa baseadas em retransmissores têm sido exploradas para melhorar o desempenho em termos da segurança em redes sem fio. Particularmente, em [21], a probabilidade de *outage* de sigilo foi investigada para uma rede cooperativa de múltiplos retransmissores, onde um esquema de seleção oportunista do retransmissor foi usado para garantir o sigilo da comunicação. Em [22], a técnica de *jamming* cooperativo foi usada para melhorar a segurança em redes com restrições de sigilo. Nessa técnica, um nó da rede, possivelmente um retransmissor, envia um sinal de interferência intencionada para os espiões, de modo a prevenir que estes espiões consigam extrair informação das mensagens proveniente da comunicação entre os usuários legítimos. Em [23], um esquema de alocação de potência baseado na técnica DBJ foi investigado considerando um sistema composto por uma fonte, múltiplos retransmissores, um destino e um espião. O critério de seleção do retransmissor considerado foi o esquema de seleção parcial, que por sua vez, visa a escolha do retransmissor que tem o melhor desempenho da SNR no enlace do segundo salto. O desempenho da capacidade de sigilo foi avaliado em termos da quantidade dos retransmissores e do fator de alocação de potência. Em [24], a segurança na camada física de um sistema composto por múltiplas fontes e múltiplos retransmissores foi investigada, analisando o compromisso entre segurança e con-

fiabilidade (SRT, *security-reliability tradeoff*). A SRT é caracterizada pelas probabilidades de *outage* e interceptação, as quais são baseadas, respectivamente, na capacidade do canal legítimo até o destino e na capacidade do canal de escuta até o espião.

Entretanto, os benefícios de se utilizar técnicas de comunicações cooperativas baseadas em retransmissores nos cenários mencionados baseiam-se na premissa de que o retransmissor é confiável. Porém, estes retransmissores podem, eventualmente, vazar informações para seu próprio benefício, se tornando possíveis espiões. Nesse sentido, o estudo de cenários onde os retransmissores são *não confiáveis* tem chamado um alto interesse. Em [25], apresentou-se um cenário cooperativo com múltiplos retransmissores não confiáveis operando no protocolo AF. Nesse trabalho, foi provado que uma capacidade de sigilo positiva pode ser alcançada, independentemente da potência transmitida e condições do canal, porém, com a premissa de que exista um número considerável de retransmissores não confiáveis assistindo a comunicação entre a fonte e destino. Em [26], um limitante superior para a capacidade de sigilo é obtida, considerando uma rede cooperativa de dois saltos com a presença de um retransmissor não confiável. Para isso, a técnica de DBJ foi proposta, de forma a confundir o nó retransmissor e atingir uma taxa de sigilo não nula, como apresentado na Seção 1.2.3. Em [27], uma expressão analítica aproximada para a probabilidade de *outage* de sigilo de uma rede composta por múltiplos retransmissores AF não confiáveis utilizando a técnica DBJ foi derivada, ainda que nesse caso foram explorados os benefícios de aproveitar o enlace de transmissão direta entre os usuários legítimos fonte e destino. Em [28], foi proposto um sistema similar com múltiplas antenas no destino. Os resultados mostraram o ganho de diversidade que este sistema pode oferecer, ao utilizar a técnica de seleção ótima de antena.

Por outro lado, diversos trabalhos que consideram um contexto de redes cooperativas com restrições de energia também têm sido estudados [29, 30, 31, 32, 33, 34]. Em [29], três esquemas de WET considerando uma rede cooperativa com um retransmissor confiável são analisados, na qual parâmetros de sistema ótimos são fornecidos de modo a maximizar a taxa de transferência de informação. A partir da suposição de que o retransmissor é um dispositivo com restrições de energia, cada esquema WET proposto consiste na energização do retransmissor através de sinais de RF a partir da fonte (S-WET, *source wireless power transfer*), a partir do destino (D-WET, *destination wireless power transfer*), e a partir de ambos os nós, fonte e destino (SD-WET, *source destination wireless power transfer*). Já em [30], a probabilidade de *outage* de sigilo de uma rede com o esquema S-WET utilizando *power-splitting*, e composto por múltiplos retransmissores não confiáveis com restrições de energia operando no protocolo AF foi analisada. Também, uma nova técnica de *jamming* foi proposta, onde um nó externo (*John*) e o nó de destino (Bob) transmitem sinais de interferência intencionada aos retransmissores de forma a proteger a informação confidencial provida pela fonte (Alice). Os autores concluíram que a segurança no modo de transmissão através do enlace de *relaying* é comprometida quando os retransmissores são localizados próximos à fonte ou destino. Em [31], foi proposto um al-

goritmo de otimização para maximizar a taxa de sigilo alcançável em termos da política de uso do *power splitting*. Para isso, foi analisada a estratégia SD-WPT usando SWIPT através de *power splitting* em uma rede cooperativa de três nós com um retransmissor não confiável. Para prevenir que o retransmissor espione a informação confidencial, a técnica DBJ foi empregada. Em [32], um compromisso entre o consumo de energia e a segurança na camada física sobre uma rede composta por múltiplos retransmissores não confiáveis foi analisado. Nesse esquema, empregou-se a técnica SBJ para melhorar o desempenho de sigilo do sistema. Em [33], os autores mostraram a comparação do desempenho de sigilo sobre as políticas de uso de SWIPT, usando *time switching* e *power splitting*, junto à estratégia S-WET. Além disso, considerou-se uma rede cooperativa de três nós com um retransmissor não confiável e utilizou-se a técnica DBJ. Com uma metodologia similar a [33], em [34] foi feito um comparativo entre as políticas de *time switching* e *power splitting* baseados no esquema de energização conjunta SD-WET. Nesse estudo, o sistema consistiu em uma rede cooperativa de dois saltos, incluindo um retransmissor não confiável e múltiplos destinos com múltiplas antenas. Para tanto, uma estratégia de *beamforming* foi aplicada no destino, alcançando sistemas de comunicações mais seguros.

Apesar de todos esses cenários analisados até o momento, muitos outros permanecem inexplorados. Nesse sentido, apresenta-se as contribuições deste trabalho.

1.4 Contribuições

No presente trabalho é investigado o desempenho de *outage* de sigilo de uma rede composta por uma fonte, um destino e um retransmissor não confiável operando no protocolo AF e em modo de retransmissão HD. Para evitar que o retransmissor espione as mensagens confidenciais provenientes da fonte, a técnica DBJ é adotada. Além disso, considera-se que o retransmissor é um dispositivo com restrições de energia, e para isso, três estratégias baseadas em *time switching* são consideradas, a saber: S-WET, D-WET e SD-WET, que serão apresentadas no seguinte capítulo. Para este cenário, analisa-se a probabilidade de *outage* de sigilo considerando parâmetros chave do sistema, tais como o fator de alocação de potência entre fonte e destino para a fase de IT, fator de alocação de tempo entre as fases de EH e IT, e a posição relativa do retransmissor entre fonte e destino. A seguir, são apresentadas as principais contribuições:

- Expressões analíticas assintóticas em forma fechada para a probabilidade de *outage* de sigilo são derivadas para as três estratégias de energização do retransmissor, as quais são validadas através de simulações de Monte Carlo;
- Resultados numéricos são ilustrados para mostrar o impacto sobre o desempenho de sigilo dos seguintes parâmetros: fator de alocação de potência entre a fonte e o destino durante o primeiro subintervalo da fase de IT, fator de alocação de tempo entre as fases de EH,

IT, posição relativa do retransmissor entre fonte e destino e fator de alocação de potência fara a fase de EH, especificamente para o caso SD-WET;

- Um comparativo da probabilidade de *outage* de sigilo entre as estratégias S-WET, D-WET e SD-WET é realizado, fornecendo critérios de projeto para redes seguras com eficiência energética.

Parte das contribuições deste trabalho, referente às estratégias S-WET e D-WET, resultou na publicação dos artigos [35] e [36], respectivamente. A autorização para reprodução de conteúdo está anexada no Apêndice A. A seguir é apresentada a organização do trabalho.

1.5 Organização do Trabalho

O presente trabalho é apresentado em cinco capítulos, mostrados a seguir:

- O Capítulo 2 apresenta o modelo do sistema proposto considerando as estratégias de energização do retransmissor através da fonte, energização do retransmissor através do destino e energização do retransmissor a partir da fonte e destino. Para cada estratégia, é apresentado o modelo de sinais correspondente;
- No Capítulo 3, uma análise da probabilidade de *outage* de sigilo para as três estratégias é realizada;
- O Capítulo 4 apresenta os resultados numéricos obtidos da avaliação da probabilidade de *outage* de sigilo, determinando alguns critérios para atingir comunicações mais seguras e de maior eficiência energética;
- Por fim, no Capítulo 5 as conclusões finais são apresentadas junto com as propostas de trabalhos futuros.

2 MODELO DE SISTEMA E SINAIS

2.1 Modelo de Sistema

O modelo do sistema considerado é uma rede cooperativa de dois saltos composta por uma fonte (S), um destino (D) e um relay (R), operando sob o protocolo AF e em modo HD, como ilustrado na Fig. 8. Todos os nós são considerados como dispositivos de antena única e operam em acesso múltiplo por divisão de tempo (TDMA, *time division multiple access*), ou seja, cada usuário pode acessar o canal em intervalos de tempo distintos. Também é considerado que a comunicação entre S e D somente poderá acontecer através do enlace de retransmissão, S$\rightarrow$R$\rightarrow$D.

Adicionalmente, nesse sistema, considera-se que todos os canais estão sujeitos a desvanecimento quase-estático e plano do tipo Rayleigh e a ruido aditivo gaussiano e branco (AGWN, *additive white Gaussian noise*) com potência média N. Consequentemente, os coeficientes de canal correspondentes aos enlaces S$\rightarrow$R e R$\rightarrow$D, denotados, respectivamente, por h_i, para $i \in \{\mathrm{SR}, \mathrm{RD}\}$, são modelados como variáveis aleatórias independentes, gaussianas complexas e circularmente simétricas de média zero, ou seja, $h_i \sim CN(0, \Omega_i)$, em que $\Omega_i = \mathrm{E}\{|h_i|^2\}$ é a potência média do canal. Consequentemente, os ganhos de canal, dados por $g_\mathrm{i} \triangleq |h_\mathrm{i}|^2$, seguem uma distribuição exponencial de média Ω_i, para i $\in \{\mathrm{SR}, \mathrm{RD}\}$.

A Fig. 9 ilustra o bloco de transmissão no domínio do tempo, baseado na técnica *time switching*. Assume-se que o intervalo total de tempo é T, dividido em duas fases: EH e IT. Na primeira fase, R armazena energia vindo de outro nó da rede (S, D, ou ambos, a depender da estratégia WET considerada, como ilustrado na Fig. 8(a), Fig. 8(b) e Fig. 8(c), respectivamente), durante o intervalo de tempo αT, sendo α o fator de alocação de tempo entre as fases de EH e IT, onde $\alpha \in (0,1)$. Na segunda fase, o tempo restante $(1-\alpha)T$ é dividido em dois subintervalos de tempo iguais. O primeiro subintervalo de tempo é alocado para a transmissão de informação da fonte para o retransmissor, ao mesmo tempo em que D envia um sinal de *jamming* para R, de forma que R não consiga extrair informação sigilosa. Para este propósito, a potência total disponível para a fase de IT, P, é alocada entre os nós S e D segundo um fator de alocação de potência $\delta \in (0,1)$. Assim, durante o segundo subintervalo de tempo referente a segunda fase, o nó R envia a D uma versão amplificada de um sinal composto pelos sinais recebidos de informação e *jamming*, usando a energia armazenada durante a primeira fase. Assume-se que o sinal de *jamming* é perfeitamente conhecido por D, tal que este pode efetivamente cancelá-lo do sinal composto recebido e recuperar o sinal de informação vindo de S.

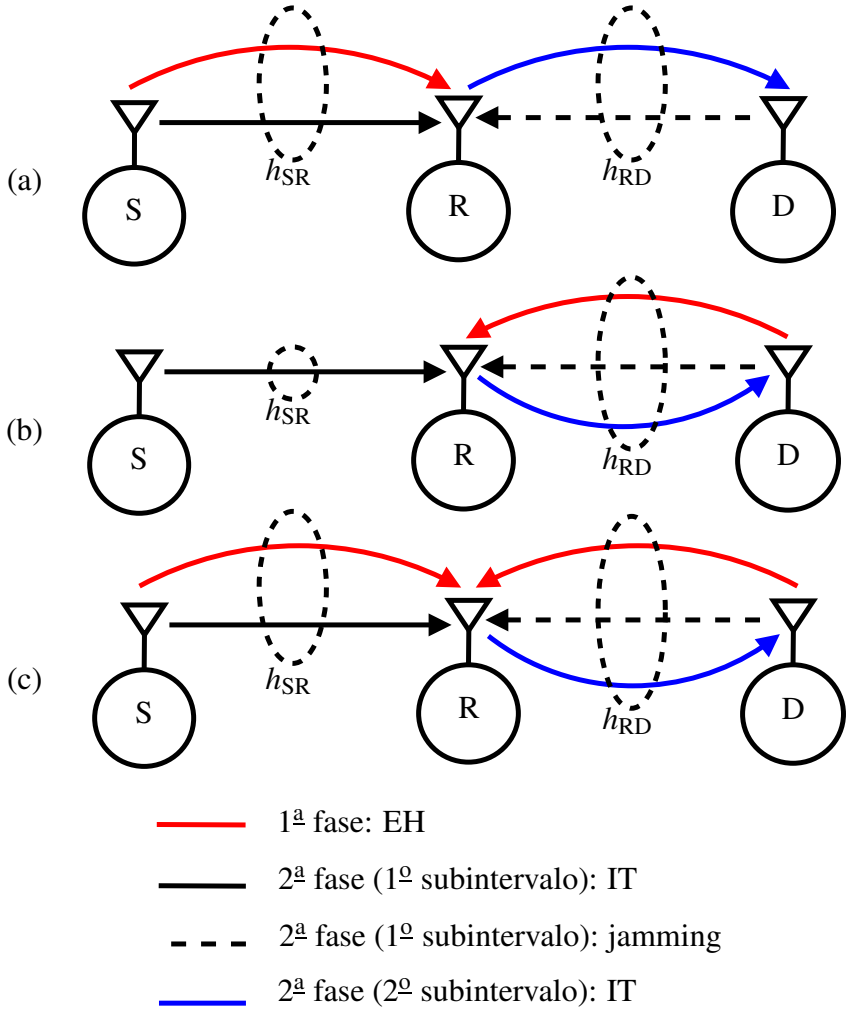

Figura 8 - Modelo do sistema consistindo por uma fonte, um destino e um retransmissor que opera em protocolo AF, considerando três estratégias distintas: (a) retransmissor energizado por sinais RF vindos de S; (b) retransmissor energizado por sinais RF vindos de D; e (c) retransmissor energizado por sinais RF vindos de S e D, simultaneamente. Fonte: Elaborada pelo autor.

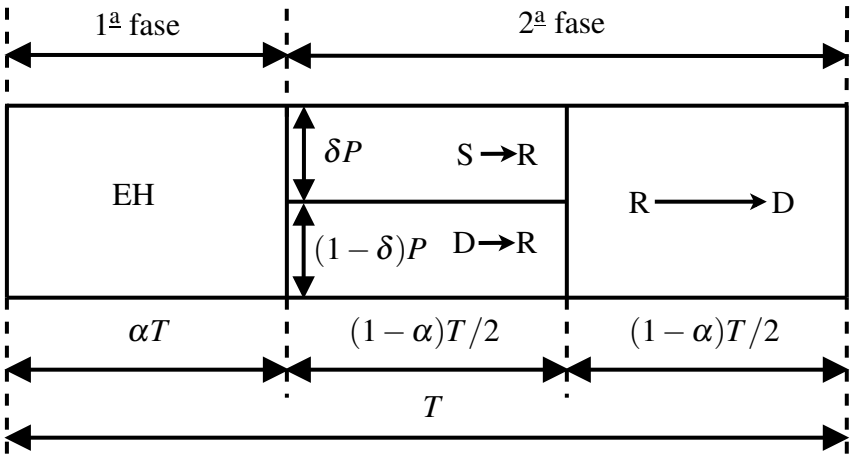

Figura 9 - Bloco de transmissão temporal referente ao protocolo *time switching*. Na 1ª fase, EH consiste nas estratégias S-WET, D-WET ou SD-WET, e na 2ª fase, refere-se a transmissão de informação, com duração total de $(1-\alpha)T$. Fonte: Elaborada pelo autor.

As SNRs transmitidas em S, R e D são denotadas por $\gamma_S = P_S/N$, $\gamma_R = P_R/N$, e $\gamma_D = P_D/N$, em que P_S, P_R, e P_D são as potências transmitidas em S, R, e D, respectivamente. Considera-se que a potência transmitida para a fase de EH é limitada a P, e para a fase de IT, a potência transmitida também é limitada a P. Portanto, a SNR transmitida total para cada fase é dada por $\gamma_P = P/N$.

Na sequência, são apresentadas as expressões para a potência transmitida em R, considerando os casos do retransmissor ser energizado por sinais de RF vindos de S, D ou ambos.

2.2 Estratégia S-WET

Fig. 8(a) ilustra a estratégia S-WET, onde R é energizado por sinais de RF providos do nó S. Nesta estratégia, a energia armazenada em R durante a primeira fase de EH é dado por

$$E_S = \eta \alpha T P g_{SR}, \tag{3}$$

em que $\eta \in (0,1)$ é o fator de eficiência de conversão de energia[1], portanto a potência transmitida em R é dada por

$$\begin{aligned} P_R &= \frac{E_S}{(1-\alpha)T/2} \\ &= \theta P g_{SR}, \end{aligned} \tag{4}$$

[1]O fator de eficiência de conversão de energia é a relação entre a energia de saída (utilizada) e a energia de entrada do sistema.

em que

$$\theta = \frac{2\alpha\eta}{1-\alpha}. \tag{5}$$

2.3 Estratégia D-WET

Em certos cenários em que o retransmissor está mais perto do destino, as condições de g_{SR} podem resultar em um processo de energização de R ineficaz. Para tanto, a estratégia D-WET, proposta na Fig. 8(b) é ilustrada, na qual R é energizado por D. Assim, a energia armazenada em R durante a primeira fase de EH é dada por

$$E_{\mathrm{D}} = \eta\alpha T P g_{\mathrm{RD}}, \tag{6}$$

De forma similar à estratégia S-WET, a potência transmitida em R é dada por

$$\begin{aligned} P_{\mathrm{R}} =& \frac{E_{\mathrm{D}}}{(1-\alpha)T/2} \\ =& \theta P g_{\mathrm{RD}}, \end{aligned} \tag{7}$$

em que foi substituído E_{D} por (6) e θ é dado por (5).

2.4 Estratégia SD-WET

Conforme a Fig. 8(c), é proposta uma estratégia de energização de R através de sinais de RF vindos de S e D, simultaneamente. Nesta estratégia, durante a primeira fase de EH, é considerado que a potência transmitida do sistema P é alocada para S e D utilizando um fator de alocação de potência $\mu \in (0,1)$. Assim, a energia armazenada em R é dada por

$$E_{\mathrm{SD}} = \eta\alpha T[P\mu g_{\mathrm{SR}} + P(1-\mu)g_{\mathrm{RD}}]. \tag{8}$$

A partir de algumas manipulações, a potência transmitida em R é dada por

$$\begin{aligned} P_{\mathrm{R}} =& \frac{E_{\mathrm{SD}}}{(1-\alpha)T/2} \\ =& \theta P[\mu g_{\mathrm{SR}} + (1-\mu)g_{\mathrm{RD}}], \end{aligned} \tag{9}$$

sendo θ dado por (5).

A seguir, a partir do modelo de sistema proposto anteriormente, será realizada uma análise de sinais e, na sequência, serão determinadas as SNRs do enlace legítimo e do enlace de escuta.

2.5 Modelo de Sinais

Durante o primeiro subintervalo de IT, o sinal recebido em R é dado por

$$y_{\mathrm{R}}(t) = \sqrt{P_{\mathrm{S}}} h_{\mathrm{SR}} s_{\mathrm{I}}(t) + \sqrt{P_{\mathrm{D}}} h_{\mathrm{RD}} s_{\mathrm{J}}(t) + n_{\mathrm{R}}(t), \tag{10}$$

em que $s_{\mathrm{I}}(t)$ é o sinal de informação vindo de S, $s_{\mathrm{J}}(t)$ é o sinal de *jamming* vindo de D, e $n_{\mathrm{R}}(t)$ é a componente do ruído em R. Assim, durante o segundo subintervalo de IT e considerando o protocolo de retransmissão AF, o sinal recebido em D vindo de R é dado por

$$y_{\mathrm{D}}(t) = \sqrt{P_{\mathrm{R}}} h_{\mathrm{RD}} G y_{\mathrm{R}}(t) + n_{\mathrm{D}}(t), \tag{11}$$

em que $n_{\mathrm{D}}(t)$ é a componente do ruído em D, e G é o fator de amplificação relativo ao protocolo AF. Note que G é obtido considerando sinais de potência normalizados, de tal forma que $\mathrm{E}\{|s_{\mathrm{I}}(t)|^2\} = \mathrm{E}\{|s_{\mathrm{J}}(t)|^2\} = 1$. Da mesma forma, para determinar G, é considerado que $\mathrm{E}\{|G y_{\mathrm{R}}(t)|^2\}=1$. Portanto, essa expressão é dada por

$$\mathrm{E}\left\{ |G|^2 \left| \left[\sqrt{P_{\mathrm{S}}} h_{\mathrm{SR}} s_{\mathrm{I}}(t) + \sqrt{P_{\mathrm{D}}} h_{\mathrm{RD}} s_{\mathrm{J}}(t) + n_{\mathrm{R}}(t) \right] \right|^2 \right\} = 1. \tag{12}$$

Resolvendo (12) e realizando algumas manipulações, o fator de amplificação G é obtido como

$$G = \sqrt{\frac{1}{P_{\mathrm{S}} g_{\mathrm{SR}} + P_{\mathrm{D}} g_{\mathrm{RD}} + N}}, \tag{13}$$

Assim, substituindo (10) em (11), o sinal recebido em D pode ser expresso como

$$y_{\mathrm{D}}(t_2) = \sqrt{P_{\mathrm{R}}} G h_{\mathrm{RD}} \left[\sqrt{P_{\mathrm{S}}} h_{\mathrm{SR}} s_{\mathrm{I}}(t_1) + \sqrt{P_{\mathrm{D}}} h_{\mathrm{RD}} s_{\mathrm{J}}(t_1) + n_{\mathrm{R}}(t_1) \right] + n_{\mathrm{D}}(t_2). \tag{14}$$

Como mencionado anteriormente, considerando que D é capaz de cancelar perfeitamente o sinal de *jamming* transmitido por ele mesmo na fase anterior, o sinal recebido em D é dado por

$$y_{\mathrm{D}}(t_2) = \sqrt{P_{\mathrm{R}}} G h_{\mathrm{RD}} \left[\sqrt{P_{\mathrm{S}}} h_{\mathrm{SR}} s_{\mathrm{I}}(t_1) + n_{\mathrm{R}}(t_1) \right] + n_{\mathrm{D}}(t_2). \tag{15}$$

Assim, a SNR recebida fim-a-fim no enlace legítimo pode ser obtido a partir de (15) como

$$\begin{aligned} \Gamma_{\ell} &= \frac{P_{\mathrm{S}} P_{\mathrm{R}} g_{\mathrm{SR}} g_{\mathrm{RD}} G^2}{P_{\mathrm{R}} g_{\mathrm{RD}} G^2 N + N} \\ &\overset{(a)}{=} \frac{P_S P_R g_{\mathrm{SR}} g_{\mathrm{RD}}}{P_{\mathrm{R}} g_{\mathrm{SR}} g_{\mathrm{RD}} N + P_{\mathrm{S}} g_{\mathrm{SR}} N + P_{\mathrm{D}} g_{\mathrm{RD}} N + N^2} \\ &\overset{(b)}{=} \frac{\gamma_{\mathrm{S}} \gamma_{\mathrm{R}} g_{\mathrm{SR}} g_{\mathrm{RD}}}{\gamma_{\mathrm{R}} g_{\mathrm{RD}} + \gamma_{\mathrm{S}} g_{\mathrm{SR}} + \gamma_{\mathrm{D}} g_{\mathrm{RD}} + 1}, \end{aligned} \tag{16}$$

onde no passo (a) foi substituído G por (13) e realizadas diversas manipulações matemáticas. No passo (b), numerador e denominador foram divididos por N^2 e as definições das SNRs

transmitidas em S, R e D foram usadas.

Finalmente, a SNR recebida no retransmissor não confiável pode ser obtida baseado no sinal recebido em R durante o primeiro subintervalo da segunda fase. Assim, a SNR recebida no enlace de escuta é determinada a partir de (10) como

$$\begin{aligned}\Gamma_e &= \frac{P_{\mathrm{S}} g_{\mathrm{SR}}}{P_{\mathrm{D}} g_{\mathrm{RD}} + N} \\ &= \frac{\gamma_{\mathrm{S}} g_{\mathrm{SR}}}{\gamma_{\mathrm{D}} g_{\mathrm{RD}} + 1}.\end{aligned} \tag{17}$$

No próximo capítulo, é apresentado o procedimento de obtenção da capacidade de sigilo do sistema proposto, assim como da probabilidade de *outage* de sigilo desse sistema.

3 PROBABILIDADE DE OUTAGE DE SIGILO

Nesta seção, são apresentadas as expressões analíticas da probabilidade de *outage* de sigilo para as estratégias propostas, nas quais o retransmissor não confiável é energizado por sinais de RF provenientes de S, D ou ambos. Baseando-se nos conceitos da capacidade de sigilo e probabilidade de *outage* de sigilo mencionadas na Seção 1.2.1, substituindo (16) e (17) em (2), a probabilidade de *outage* de sigilo pode ser expressa como

$$\begin{aligned} P_{\text{sout}} &= \Pr\left(\frac{1+\Gamma_\ell}{1+\Gamma_e} < 2^{2R} \stackrel{\Delta}{=} \tau\right) \\ &= \Pr\left(\frac{1+\frac{\gamma_{\text{S}}\gamma_{\text{R}}g_{\text{SR}}g_{\text{RD}}}{\gamma_{\text{R}}g_{\text{RD}}+\gamma_{\text{S}}g_{\text{SR}}+\gamma_{\text{D}}g_{\text{RD}}+1}}{1+\frac{\gamma_{\text{S}}g_{\text{SR}}}{\gamma_{\text{D}}g_{\text{RD}}+1}} < \tau\right). \end{aligned} \tag{18}$$

Como as três estratégias propostas possuem diferentes expressões de SNR transmitida em R, discute-se a probabilidade de *outage* de sigilo separadamente. Com isso, em (18), para cada caso foi substituído γ_{R} dado por (4), (7) e (9), divididos por N. Cabe mencionar que, para todos os casos, a análise exata da probabilidade de *outage* de sigilo se mostra um problema intricado, dado que a SNR transmitida em R depende de um ou mais ganhos de canal correspondentes ao primeiro e segundo saltos do enlace de retransmissão. Portanto, a partir de uma análise assintótica, foi possível obter expressões em forma fechada para todas as estratégias consideradas, as quais mostram ser bastante precisas em relação ao desempenho exato no regime de média-a-alta SNR. A partir destas considerações, o desenvolvimento matemático do desempenho de sigilo é apresentado a seguir.

3.1 Estratégia S-WET

Realizando algumas manipulações em (18), a probabilidade de *outage* de sigilo é expressa como

$$\begin{aligned} P_{\text{sout}} &= \Pr\left(1+\frac{\gamma_{\text{S}}\gamma_{\text{R}}g_{\text{SR}}g_{\text{RD}}}{\gamma_{\text{R}}g_{\text{RD}}+\gamma_{\text{S}}g_{\text{SR}}+\gamma_{\text{D}}g_{\text{RD}}+1} < \tau\left(\frac{\gamma_{\text{S}}g_{\text{SR}}+\gamma_{\text{D}}g_{\text{RD}}+1}{\gamma_{\text{D}}g_{\text{RD}}+1}\right)\right) \\ &\stackrel{(c)}{=} \Pr\left(1+\frac{\delta\theta\gamma_P^2 g_{\text{SR}}^2 g_{\text{RD}}}{\delta\gamma_P g_{\text{SR}}+g_{\text{RD}}[\theta\gamma_P g_{\text{SR}}+(1-\delta)\gamma_P]+1} < \tau\left(\frac{\delta\gamma_P g_{\text{SR}}+(1-\delta)\gamma_P g_{\text{RD}}+1}{(1-\delta)\gamma_P g_{\text{RD}}+1}\right)\right) \\ &\stackrel{(d)}{=} \Pr\left(1+\frac{\delta\theta\gamma_P g_{\text{SR}}^2 g_{\text{RD}}}{\delta g_{\text{SR}}+g_{\text{RD}}(\theta g_{\text{SR}}+1-\delta)} < \tau\left(\frac{\delta g_{\text{SR}}+(1-\delta)g_{\text{RD}}}{(1-\delta)g_{\text{RD}}}\right)\right), \end{aligned} \tag{19}$$

em que no passo (c), o termo γ_{R} foi substituído por $\theta\gamma_P g_{\text{SR}}$, sendo θ dado por (5), e os termos γ_{S} e γ_{D} substituídos por $\delta\gamma_P$ e $(1-\delta)\gamma_P$, respectivamente, e no passo (d) foi considerado um

regime de alta SNR, em que $\gamma_P \to \infty$. Por consequência, os termos $1/\gamma_P$ foram aproximados para um valor nulo, referente ao passo anterior. A expressão em (19) é o primeiro passo para a obtenção de uma expressão analítica para a probabilidade de *outage* de sigilo do sistema em análise, como apresentado na Proposição 1.

Proposição 1. *Uma expressão analítica em forma fechada obtida a partir de uma análise assintótica em alta SNR para a probabilidade de* outage *de sigilo de uma rede cooperativa com o retransmissor AF não confiável, utilizando DBJ e S-WET via protocolo time switching é dada por*

$$P_{\text{sout}} \simeq \sqrt{\frac{(1-\delta)(\tau-1)}{\delta\theta\gamma_P}}\left(\frac{1}{\Omega_{\text{SR}}}\right)+\sqrt{\frac{\delta\tau}{(1-\delta)\theta\gamma_P}}\left(\frac{1}{\Omega_{\text{RD}}}\right). \tag{20}$$

Demonstração. Vide Apêndice B. □

3.2 Estratégia D-WET

Considerando a estratégia de energização do retransmissor através de sinais de RF vindos de D, e também considerando um regime de alta SNR, foi aproximado o numerador da razão em $\Pr(\cdot)$, de (18) como a SNR recebida no enlace legítimo. Adicionalmente, realizando algumas manipulacões algébricas e utilizando o limitante superior para a média harmônica, ou seja, $\min\{A,B\} \geq AB/(A+B+1)$, a probabilidade de *outage* de sigilo é dada por

$$\begin{aligned}
P_{\text{sout}} &= \Pr\left(\frac{\frac{\gamma_{\text{R}}}{\gamma_{\text{R}}+\gamma_{\text{D}}}}{1+\frac{\gamma_{\text{S}}g_{\text{SR}}}{\gamma_{\text{D}}g_{\text{RD}}+1}}\min\{\gamma_{\text{S}}g_{\text{SR}},(\gamma_{\text{R}}+\gamma_{\text{D}})g_{\text{RD}}\}<\tau\right)\\
&\overset{(e)}{=}\Pr\left(\frac{\theta\gamma_P g_{\text{RD}}}{\theta\gamma_P g_{\text{RD}}+(1-\delta)\gamma_P}\min\{\delta\gamma_P g_{\text{SR}},[\theta\gamma_P g_{\text{RD}}+(1-\delta)\gamma_P]g_{\text{RD}}\}\right.\\
&\qquad\left.<\tau\left(\frac{(1-\delta)\gamma_P g_{\text{RD}}+1+\delta\gamma_P g_{\text{SR}}}{(1-\delta)\gamma_P g_{\text{RD}}+1}\right)\right)\\
&=\Pr\left(\frac{\theta\gamma_P g_{\text{RD}}}{\theta g_{\text{RD}}+1-\delta}\min\{\delta g_{\text{SR}},[\theta g_{\text{RD}}+(1-\delta)]g_{\text{RD}}\}<\tau\left(\frac{(1-\delta)g_{\text{RD}}+\frac{1}{\gamma_P}+\delta g_{\text{SR}}}{(1-\delta)g_{\text{RD}}+\frac{1}{\gamma_P}}\right)\right)\\
&\overset{(f)}{=}\Pr\left(\min\{\delta g_{\text{SR}},[\theta g_{\text{RD}}+(1-\delta)]g_{\text{RD}}\}<\tau\left(\frac{(1-\delta)g_{\text{RD}}+\delta g_{\text{SR}}}{(1-\delta)g_{\text{RD}}}\right)\left(\frac{\theta g_{\text{RD}}+1-\delta}{\theta\gamma_P g_{\text{RD}}}\right)\right),
\end{aligned} \tag{21}$$

em que no passo (e) foi substituído γ_{R} por (7) dividido por N, com θ expressado em (5), e os termos γ_{S} e γ_{D} substituídos por $\delta\gamma_P$ e $(1-\delta)\gamma_P$, respectivamente, e no passo (f) foi considerado um regime de alta SNR, que por sua vez, os termos $1/\gamma_P$ foram negligenciados. Assim, foi isolado o termo $\min\{\cdot,\cdot\}$, para possibilitar a análise das regiões de integração. Em seguida,

a expressão em (21) é o ponto de partida para a Proposição 2, que apresenta uma expressão analítica assintótica para a probabilidade de *outage* de sigilo.

Proposição 2. *Uma expressão analítica em forma fechada obtida a partir de uma análise assintótica em alta SNR para a probabilidade de* outage *de sigilo de uma rede cooperativa com o retransmissor AF não confiável, utilizando DBJ e D-WET via protocolo time switching é dada por*

$$P_{\text{sout}} \simeq \frac{\tau}{\delta\gamma_P\Omega_{\text{RD}}} + \left(\frac{\delta\tau\Omega_{\text{SR}}}{(1-\delta)\gamma_P\theta}\right)^{\frac{1}{3}} \frac{\Gamma(\frac{4}{3})}{\Omega_{\text{RD}}}. \tag{22}$$

Demonstração. Vide Apêndice C. □

3.3 Estratégia SD-WET

Baseado na estratégia de energização conjunta do retransmissor AF não confiável, ou seja, a energização por sinais de RF ocorre dos nós S e D simultaneamente, especificamente durante a fase de EH, partindo de (18), a probabilidade de *outage* de sigilo é obtida como

$$\begin{aligned} P_{\text{sout}} &\overset{(g)}{=} \Pr\left(\frac{\delta\theta\gamma_P g_{\text{SR}} g_{\text{RD}}[\mu g_{\text{SR}} + (1-\mu) g_{\text{RD}}]}{\delta g_{\text{SR}} + g_{\text{RD}}\left\{\theta[\mu g_{\text{SR}} + (1-\mu) g_{\text{RD}}] + (1-\delta) + \frac{1}{\gamma_P}\right\}}\right. \\ &\qquad \left. < \tau\left(\frac{\delta g_{\text{SR}} + (1-\delta) g_{\text{RD}} + \frac{1}{\gamma_P}}{(1-\delta) g_{\text{RD}} + \frac{1}{\gamma_P}}\right)\right) \\ &= \Pr\left(\frac{\delta\theta\gamma_P\mu g_{\text{SR}}^2 g_{\text{RD}} + \delta\theta\gamma_P(1-\mu) g_{\text{SR}} g_{\text{RD}}^2}{\delta g_{\text{SR}} + g_{\text{RD}}\{\theta[\mu g_{\text{SR}} + (1-\mu) g_{\text{RD}}] + (1-\delta)\}}\right. \\ &\qquad \left. < \tau\left(\frac{\delta g_{\text{SR}} + (1-\delta) g_{\text{RD}}}{(1-\delta) g_{\text{RD}}}\right)\right) \end{aligned} \tag{23}$$

em que no passo (g) foi realizado a substituição da SNR transmitida em R, γ_{R}, pela SNR transmitida utilizando a estratégia conjunta SD-WET, $\theta\gamma_P[\mu g_{\text{SR}} + (1-\mu) g_{\text{RD}}]$, sendo θ dado por (5). Além disso, o numerador e o denominador do argumento de $\Pr(\cdot)$ foi dividido por γ_P. Assim, a expressão assintótica em forma fechada para a probabilidade de *outage* de sigilo pode ser formulada conforme a proposição abaixo.

Proposição 3. *Uma expressão analítica em forma fechada obtida a partir de uma análise assintótica em alta SNR para a probabilidade de* outage *de sigilo de uma rede cooperativa com o retransmissor AF não confiável, utilizando DBJ e a estratégia conjunta de energização SD-WET via protocolo time switching é dada por*

$$P_{\text{sout}} \simeq \frac{\tau}{\delta\gamma_P\Omega_{\text{SR}}} + \frac{\tau\theta\mu + \sqrt{\tau^2\theta^2\mu^2 + 4\delta(1-\delta)\tau\theta\gamma_P\mu}}{2(1-\delta)\theta\gamma_P\mu\Omega_{\text{RD}}} \tag{24}$$

Demonstração. Vide Apêndice D. □

No capítulo a seguir, são apresentados alguns resultados numéricos, considerando o modelo do sistema proposto e as três estratégias de energização do retransmissor.

4 RESULTADOS NUMÉRICOS E DISCUSSÕES

A partir das expressões analíticas obtidas na seção anterior, o desempenho do sistema proposto em termos da probabilidade de *outage* de sigilo é avaliado e as expressões analíticas obtidas são validadas via simulações de Monte Carlo para diversos casos ilustrativos. As simulações de Monte Carlo permitem obter uma estimação assertiva de uma determinada probabilidade. Na execução dessas simulações foram considerados 10^6 experimentos, usando um computador com processador Intel (R) Core (TM) i5-7200U de 2,71 GHz e memória RAM de 4 GB.

Para este propósito, uma topologia de rede linear é considerada, onde as distâncias normalizadas entre S e R, entre R e D, e entre S e D são fixadas em $d_{\mathrm{SR}} = 0{,}5$, $d_{\mathrm{RD}} = 0{,}5$ e $d_{\mathrm{SD}} = 1$, respectivamente, a menos que indicado de outra forma. Considera-se que o ganho médio do canal de todos os enlaces é determinado pela perda de percurso, isto é, $\Omega_i = d_i^{-\beta}$, para $i \in \{\mathrm{SR}, \mathrm{RD}\}$, em que d_i é a distância entre dois nós e $\beta = 4$ é o expoente de perda de percurso (este valor foi utilizado em diversos trabalhos, como em [23, 27, 37]), e é usado para enformas urbanas [38]. Além disso, assume-se que a taxa de sigilo alvo é fixada em $R = 1$ bps/Hz e o fator de eficiência de energia é fixado em $\eta = 0{,}5$ (sendo um valor tipicamente utilizado em diversos trabalhos, por exemplo, [39, 40, 41]). A partir destes parâmetros, é analisado o desempenho de sigilo dos sistemas propostos, os quais consideram a energização do retransmissor através de sinais de RF vindos da fonte, do destino, e de ambos fonte e destino. Em seguida, os resultados referentes a uma comparação entre as três estratégias de energização propostas são apresentados.

4.1 Estratégia S-WET

A Fig. 10 mostra a probabilidade de *outage* de sigilo em função da SNR transmitida γ_P, para diferentes valores do fator de alocação de potência entre fonte e destino, δ. Nota-se que os resultados obtidos da avaliação da expressão assintótica dada por (20) e aqueles obtidos por simulação são bastante próximos na região de média-a-alta SNR. Percebe-se que, um balanceamento de potência para $\delta = 0{,}5$ se mostrou o melhor cenário para se atingir a menor probabilidade de *outage* de sigilo. Além disso, percebe-se um comportamento simétrico das curvas para os casos $\delta = (0{,}1;\ 0{,}9)$ e $\delta = (0{,}3;\ 0{,}7)$. Também pode-se observar que não é possível alcançar um desempenho de sigilo favorável sem a técnica de *jamming* cooperativo.

A Fig. 11 mostra a probabilidade de *outage* de sigilo em função do fator de alocação de potência entre fonte e destino durante o primeiro subintervalo de IT, δ, para diferentes valores

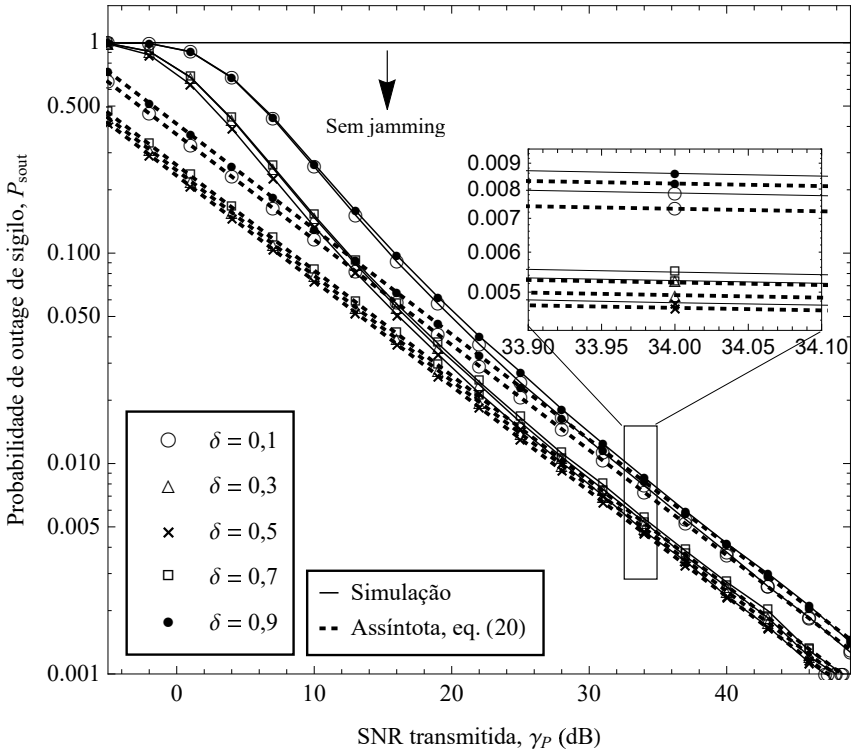

Figura 10 - Probabilidade de *outage* de sigilo em função da SNR transmitida γ_P, para o esquema S-WET com diferentes valores de δ e considerando $\alpha = 0,5$. Além disso, a probabilidade de *outage* de sigilo considerando um sistema sem *jamming* é apresentado. Fonte: Elaborada pelo autor.

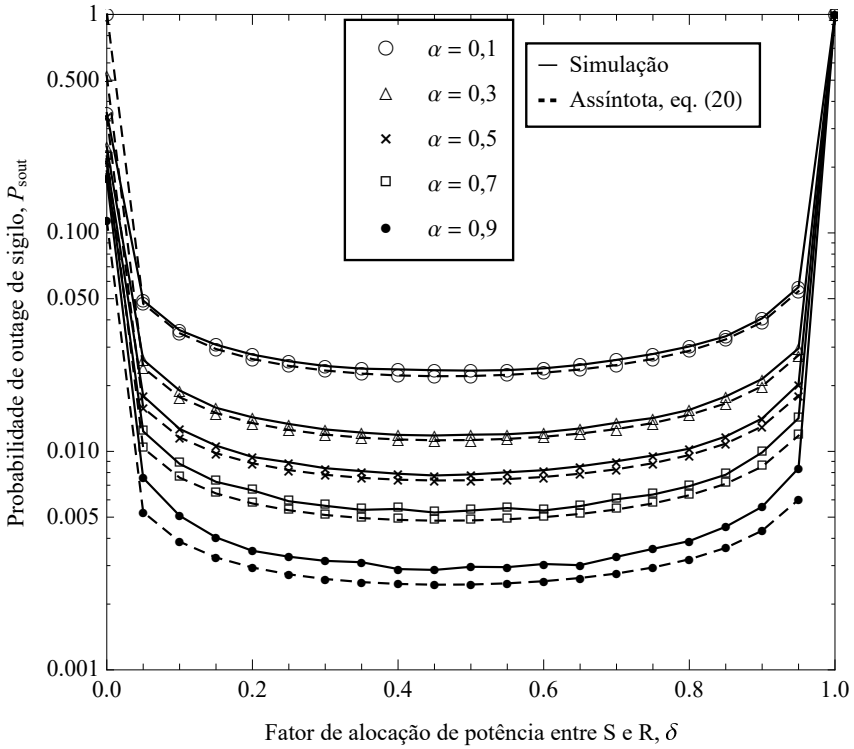

Figura 11 - Probabilidade de *outage* de sigilo em função do fator de alocação de potência δ, para o esquema S-WET para diferentes valores de $\alpha = 0{,}1,\ 0{,}3,\ 0{,}5,\ 0{,}7,\ 0{,}9$ e considerando $\gamma_P = 30$ dB. Fonte: Elaborada pelo autor.

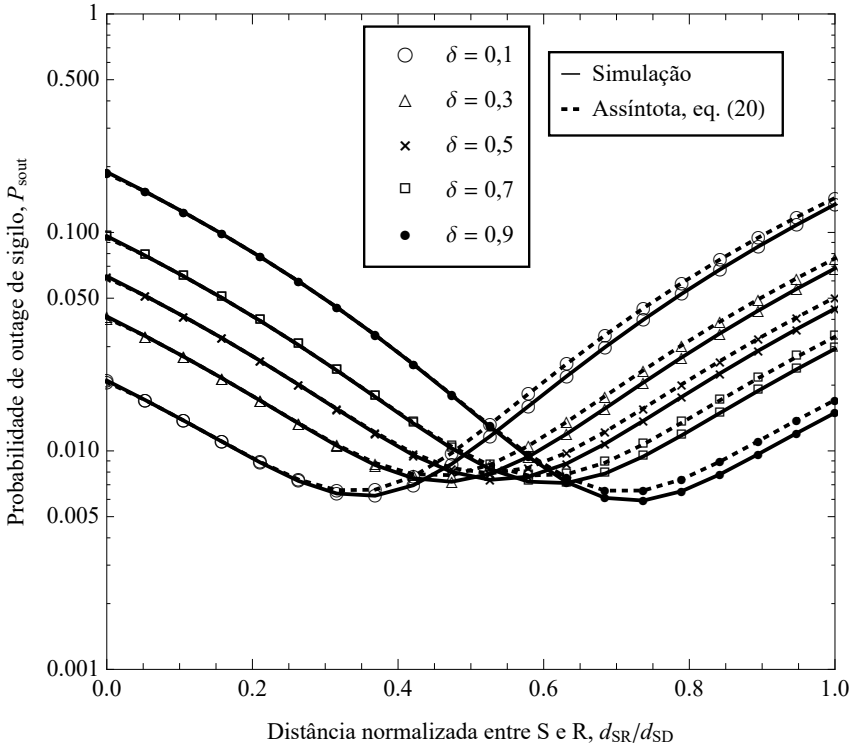

Figura 12 - Probabilidade de *outage* de sigilo em função da distância entre a fonte e o retransmissor normalizada d_{SR}/d_{SD}, considerando o esquema S-WET com diferentes valores de $\delta = 0{,}1,\ 0{,}3,\ 0{,}5,\ 0{,}7,\ 0{,}9$ e a SNR transmitida como $\gamma_P = 30$ dB. Fonte: Elaborada pelo autor.

do fator de alocação de tempo entre as fases de EH e IT, α. Nota-se que a curva das simulações de Monte Carlo e as curvas da expressão assintótica dada por (20) são muito semelhantes, principalmente para contextos em que um intervalo de tempo menor é alocado para a energização do retransmissor. Nota-se ainda que, conforme a SNR transmitida γ_P aumenta, a expressão referida em (20) será mais acurada. Assim, mostra-se que o fator de alocação de potência entre S e D, δ não interfere substancialmente na alocação de tempo para as fases de EH e IT.

A Fig. 12 ilustra a probabilidade de *outage* de sigilo em função da distância normalizada entre S e R em relação à distancia total, d_{SR}/d_{SD}. Observa-se que, conforme o retransmissor não confiável se aproxima da fonte, a melhor estratégia a adotar é a alocação da maior parte da potência ao destino durante o primeiro subintervalo da fase de transmissão de informação, tornando o sinal de *jamming* mais forte. Da mesma forma que, para posições do retransmissor relativamente mais próximas ao destino, a melhor estratégia a se adotar é alocar mais potência ao primeiro salto do enlace legítimo, fortalecendo o sinal de informação vindo da fonte e por consequência, acarretando no melhor desempenho de sigilo.

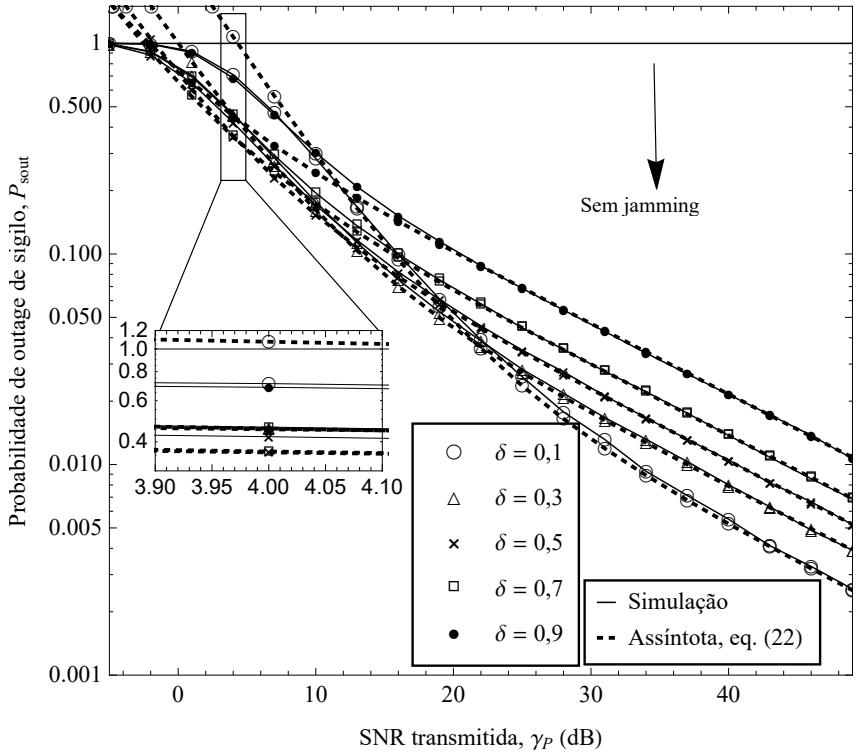

Figura 13 - Probabilidade de *outage* de sigilo em função da SNR transmitida γ_P, para o esquema D-WET com diferentes valores de δ e considerando $\alpha = 0,5$. Também, a probabilidade de *outage* de sigilo considerando um sistema sem *jamming* é apresentado. Fonte: Elaborada pelo autor.

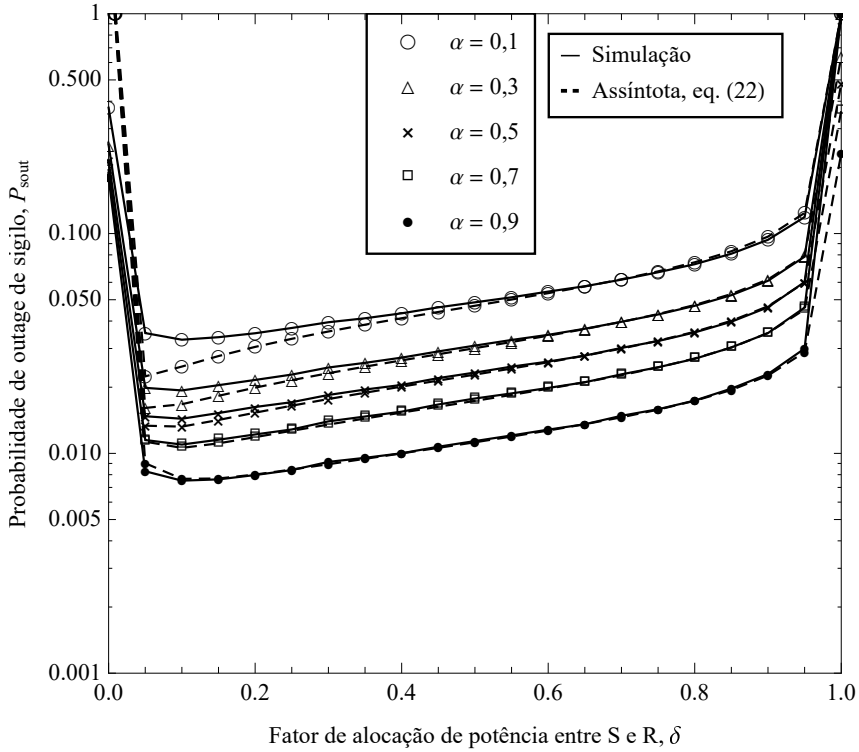

Figura 14 - Probabilidade de *outage* de sigilo em função do fator de alocação de potência δ, para o esquema D-WET para diferentes valores de $\alpha = 0,1,\ 0,3,\ 0,5,\ 0,7,\ 0,9$ e considerando $\gamma_P = 30$ dB. Fonte: Elaborada pelo autor.

4.2 Estratégia D-WET

A Fig. 13 apresenta a probabilidade de *outage* de sigilo em função da SNR transmitida γ_P, para diferentes valores do fator de alocação de potência entre fonte e destino δ, considerando o sistema com um retransmissor não confiável energizado através de sinais de RF vindos exclusivamente de D. Nota-se que as expressões analíticas são validadas através de simulações de Monte Carlo, mostrando excelentes resultados. Para um baixo regime de SNR, é observado um comportamento parecido com a estratégia S-WET. Além disso, o melhor desempenho de sigilo é obtido quando $\delta = 0,5$, ou seja, a mesma potência fornecida para a transmissão de informação é utilizada para o *jamming* no destino. Entretanto, já para o regime de média-a-alta SNR, o desempenho de sigilo melhora ao fortalecer o sinal de *jamming* durante o primeiro subintervalo da fase de IT. Também, assim como na estratégia S-WET, é concluído que a técnica de DBJ é essencial para alcançar uma comunicação segura.

A Fig. 14 mostra a probabilidade de *outage* de sigilo em função do fator de alocação de potência entre a fonte e o destino durante o primeiro subintervalo de IT, δ, para diferentes valores do fator de alocação de tempo entre as fases de EH e IT, α. Para este resultado, considera-se que o retransmissor AF é energizado por D. Além disso, fixa-se a SNR transmitida em $\gamma_P = 30$ dB. Percebe-se que o melhor desempenho de sigilo é alcançado quando é alocado mais tempo para

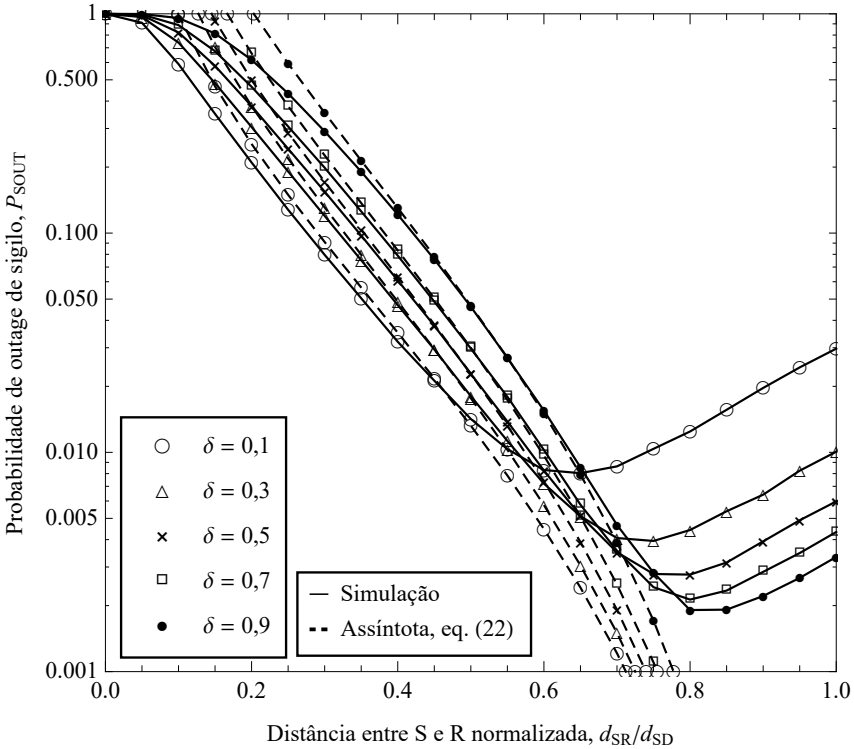

Figura 15 - Probabilidade de *outage* de sigilo em função da distância entre a fonte e o retransmissor normalizada d_{SR}/d_{SD}, considerando o esquema D-WET com diferentes valores de $\delta = 0,1,\ 0,3,\ 0,5,\ 0,7,\ 0,9$ e a SNR transmitida como $\gamma_P = 30$ dB. Fonte: Elaborada pelo autor.

a energização do retransmissor. Além disso, é observado que o desempenho de sigilo piora conforme mais potência é alocada para a fonte, para a transmissão do sinal de informação, durante o primeiro subintervalo da segunda fase, independentemente do fator de alocação de tempo para as fases de EH e IT adotado.

A Fig. 15 mostra a probabilidade de *outage* de sigilo de um sistema com o retransmissor energizado através da estratégia D-WET, em função da distância normalizada entre S e R em relação à distancia total, d_{SR}/d_{SD}, e diferentes valores de fator de alocação de potência para o sinal de informação e o sinal de *jamming*, δ. Além disso, assume-se que nesse gráfico, $\alpha = 0{,}5$ e $\gamma_P = 30$ dB. Para garantir o melhor desempenho de sigilo, uma estratégia eficaz é alocar o retransmissor não confiável mais próximo ao destino, em distâncias normalizadas de $d_{SR}/d_{SD} = 0{,}6$ a $d_{SR}/d_{SD} = 0{,}8$, dependendo do fator de alocação de potência utilizado. Depois disso, o desempenho de sigilo começa a piorar. Porém, isto pode ser aliviado ao alocar mais potência para a transmissão de informação pela fonte, durante o segundo subintervalo de IT (ou seja, considerando um elevado δ).

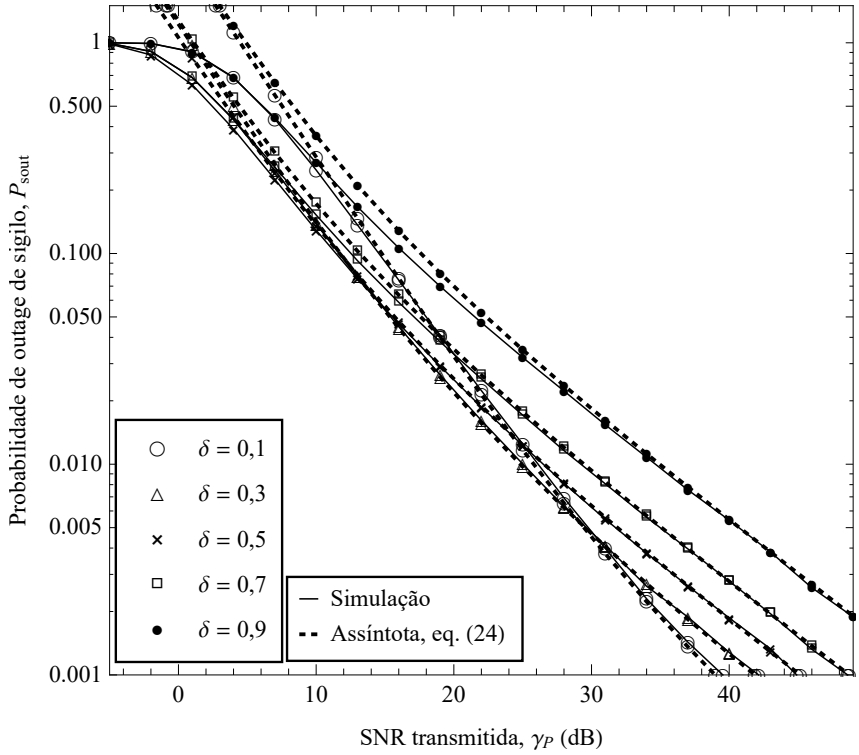

Figura 16 - Probabilidade de *outage* de sigilo em função da SNR transmitida γ_P, para o esquema SD-WET com diferentes valores de δ, considerando $\alpha = 0,5$ e $\mu = 0,5$. Fonte: Elaborada pelo autor.

4.3 Estratégia SD-WET

Fig. 16 mostra a probabilidade de *outage* de sigilo em função da SNR transmitida γ_P, para diferentes valores do fator de alocação de potência entre a fonte e destino δ, considerando o cenário em que o retransmissor é energizado pelos nós S e D simultaneamente. Nesse caso, o fator de alocação de potência durante a fase de EH foi fixado em $\mu = 0,5$, significando que fonte e destino energizam R com o mesmo nível de potência, como mostrado em (9). Note que a expressão analítica assintótica determinada em (24) é bem próxima aos resultados numéricos de simulação, principalmente nas regiões de média-a-alta SNR. Ao analisar a expressão em (24) em termos da SNR transmitida, observa-se que a estratégia conjunta de SD-WET e as estratégias S-WET e D-WET possuem uma ordem de diversidade do sistema similar, já que nas equações (4), (7) e (9) a SNR transmitida do sistema possui a mesma influência. Para uma baixa região de SNR, nota-se um comportamento simétrico análogo à estratégia S-WET, ou seja, para os casos $\delta = (0,1,\ 0,9)$ e $\delta = (0,3,\ 0,7)$, o desempenho de sigilo é similar. Por outro lado, para um regime de alta SNR, o desempenho de *outage* de sigilo se torna muito próximo ao comportamento utilizando D-WET, ou seja, a melhor estratégia é alcançada quando um forte sinal de *jamming* é fornecido durante o primeiro subintervalo da fase de IT.

A Fig. 17 mostra a probabilidade de *outage* de sigilo em função do fator de alocação de po-

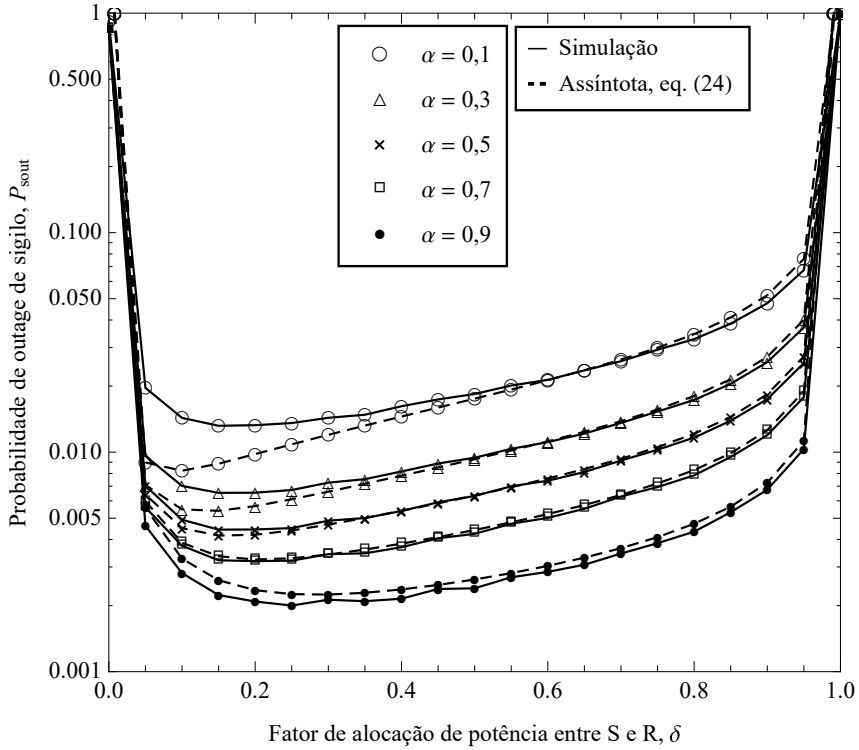

Figura 17 - Probabilidade de *outage* de sigilo em função do fator de alocação de potência δ, para o esquema SD-WET para diferentes valores de $\alpha = 0,1,\ 0,3,\ 0,5,\ 0,7,\ 0,9$, considerando $\gamma_P = 30$ dB e $\mu = 0,5$. Fonte: Elaborada pelo autor.

tência entre a fonte e o destino durante o primeiro subintervalo de IT, δ, para diferentes valores do fator de alocação de tempo entre as fases de EH e IT, α. Para este resultado, considera-se que o retransmissor AF é energizado por S e D simultaneamente, durante o tempo de energização para o EH. Além disso, fixa-se a SNR transmitida em $\gamma_P = 30$ dB para ilustrar esses casos. Assim como os casos S-WET e D-WET, a menor probabilidade de *outage* de sigilo é obtida quando se deixa mais tempo alocado para a energização do retransmissor durante a fase de EH. Além disso, percebe-se que ao fixar o fator de alocação de potência para a fase de EH em $\mu = 0,5$, o desempenho de *outage* de sigilo da estratégia SD-WET supera as estratégias S-WET e D-WET para a maior parte dos casos de alocação de potência para o sinal de *jamming*, exceto para os casos onde $\delta > 0,65$, nos quais quase nenhuma potência é alocada para o sinal de *jamming* durante a fase de IT, tornando o desempenho similar à estratégia S-WET.

Na Fig. 18 ilustra a probabilidade de *outage* de sigilo baseada em um cenário de rede com a estratégia SD-WET, em função da distância normalizada entre S e R em relação à distancia total, $d_{\mathrm{SR}}/d_{\mathrm{SD}}$, utilizando diferentes valores de fator de alocação de potência entre S e D, δ. Nota-se que (24) mostra uma boa aproximação aos resultados de simulação, principalmente para os casos em que $d_{SR}/d_{SD} < 0,6$. O desempenho de sigilo do sistema se comporta majoritariamente de modo similar a estratégia D-WET. De fato, como o fator de alocação de potência durante a fase de EH é $\mu = 0,5$, (9) aparentemente mostra que os canais g_{SR} e g_{RD} têm a mesma influência

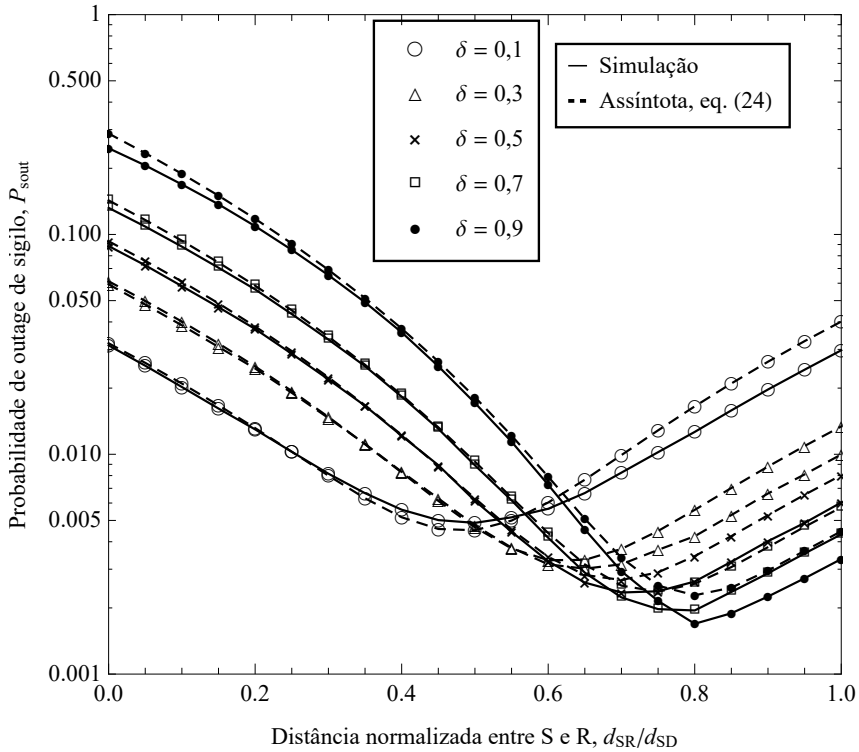

Figura 18 - Probabilidade de *outage* de sigilo em função da distância entre a fonte e o retransmissor normalizada $d_{\text{SR}}/d_{\text{SD}}$, considerando o esquema de energização conjunta SD-WET com diferentes valores de δ, SNR transmitida fixada em $\gamma_P = 30$ dB e $\mu = 0,5$. Fonte: Elaborada pelo autor.

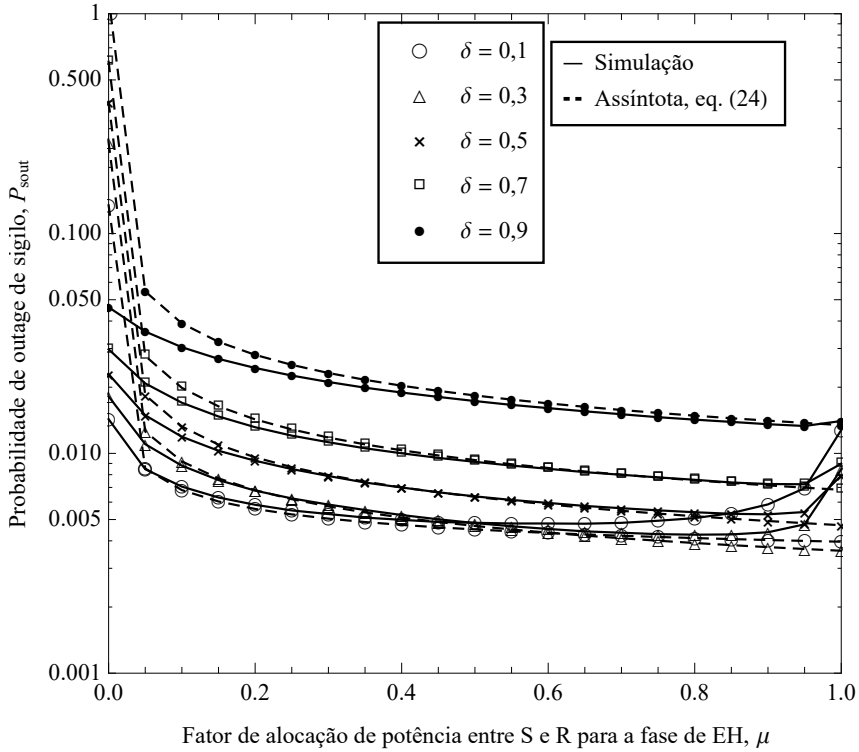

Figura 19 - Probabilidade de *outage* de sigilo em função do fator de alocação de potência entre S e R durante a fase de EH, μ, para o esquema SD-WET com diferentes valores de δ, considerando $\gamma_P = 30$ dB e $\alpha = 0,5$. Fonte: Elaborada pelo autor.

no sistema, porém, com a presença da técnica DBJ, o canal g_{RD} acaba tendo maior impacto, principalmente na SNR recebida no enlace fim-a-fim. Ao comparar as Figs. 12, 15 e 18, pode-se observar que a melhor estratégia WET em termos do desempenho de sigilo depende da posição que o retransmissor se encontra, conforme a seguir: S-WET para posições do retransmissor mais próximas da fonte; SD-WET para posições do retransmissor no meio entre a fonte e destino; e tanto D-WET quanto SD-WET para posições do retransmissor próximas ao destino.

A Fig. 19 mostra a probabilidade de *outage* de sigilo em função do fator de alocação de potência durante a fase de EH, μ, para diferentes valores do fator de alocação de potência entre a fonte e destino para o sinal de informação e de *jamming*, δ. No geral, pode-se observar que, para $\delta > 0,5$ (considerando um sinal de *jamming* mais fraco durante a fase de IT), o desempenho de sigilo melhora conforme μ aumenta, ou seja, quando mais potência é alocada para a fonte durante o EH. Por outro lado, para $\delta < 0,5$ (sinal de *jamming* fortalecido), a estratégia para garantir o melhor desempenho de sigilo é alcançada quando se realiza uma alocação balanceada de potência entre a fonte e destino durante a energização do retransmissor. Note que, os casos nos quais $\mu = 1$ e $\mu = 0$ correspondem as estratégias S-WET e D-WET, respectivamente.

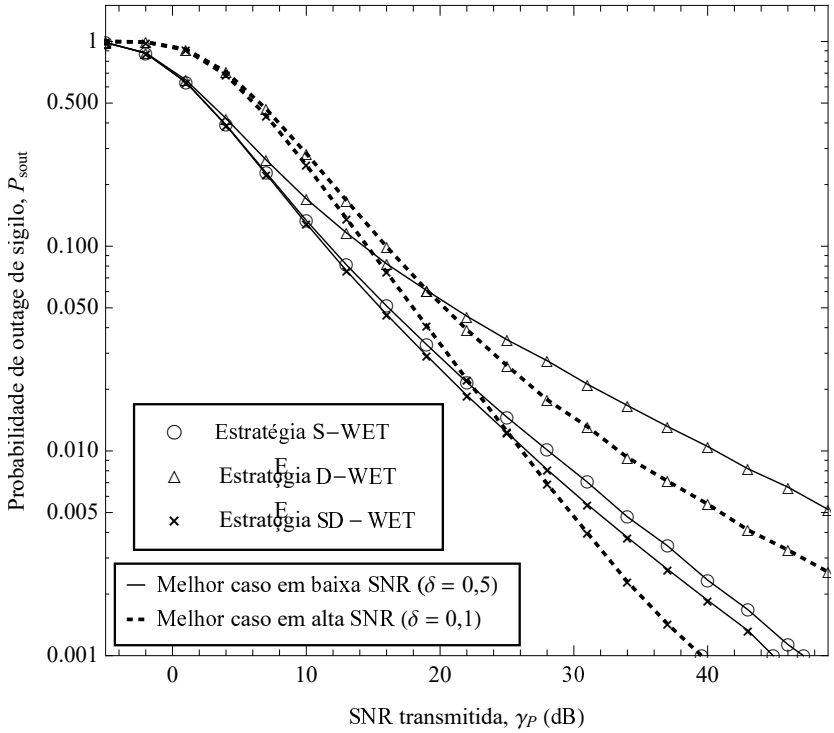

Figura 20 - Comparativo da probabilidade de *outage* de sigilo em função da SNR transmitida γ_P, considerando as estratégias de S-WET, D-WET e SD-WET, fixando $\alpha = 0,5$ e $\mu = 0,5$. Os casos para um regime de alta SNR são ilustrados com o $\delta = 0.1$, e para baixa SNR são fixados em $\delta = 0.5$. Fonte: Elaborada pelo autor.

4.4 Comparativo das estratégias S-WET, D-WET e SD-WET

A Fig. 20 retrata a melhor probabilidade de *outage* de sigilo em função da SNR transmitida, γ_P, considerando todas as estratégias de energização propostas. Para propósitos de clareza na apresentação, todas as curvas mostradas são referentes às simulações de Monte Carlo. Para o caso S-WET, foi considerado um fator de alocação de potência $\delta = 0,5$, enquanto que, para os casos D-WET e SD-WET, foram considerados dois tipos de curvas: curvas em linha cheia, que representam o melhor caso para o regime de baixa SNR (nas estratégias D-WET e SD-WET, o melhor caso ocorre quando o fator de alocação de potência entre a fonte e destino é $\delta = 0,5$); e curvas em linha pontilhada, que representam o melhor caso para o regime de alta SNR (nas estratégias D-WET e SD-WET, o melhor caso ocorre quando a maior parte da potência é alocada para o *jamming* no destino, ou seja, $\delta = 0,1$). Pode-se perceber que, para um regime de baixa SNR, as estratégias S-WET e SD-WET são as que possuem o melhor desempenho de sigilo. Já para um regime de média-a-alta SNR, a estratégia de energização conjunta SD-WET se mostrou com a menor probabilidade de *outage* de sigilo, sendo a melhor estratégia a ser utilizada como critérios de projeto.

A Fig. 21 mostra os melhores casos, considerando a probabilidade de *outage* de sigilo em função do fator de alocação de potência entre S e D durante a fase de IT, δ, considerando

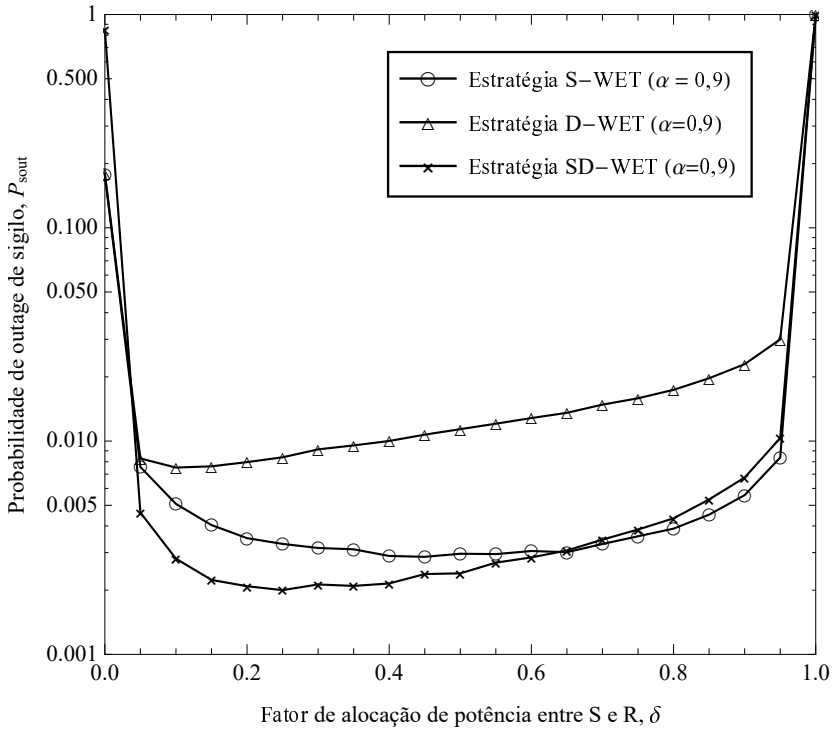

Figura 21 - Comparativo dos melhores casos das estratégias S-WET, D-WET e SD-WET da probabilidade de *outage* de sigilo em função do fator de alocação de potência entre S e R δ, considerando $\gamma_P = 30$ dB e para o caso SD-WET, $\mu = 0,5$. Para todos os casos, foi considerado $\alpha = 0,9$. Fonte: Elaborada pelo autor.

todas as estratégias de energização propostas. Para todos os casos, foi considerado um fator de alocação de tempo referente as fases de EH e IT, $\alpha = 0,9$. Assumindo que a maior parte da potência disponível é alocada para o sinal de *jamming*, é interessante utilizar a estratégia SD-WET, entretanto já para os casos em que a maior parte da potência disponível durante a fase de IT é alocada para o sinal de informação na fonte, a mais interessante utilizar a estratégia S-WET, garantido o melhor desempenho de sigilo.

A Fig. 22 ilustra o melhor das três estratégias, considerando a probabilidade de *outage* de sigilo em função da distância entre a fonte e o retransmissor normalizada $d_{\mathrm{SR}}/d_{\mathrm{SD}}$. Em todos os casos, é possível verificar que para posições relativas de R mais próximos de S, a melhor estratégia acontece quando a maior parte da potência é alocada para o sinal de *jamming*, durante o primeiro subintervalo da fase de transmissão de informação. Já para posições mais próximas ao destino, o melhor desempenho de sigilo é alcançado quando a maior parte da potência disponível durante a fase de IT é alocada para o sinal de informação na fonte. Percebe-se também que, a melhor estratégia de energização do retransmissor em termos do desempenho de sigilo depende da posição em que o retransmissor se encontra: S-WET para posições do retransmissor mais próximas da fonte; SD-WET para o retransmissor localizado no meio entre a fonte e o destino; e D-WET ou SD-WET para posições próximas do destino.

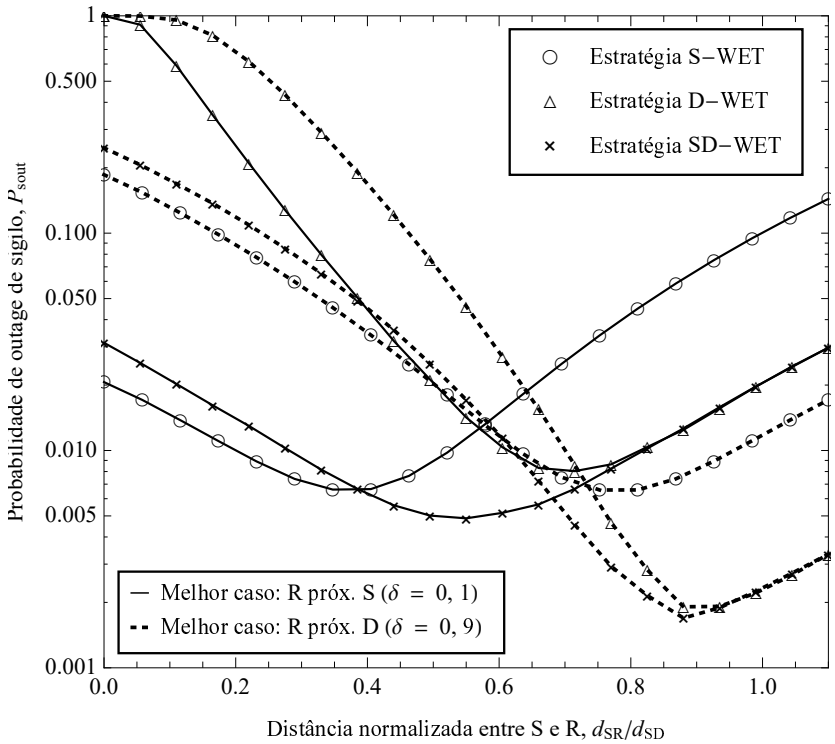

Figura 22 - Comparativo das estratégias S-WET, D-WET e SD-WET, considerando a probabilidade de *outage* de sigilo em função da distância entre a fonte e o retransmissor normalizada d_{SR}/d_{SD}, considerando $\alpha = 0,5$ e $\gamma_P = 30$ dB. Para todos os casos, o melhor caso de R mais próximo de S é quando $\delta = 0,1$, enquanto que no caso de R mais próximo de D, são ilustrados os casos em que $\delta = 0,9$. Fonte: Elaborada pelo autor.

5 CONCLUSÕES

Neste trabalho, o desempenho em termos da probabilidade de *outage* de sigilo para uma rede cooperativa com um retransmissor AF não confiável foi analisado. Considerou-se o uso da técnica DBJ para prover segurança de camada física na comunicação entre fonte e destino. Considerou-se ainda que o retransmissor é energizado via *time-switching* usando três estratégias: a primeira consiste na energização a partir da fonte, a segunda a partir do destino e a terceira a partir da fonte e destino, simultaneamente. Para cada cenário, uma expressão analítica assintótica em forma fechada foi obtida e validada por simulações de Monte Carlo. Para as estratégias propostas, foi investigado o efeito no desempenho dos seguintes parâmetros do sistema: o fator de alocação de potência entre a fonte e o destino durante a fase de transmissão de informação, fator de alocação de tempo para as fases de EH e IT, posição relativa normalizada do retransmissor em relação a fonte, e para o caso conjunto SD-WET, o fator de alocação de potência para a energização do retransmissor durante a fase de EH.

Dos resultados foi observado que, nos casos S-WET e D-WET, a técnica DBJ é essencial para transmitir informação de forma segura. Também, nos três casos foi possível verificar que o melhor desempenho de sigilo pode ser alcançado conforme um maior intervalo de tempo é alocado para a energização do retransmissor durante a fase de EH. Adicionalmente, nas três estratégias percebe-se que para posições relativas do retransmissor próximas da fonte, a menor probabilidade de *outage* de sigilo é alcançada conforme mais potência é alocada para o sinal de *jamming* durante o primeiro subintervalo da fase de transmissão de informação. Em contrapartida, para posições mais próximas ao destino, a melhor estratégia é alcançada conforme se aloca mais potência à fonte para o sinal de informação, fortalecendo o enlace do primeiro salto.

Dos resultados, para o caso da alimentação do retransmissor pela fonte, concluiu-se que a melhor estratégia é a realização de uma alocação balanceada de potência, ou seja, metade da potência disponível seria alocada para a fonte para transmissão de informação, e o restante para o destino para a transmissão do sinal de *jamming*. Nota-se que isso ocorre para toda a faixa de SNR considerada.

Já considerando a alimentação do retransmissor pelo destino, percebe-se o mesmo comportamento somente para um regime de baixa SNR. No regime de média-a-alta SNR, o melhor desempenho da probabilidade de *outage* ocorre ao fortalecer a potência alocada para o *jamming* durante a fase de transmissão de informação. Ainda neste mesmo cenário, observou-se que a a segurança do processo de comunicação é melhorada conforme o retransmissor é posicionado mais próximo do destino.

Para a energização conjunta do retransmissor através da fonte e destino, tem-se um comportamento similar ao caso D-WET, ou seja, no regime de baixa SNR, uma alocação balanceada de potência é a melhor forma de garantir uma comunicação segura, a para o regime de alta SNR, o desempenho de sigilo melhora ao alocar mais potência ao sinal de *jamming*, durante o primeiro subintervalo da fase de IT. Pode-se observar que, para sinais de informação da fonte fortalecidos, o desempenho de sigilo melhora conforme o retransmissor é energizado mais pela fonte. Por outro lado, para sinais de *jamming* fortalecidos, a melhor estratégia a ser considerada é realizar uma energização balanceada do retransmissor através da fonte e destino em conjunto.

Da comparação das três estratégias, é possível aferir que nem sempre a estratégia de energização conjunta é a melhor para se garantir sigilo na comunicação. Por exemplo, considerando um regime de baixa SNR, a estratégia S-WET se equipara com a estratégia SD-WET, e para um regime de alta SNR, SD-WET se mostra com o melhor desempenho de sigilo. Além disso, a estratégia S-WET supera em desempenho as outras estratégias quando a maior parte da potência é alocada para a fonte durante a fase de transmissão de informação. Por fim, considerando a posição relativa do retransmissor, percebe-se que para posições mais próximas a fonte, a estratégia S-WET mostra o melhor desempenho de sigilo. Em contrapartida, para posições mais próximas ao destino, as estratégias D-WET e SD-WET se mostram mais promissoras para atingir uma comunicação mais segura.

5.1 Trabalhos Futuros

Considerando a análise de desempenho de sigilo das estratégias WET apresentadas neste trabalho, foi adotado um modo de retransmissão HD, ou seja, o retransmissor recebe e encaminha os sinais em canais ortogonais, causando assim uma perda em termos de eficiência espectral. Um possível trabalho futuro seria considerar o modo de retransmissão *full duplex* (FD), na qual o retransmissor poderá transmitir e receber sinais na mesma frequência e intervalo de tempo.

Outro possível trabalho futuro seria considerar a técnica SBJ, possibilitando análises de vantagens e desvantagens que esta técnica pode oferecer em termos de desempenho de sigilo.

Uma outra proposta seria analisar o desempenho de sigilo considerando a presença de múltiplos retransmissores na rede por meio de técnicas de seleção de retransmissor, que vise maior segurança na transmissão de sinais de informação.

APÊNDICE A

A.1 Autorização para Reprodução do Artigo Publicado

Copyright Clearance Center RightsLink®

Home | Help | Email Support | Sign in | Create Account

IEEE Requesting permission to reuse content from an IEEE publication

Secrecy Performance of Untrustworthy AF Relay Networks using Cooperative Jamming and SWIPT

Conference Proceedings:
2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)

Author: E. N. Egashira

Publisher: IEEE

Date: Sept. 2019

Copyright © 2019, IEEE

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

BACK CLOSE WINDOW

APÊNDICE B

B.1 Demonstração da Proposição 1

Para determinar a expressão assintótica em forma fechada para a probabilidade de *outage* de sigilo de um sistema composto por um retransmissor não confiável que é energizado por sinais de RF a partir da fonte, primeiramente será analisada a região de integração envolvida, conforme (19). Como a região de integração é relativamente complexa, uma aproximação baseada em duas áreas retangulares é proposta, na qual é obtida baseada nas retas assíntotas provenientes dos limites de $g_{\mathrm{SR}} \to \infty$ e $g_{\mathrm{RD}} \to \infty$ aplicadas na expressão (19). Assim, a região da assíntota horizontal A1 é dada por

$$\begin{aligned}
\mathrm{A1} &= \lim_{g_{\mathrm{SR}}\to\infty}\left(1+\frac{\delta\theta\gamma_P g_{\mathrm{SR}}^2 g_{\mathrm{RD}}}{g_{\mathrm{SR}}\left(\delta+\theta g_{\mathrm{RD}}+\frac{(1-\delta)g_{\mathrm{RD}}}{g_{\mathrm{SR}}}\right)} < \tau\left(\frac{\delta g_{\mathrm{SR}}}{(1-\delta)g_{\mathrm{RD}}}\right)\right) \\
&\simeq \frac{\delta\theta\gamma_P g_{\mathrm{RD}}}{(\delta+\theta g_{\mathrm{RD}})} < \frac{\tau\delta}{(1-\delta)g_{\mathrm{RD}}} \\
&\overset{(h)}{=} \delta(1-\delta)\theta\gamma_P g_{\mathrm{RD}}^2 - \tau\delta\theta g_{\mathrm{RD}} - \tau\delta^2 < 0 \\
&= g_{\mathrm{RD}} < \frac{\tau\delta\theta+\sqrt{\tau^2\delta^2\theta^2+4\tau\delta^3(1-\delta)\theta\gamma_P}}{2\delta(1-\delta)\theta\gamma_P} \\
&= g_{\mathrm{RD}} < \frac{\tau\theta+\sqrt{\tau^2\theta^2+4\tau\delta(1-\delta)\theta\gamma_P}}{2(1-\delta)\theta\gamma_P},
\end{aligned} \tag{25}$$

em que no passo (h) foi resolvida a inequação de segundo grau, como função de g_{SR}. Adicionalmente, utilizando uma abordagem similar, a região $A2$ referente a assíntota vertical é derivada a partir de (19), expresso como

$$\begin{aligned}
\mathrm{A2} &= \lim_{g_{\mathrm{RD}}\to\infty}\left(1+\frac{\delta\theta\gamma_P g_{\mathrm{SR}}^2 g_{\mathrm{RD}}}{\delta g_{\mathrm{SR}}+g_{\mathrm{RD}}(\theta g_{\mathrm{SR}}+1-\delta)} < \tau\left(\frac{\delta g_{\mathrm{SR}}+(1-\delta)g_{\mathrm{RD}}}{(1-\delta)g_{\mathrm{RD}}}\right)\right) \\
&\simeq \lim_{g_{\mathrm{RD}}\to\infty}\left(1+\frac{\delta\theta\gamma_P g_{\mathrm{SR}}^2 g_{\mathrm{RD}}}{g_{\mathrm{RD}}(\theta g_{\mathrm{SR}}+1-\delta+\frac{\delta g_{\mathrm{SR}}}{g_{\mathrm{RD}}})} < \tau\right) \\
&\simeq \frac{\delta\theta\gamma_P g_{\mathrm{SR}}^2}{\theta g_{\mathrm{SR}}+1-\delta} < \tau-1 \\
&= \delta\theta\gamma_P g_{\mathrm{SR}}^2 - \theta g_{\mathrm{SR}}(\tau-1) - (1-\delta)(\tau-1) < 0 \\
&= g_{\mathrm{SR}} < \frac{\theta(\tau-1)}{2\delta\theta\gamma_P} + \frac{\sqrt{\theta^2(\tau-1)^2+4\delta(1-\delta)\theta\gamma_P(\tau-1)}}{2\delta\theta\gamma_P}.
\end{aligned} \tag{26}$$

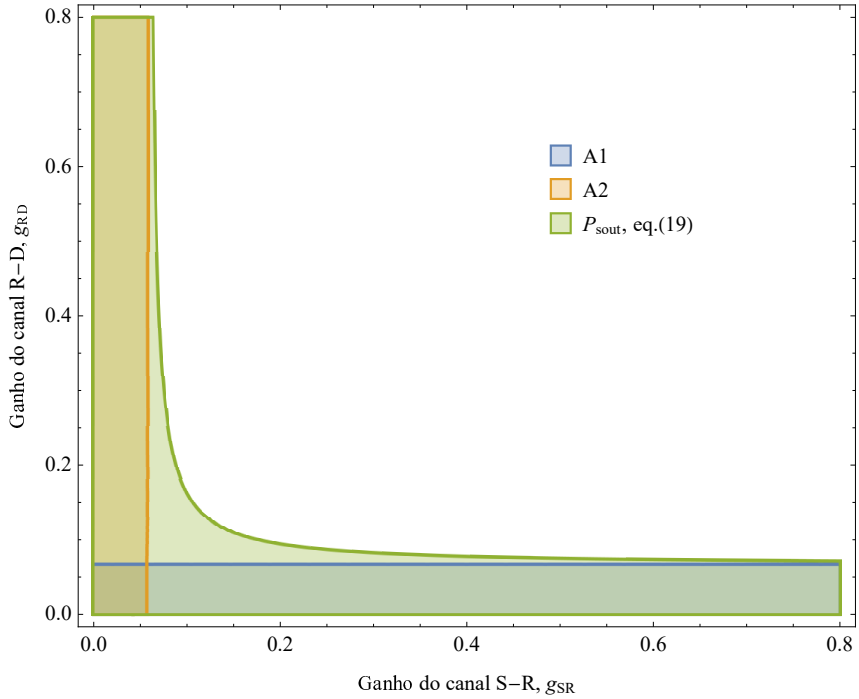

Figura 23 - Comparativo das regiões de integração retangulares propostas com a probabilidade de *outage* de sigilo exata, utilizando a estratégia S-WET. Fonte: Elaborada pelo autor.

Conforme a Fig. 23, a probabilidade de *outage* de sigilo do evento em $\Pr(\cdot)$ em (19) pode ser aproximada através das regiões A1 e A2, regidas pelas equações (25) e (26), respectivamente. Portanto, a aproximação em forma assintótica para a probabilidade de *outage* de sigilo pode ser definida como $\Pr(\mathrm{A1}\bigcup\mathrm{A2})$, ou seja

$$P_{\text{sout}} \simeq \Pr(\mathrm{A1}) + \Pr(\mathrm{A2}) - \Pr(\mathrm{A1})\Pr(\mathrm{A2}). \tag{27}$$

Assim, substituindo (25) e (26) em (27) e considerando que cada região é independente, a probabilidade de *outage* de sigilo pode ser desenvolvida como

$$\begin{aligned} P_{\text{sout}} = {} & F_{g_{\text{SR}}}\left(\frac{\theta(\tau-1)+\sqrt{\theta^2(\tau-1)^2+4\delta(1-\delta)\theta\gamma_P(\tau-1)}}{2\delta\theta\gamma_P}\right) \\ & + F_{g_{\text{RD}}}\left(\frac{\tau\delta\theta+\sqrt{\tau^2\delta^2\theta^2+4\tau\delta^3(1-\delta)\theta\gamma_P}}{2\delta(1-\delta)\theta\gamma_P}\right) \\ & - F_{g_{\text{SR}}}\left(\frac{\theta(\tau-1)+\sqrt{\theta^2(\tau-1)^2+4\delta(1-\delta)\theta\gamma_P(\tau-1)}}{2\delta\theta\gamma_P}\right) \\ & \times F_{g_{\text{RD}}}\left(\frac{\tau\delta\theta+\sqrt{\tau^2\delta^2\theta^2+4\tau\delta^3(1-\delta)\theta\gamma_P}}{2\delta(1-\delta)\theta\gamma_P}\right). \end{aligned} \tag{28}$$

Nota-se que $F_{g_{\text{SR}}}$ e $F_{g_{\text{RD}}}$ são as funções de distribuição acumulada (CDFs, *cummulative distribution function*) dos ganhos dos enlaces S→R e R→D, respectivamente, e que estes ganhos dos canais seguem uma distribuição exponencial de média Ω_{i}, para $\text{i} \in \{\text{SR}, \text{RD}\}$. Nota-se ainda

que $F_{g_{\mathrm{SR}}}(x)$ é dada por

$$F_{g_{\mathrm{SR}}}(x) = 1 - e^{\frac{-x}{\Omega_{\mathrm{SR}}}}, \tag{29}$$

e de forma análoga, $F_{g_{\mathrm{RD}}}(x)$ é dada por

$$F_{g_{\mathrm{RD}}}(x) = 1 - e^{\frac{-x}{\Omega_{\mathrm{RD}}}}. \tag{30}$$

Finalmente, para obter a expressão analítica assintótica referida, são negligenciados os termos proporcionais a $1/\gamma_P$ e seus equivalentes em maiores ordens, referentes a (28). Note que, conforme P cresce em um regime de alta SNR, esses termos se tornam insignificantes. Também, foi aplicada a expansão das séries de Maclaurin para uma função exponencial, como mostrado em [42, eq. (0.318.2)], especialmente para o caso $e^{-x} \simeq 1 - x$ para $x \to 0$. Ao utilizar esta aproximação em (28), e depois de algumas manipulações, a expressão assintótica em forma fechada para a probabilidade de *outage* de sigilo referente a estratégia de energização S-WET é obtida conforme mostrado em (20).

APÊNDICE C

C.1 Demonstração da Proposição 2

Neste apêndice é mostrado em mais detalhes o processo para a obtenção da probabilidade de *outage* de sigilo do sistema usando a estratégia D-WET. Para este propósito, determinam-se as regiões de integração para os eventos de *outage* referente ao argumento de $\Pr(\cdot)$ em (21). O termo $\min\{\cdot,\cdot\}$ é abordado a partir dos seguintes eventos: (*i*) $\delta g_{\mathrm{SR}} < (\theta g_{\mathrm{RD}} + 1 - \delta) g_{\mathrm{RD}}$ e (*ii*) $\delta g_{\mathrm{SR}} > (\theta g_{\mathrm{RD}} + 1 - \delta) g_{\mathrm{RD}}$. Esses eventos geram duas regiões de integração, denominadas por $B1$ e $B2$, nos quais são ilustrados na Fig. 24. Para a primeira condição, procede-se de (21), sendo obtida a região de integração $B1$, dada por

$$
\begin{aligned}
B1 = 0 < g_{\mathrm{SR}} \leq \frac{\tau}{\gamma_P \delta} \bigcap \theta \left[1 - \delta + 2\theta g_{\mathrm{RD}} - \left((1-\delta)^2 + 4\delta\theta g_{\mathrm{SR}} \right)^{\frac{1}{2}} \right] > 0 \bigcup \Bigg\{ g_{\mathrm{SR}} > \frac{\tau}{\gamma_P \delta} \\
\bigcap \frac{1}{\gamma_P^2 \delta (1-\delta)^2} \left\{ \theta\tau \left[\left(\frac{8\tau\gamma_P (1-\delta)^2}{\theta} + \tau^2 \right)^{\frac{1}{2}} + \tau \right] + \gamma_P (1-\delta)^2 \right. \\
\left. \times \left[\left(\frac{8\tau\gamma_P (1-\delta)^2}{\theta} + \tau^2 \right)^{\frac{1}{2}} + 5\tau \right] \right\} > 2 g_{\mathrm{SR}} \bigcap \frac{\sqrt{(1-\delta)^2 + 4\delta\theta g_{\mathrm{SR}}} - 1 + \delta}{2\theta} < g_{\mathrm{RD}} \\
< \Bigg[(1-\delta)^2 \tau + \delta\theta\tau g_{\mathrm{SR}} + \sqrt{\tau} \left(\gamma_P \delta g_{\mathrm{SR}} - \tau \right) \left(\frac{4\gamma_P \delta^2 (1-\delta)^2 \theta g_{\mathrm{SR}}^2}{(\tau - \gamma_P \delta g_{\mathrm{SR}})^2} \right. \\
\left. + \frac{\tau \left[(1-\delta)^2 - \delta\theta g_{\mathrm{SR}}^2 \right]}{(\tau - \gamma_P \delta g_{\mathrm{SR}})^2} \right)^{\frac{1}{2}} \Bigg] \left(\frac{1}{2(1-\delta)\theta(\gamma_P \delta g_{\mathrm{SR}} - \tau)} \right) \Bigg\}. \qquad (31)
\end{aligned}
$$

E para a segunda condição, a região de integração $B2$ é expressa como

$$
\begin{aligned}
B2 = \Bigg\{ g_{\mathrm{RD}} < \Bigg[\frac{\tau\delta g_{\mathrm{SR}}}{2(1-\delta)\theta\gamma_P} \left(\frac{\delta^2 g_{\mathrm{SR}}^2 \tau^2}{4\theta^2 \gamma_P^2 (1-\delta)^2} - \frac{\tau^3}{27\gamma_P^3 \theta^3} \right)^{\frac{1}{2}} \Bigg]^{\frac{1}{3}} + \frac{\tau}{3\theta\gamma_P} \Bigg[\frac{\tau\delta g_{\mathrm{SR}}}{2(1-\delta)\theta\gamma_P} \\
\times \left(\frac{\delta^2 g_{\mathrm{SR}}^2 \tau^2}{4\theta^2 \gamma_P^2 (1-\delta)^2} - \frac{\tau^3}{27\gamma_P^3 \theta^3} \right)^{\frac{1}{2}} \Bigg]^{-\frac{1}{3}} \bigcap \frac{1}{\gamma_P^2 \delta (1-\delta)^2} \left\{ \theta\tau \left[\left(\frac{8\tau\gamma_P (1-\delta)^2}{\theta} + \tau^2 \right)^{\frac{1}{2}} + \tau \right] \right. \\
\left. + \gamma_P (1-\delta)^2 \left[\left(\frac{8\tau\gamma_P (1-\delta)^2}{\theta} + \tau^2 \right)^{\frac{1}{2}} + 5\tau \right] \right\} < 2 g_{\mathrm{SR}} \Bigg\} \bigcup \Bigg\{ 0 < g_{\mathrm{RD}} < \frac{1}{2} \\
\times \sqrt{\frac{(1-\delta)^2 + 4\delta\theta g_{\mathrm{SR}}}{\theta^2}} - \frac{1-\delta}{2\theta} \bigcap \frac{1}{\gamma_P^2 \delta (1-\delta)^2} \left\{ \theta\tau \left[\left(\frac{8\tau\gamma_P (1-\delta)^2}{\theta} + \tau^2 \right)^{\frac{1}{2}} + \tau \right] \right. \\
\left. + \gamma_P (1-\delta)^2 \left[\left(\frac{8\tau\gamma_P (1-\delta)^2}{\theta} + \tau^2 \right)^{\frac{1}{2}} + 5\tau \right] \right\} \geq 2 g_{\mathrm{SR}} \Bigg\}. \qquad (32)
\end{aligned}
$$

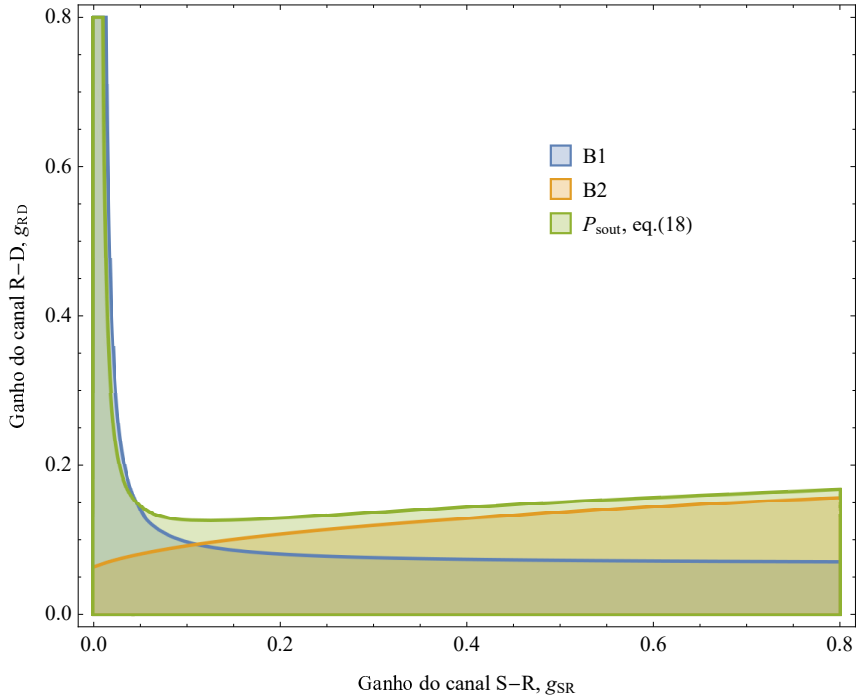

Figura 24 - Comparativo das regiões de integração propostas com a probabilidade de *outage* de sigilo exata, utilizando a estratégia D-WET. Fonte: Elaborada pelo autor.

Dessa forma, consegue-se desenvolver a probabilidade de *outage* de sigilo baseado nas regiões (31) e (32) na forma integral. A Fig. 24 ilustra a comparação entre as regiões de integração aproximadas propostas e a probabilidade de *outage* exata expressa em (18). Para tanto, uma expressão analítica aproximada para a probabilidade de *outage* de sigilo de um sistema com um retransmissor AF não confiável e energizado através de sinais de RF vindos de D e utilizando a técnica *time switching* e DBJ é dada por

$$
\begin{aligned}
P_{\text{sout}} = F_{g_{\text{SR}}}(g_{\text{SR1}}) + \int_{g_{\text{SR1}}}^{g_{\text{SR2}}} F_{g_{\text{RD}}}\Bigg(\frac{1}{2}\Bigg(\frac{(1-\delta)^4\tau^2 + 4\delta^2(1-\delta)^2\theta\tau x^2\gamma_P + \delta^2\theta^2\tau^2x^2}{(1-\delta)^2\theta^2(\delta x\gamma_P - \tau)^2} \\
- \frac{2\delta(1-\delta)^2\theta\tau^2 x}{(1-\delta)^2\theta^2(\delta x\gamma_P - \tau)^2}\Bigg)^{\frac{1}{2}} + \frac{-(1-\delta)^2\tau - \delta\theta\tau x}{2(1-\delta)\theta(\tau - \delta x\gamma_P)}\Bigg) f_{g_{\text{SR}}}(x)dx \\
+ \int_{g_{\text{SR2}}}^{\infty} F_{g_{\text{RD}}}\Bigg(\Bigg(\frac{\delta}{(1-\delta)}\frac{\tau x}{2\theta\gamma_P} + \Bigg(\frac{\delta^2\tau^2x^2}{4(1-\delta)^2\theta^2\gamma_P^2} - \frac{\tau^3}{27\theta^3\gamma_P^3}\Bigg)^{\frac{1}{2}}\Bigg)^{\frac{1}{3}} + \frac{\tau}{3\theta\gamma_P} \\
\times \Bigg(\frac{\delta\tau x}{2(1-\delta)\theta\gamma_P} + \Bigg(\frac{\delta^2\tau^2x^2}{4(1-\delta)^2\theta^2\gamma_P^2} - \frac{\tau^3}{27\theta^3\gamma_P^3}\Bigg)^{\frac{1}{2}}\Bigg)^{-\frac{1}{3}}\Bigg) f_{g_{\text{SR}}}(x)dx, \qquad (33)
\end{aligned}
$$

em que

$$
\begin{aligned}
g_{\text{SR1}} &= \frac{\tau}{\gamma_P\delta}, \\
g_{\text{SR2}} &= \frac{\theta\tau^2 + 5(1-\delta)^2\tau\gamma_P}{2\delta(1-\delta)^2\gamma_P^2} + \frac{1}{2}\Bigg(\frac{\theta^3\tau^4 + 8(1-\delta)^6\tau\gamma_P^3}{\delta^2(1-\delta)^4\theta\gamma_P^4}
\end{aligned}
$$

$$+\frac{17(1-\delta)^4\theta\tau^2\gamma_P^2+10(1-\delta)^2\theta^2\tau^3\gamma_P}{\delta^2(1-\delta)^4\theta\gamma_P^4}\Bigg)^{\frac{1}{2}}.$$

Considerando que os termos proporcionais a $1/\gamma_P$ e $1/\gamma_P^2$ presentes em (33) tendem a zero em um regime de alta SNR, aplica-se a expansão das séries de Maclaurin referente a função exponencial, definido em [42, eq. (0.318.2)], tornando possível prosseguir nas integrais resultantes em (33). Após algumas manipulações, é obtida a expressão assintótica em forma fechada para a probabilidade de *outage* de sigilo, como mostrado em (22).

APÊNDICE D

D.1 Demonstração da Proposição 3

Aplicando uma abordagem similar à utilizada no Apêndice B, a análise da probabilidade de *outage* de sigilo para a estratégia SD-WET é desenvolvida a partir de (23). Para este propósito, foi realizada a aproximação da região de integração em duas áreas retangulares, $C1$ e $C2$, determinadas pelas assíntotas horizontal e vertical: $g_{\mathrm{SR}} \to \infty$ e $g_{\mathrm{RD}} \to \infty$, respectivamente. Ambas as regiões são mostradas e comparadas com a probabilidade de *outage* exata, determinada em (18), conforme a Fig. 25. Assim, a região marcada pela assíntota horizontal pode ser obtida como

$$\begin{aligned}
\mathrm{C1} &= \lim_{g_{\mathrm{SR}}\to\infty}\left(\frac{\delta\theta\gamma_P\mu g_{\mathrm{SR}}^2 g_{\mathrm{RD}} + \delta\theta\gamma_P(1-\mu)g_{\mathrm{SR}}g_{\mathrm{RD}}^2}{\delta g_{\mathrm{SR}} + g_{\mathrm{RD}}\{\theta[\mu g_{\mathrm{SR}} + (1-\mu)g_{\mathrm{RD}}] + (1-\delta)\}} < \tau\left(\frac{\delta g_{\mathrm{SR}} + (1-\delta)g_{\mathrm{RD}}}{(1-\delta)g_{\mathrm{RD}}}\right)\right) \\
&= \lim_{g_{\mathrm{SR}}\to\infty}\left(\frac{g_{\mathrm{SR}}[\delta\theta\gamma_P\mu g_{\mathrm{SR}}g_{\mathrm{RD}} + \delta\theta\gamma_P(1-\mu)g_{\mathrm{RD}}^2]}{g_{\mathrm{SR}}(\delta + \theta\mu g_{\mathrm{RD}})} < \tau\left(\frac{\delta g_{\mathrm{SR}}}{(1-\delta)g_{\mathrm{RD}}}\right)\right) \\
&= \lim_{g_{\mathrm{SR}}\to\infty}\left(\frac{\delta\theta\gamma_P\mu g_{\mathrm{RD}} + \frac{\delta\theta\gamma_P(1-\mu)g_{\mathrm{RD}}^2}{g_{\mathrm{SR}}}}{\delta + \theta\mu g_{\mathrm{RD}}} < \tau\left(\frac{\delta}{(1-\delta)g_{\mathrm{RD}}}\right)\right) \\
&= \frac{\delta\theta\gamma_P\mu g_{\mathrm{RD}}}{\delta + \theta\mu g_{\mathrm{RD}}} < \frac{\tau\delta}{(1-\delta)g_{\mathrm{RD}}} \\
&= \delta(1-\delta)\theta\gamma_P\mu g_{\mathrm{RD}}^2 < \tau\delta^2 + \tau\delta\theta\mu g_{\mathrm{RD}} \\
&= (1-\delta)\theta\gamma_P\mu g_{\mathrm{RD}}^2 - \tau\theta\mu g_{\mathrm{RD}} - \tau\delta < 0 \\
&= g_{\mathrm{RD}} < \frac{\tau\theta\mu + \sqrt{\tau^2\theta^2\mu^2 + 4\tau\delta(1-\delta)\theta\gamma_P\mu}}{2(1-\delta)\theta\gamma_P\mu}.
\end{aligned} \tag{34}$$

Da mesma forma, a região demarcada pela assíntota vertical é dada por

$$\begin{aligned}
\mathrm{C2} &= \lim_{g_{\mathrm{RD}}\to\infty}\left(\frac{g_{\mathrm{RD}}\left[\delta\theta\gamma_P\mu g_{\mathrm{SR}}^2 + \delta\theta\gamma_P(1-\mu)g_{\mathrm{SR}}g_{\mathrm{RD}}\right]}{g_{\mathrm{RD}}\left\{\theta[\mu g_{\mathrm{SR}} + (1-\mu)g_{\mathrm{RD}}] + (1-\delta) + \frac{\delta g_{\mathrm{SR}}}{g_{\mathrm{RD}}}\right\}} < \tau\left(\frac{(1-\delta)g_{\mathrm{RD}}}{(1-\delta)g_{\mathrm{RD}}}\right)\right) \\
&= \lim_{g_{\mathrm{RD}}\to\infty}\left(\frac{\delta\theta\gamma_P g_{\mathrm{SR}}\left[\mu g_{\mathrm{SR}} + (1-\mu)g_{\mathrm{RD}}\right]}{\theta[\mu g_{\mathrm{SR}} + (1-\mu)g_{\mathrm{RD}}] + (1-\delta)} < \tau\right) \\
&= \lim_{g_{\mathrm{RD}}\to\infty}\left(\frac{\delta\theta\gamma_P g_{\mathrm{SR}}\left[\mu g_{\mathrm{SR}} + (1-\mu)g_{\mathrm{RD}}\right]}{\theta[\mu g_{\mathrm{SR}} + (1-\mu)g_{\mathrm{RD}}]} < \tau\right) \\
&= \delta\gamma_P g_{\mathrm{SR}} < \tau \\
&= g_{\mathrm{SR}} < \frac{\tau}{\delta\gamma_P}.
\end{aligned} \tag{35}$$

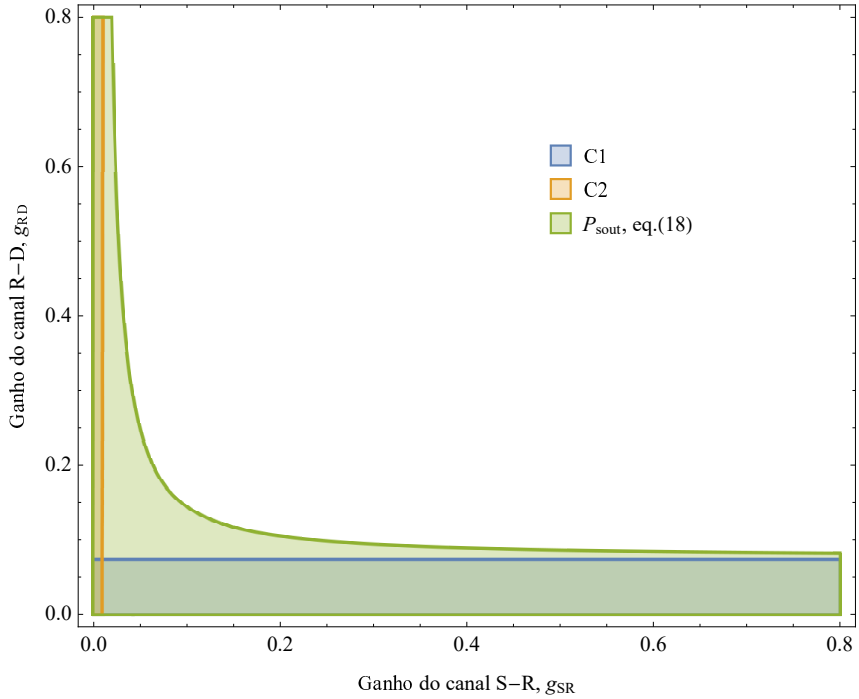

Figura 25 - Comparativo das regiões de integração retangulares propostas com a probabilidade de *outage* de sigilo exata, utilizando a estratégia SD-WET. Fonte: Elaborada pelo autor.

Ao substituir os eventos de *outage* (34) e (35) em (27), obtêm-se uma aproximação para a probabilidade de *outage* de sigilo, dada por

$$\begin{aligned} P_{\text{sout}} &\simeq \Pr(\text{C1}) + \Pr(\text{C2}) - \Pr(\text{C1})\Pr(\text{C2}) \\ &= F_{g_{\text{SR}}}\left(\frac{\tau}{\delta\gamma_P}\right) + F_{g_{\text{RD}}}\left(\frac{\tau\theta\mu + \sqrt{\tau^2\theta^2\mu^2 + 4\tau\delta(1-\delta)\theta\gamma_P\mu}}{2(1-\delta)\theta\gamma_P\mu}\right) - F_{g_{\text{SR}}}\left(\frac{\tau}{\delta\gamma_P}\right) \\ &\quad \times F_{g_{\text{RD}}}\left(\frac{\tau\theta\mu + \sqrt{\tau^2\theta^2\mu^2 + 4\tau\delta(1-\delta)\theta\gamma_P\mu}}{2(1-\delta)\theta\gamma_P\mu}\right) \end{aligned} \tag{36}$$

Assim, assumindo um cenário com regime de alta SNR, as CDFs são simplificadas utilizando a expansão da função exponencial proveniente das séries de Maclaurin, como mencionado em [42, eq. (0.318.2)]. Adicionalmente, foi negligenciado o terceiro termo, já que este é o que possui a maior taxa de decaimento relativo à γ_P. Portanto, é obtida a probabilidade de *outage* de sigilo para a estratégia SD-WET, apresentado em (24).

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Ghosh, A., Maeder, A., Baker, M., and Chandramouli, D., "5G evolution: A view on 5G cellular technology beyond 3GPP release 15," in *IEEE Access*, IEEE V.7, p. 127639 − 127651, 2019.

[2] Henry, S., Alsohaily, A. and Sousa, E. S., "5G is Real: Evaluating the Compliance of the 3GPP 5G New Radio System With the ITU IMT-2020 Requirements," in *IEEE Access*, IEEE V.8, p. 42828−42840, 2020.

[3] Agiwal,M., Roy, A. and Saxena, M., "Next Generation 5G Wireless Networks: A Comprehensive Survey," in *IEEE Commun. Surveys Tuts.*, IEEE V.18, p. 1617−1655, 2016.

[4] Yassein, M. B., Aljawarneh, S. and Al-Sadi, A., "Challenges and features of IoT communications in 5G networks," in *2017 International Conference on Elect. Comput. Techn. Appl. (ICECTA)*, p. 1−5, 2017.

[5] Vermani, S., "The next generation Internet of Things," in *2016 3rd International Conference Comput. Sustain. Global Develop. (INDIACom)*, p. 779−781, 2016.

[6] Wu, Y., Khisti, A., Xiao, C., Caire, G., Wong, K. K. and Gao, X., "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead," in *IEEE J. Sel. Areas Commun.*, IEEE, p. 1−1, 2018.

[7] Sun, L. and Du, Q., "Physical layer security with its applications in 5G networks: A review," in *China Communications*, IEEE V.14, no.12, p. 1−14, 2017.

[8] Wang, N., Wang, P., Alipour-Fanid, A., Jiao, L. and Zeng, K., "Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities," in *IEEE Internet of Things Journal*, IEEE V.6, no.5, p. 8169−8181, 2019.

[9] Li, J., Petropulu, A. P. and Weber, S., "On cooperative relaying schemes for wireless physical layer security," in *IEEE transactions on signal processing*, IEEE V.59, no.10, p. 4985−4997, 2011.

[10] Shannon, C. E., "The Bell System Technical Journal," in *Communication theory of secrecy systems*, V.28, no.4, p. 656−715, 1949.

[11] Wyner, A. D. "The wire-tap channel," in *The Bell System Technical Journal*, V.54, no.8, p. 1355−1387, 1975.

[12] Leung-Yan-Cheong, S. and Hellman, M., "The Gaussian wire-tap channel," in *IEEE Trans. Inf. Theory*, V.24, no. 4, p. 451−456, 1978.

[13] Barros, J. and Rodrigues, M. R. D.,"Secrecy Capacity of Wireless Channels," in *2006 IEEE International Symposium Inf. Theory*, p. 356−360, 2006.

[14] Sendonaris, A., Erkip, E. and Aazhang, B., "User cooperation diversity. Part I. System description," in *IEEE Trans. Commun.*, IEEE V.51, no. 11, p. 1927−1938, 2003.

[15] Laneman, J. N., Tse, D. N. C. and Wornell, G. W., "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," in *IEEE Trans. Inf. Theory*, IEEE V.50, no. 12, p. 3062−3080, 2004.

[16] Shahjabi, T. and Babu, K. V., "A cooperative mechanism for wireless energy harvesting and spectrum sharing in 5G networks," in *2017 International Conference Commun. Signal Process. (ICCSP)*, p. 0061−0065, 2017.

[17] Abrol, A. and Jha, R. K., "Power optimization in 5G networks: A step towards GrEEn communication," in *IEEE Access*, IEEE V.4, p. 1355−1374, 2016.

[18] Huang, J., Xing, C. C. and Wang, C., "Simultaneous Wireless Information and Power Transfer: Technologies, Applications, and Research Challenges," in *IEEE Commun. Mag.*, IEEE V.15, no. 11, p. 26−32, 2017.

[19] Perera, T. D. P., Jayakody, D. N. K., Sharma, S. K., Chatzinotas, S. and Li, J., "Simultaneous Wireless Information and Power Transfer (SWIPT): Recent Advances and Future Challenges," in *IEEE Commun. Surveys Tuts.*, IEEE V.20, no. 1, p. 264−302, 2018.

[20] Krikidis, I., Timotheou, S., Nikolaou, S., Zheng, G., Ng, D. W. K. and Schober, R., "Simultaneous wireless information and power transfer in modern communication systems," in *IEEE Commun. Mag.*, IEEE V.52, no. 11, p. 104−110, 2014.

[21] Nguyen, B. V. and Kim, K., "Secrecy Outage Probability of Optimal Relay Selection for Secure AnF Cooperative Networks," in *IEEE Commun. Lett.*, IEEE V.19, no. 12, p. 2086−2089, 2015.

[22] Dong, L., Han, Z., Petropulu, A. P. and Poor, H. V., "Improving Wireless Physical Layer Security via Cooperating Relays," in *IEEE Trans. Signal Process.*, IEEE V.58, no. 3, p. 1875−1888, 2010.

[23] Mabrouk, A., Tourki, K. and Hamdi, N., "Relay selection for optimized cooperative jamming scheme," in Proc. *23rd European Signal Process. Conf. (EUSIPCO)*, p. 86−89, 2015.

[24] Hu, W., Si, J. and Li, H., "Security-Reliability Tradeoff Analysis in Multisource Multirelay Cooperative Networks with Multiple Cochannel Interferers," 2018. [Online]. Available: https://www.hindawi.com/journals/wcmc/2018/2379427/

[25] Luo, G., Li, J., Liu, Z., Tao, X. and Yang, F. "Physical Layer Security with Untrusted Relays in Wireless Cooperative Networks," in *2017 IEEE Wireless Commun. Netw. Conference (WCNC)*, p. 1−6, 2017.

[26] He, X. and Yener, A., "Two-hop secure communication using an untrusted relay," in *EURASIP Journal on Wireless Communications and Networking*, V.2009, p. 1−13, 2009.

[27] Osorio, D. P. M., Olivo, E. E. B. and Alves, H., "Secrecy Performance for Multiple Untrusted Relay Networks Using Destination-Based Jamming with Direct Link," in *IEEE*

PIMRC, p. 1−5, 2018.

[28] Zhao, R., Tan, X., Chen, D.H., He, Y.C. and Ding, Z., "Secrecy performance of untrusted relay systems with a full-duplex jamming destination," in *IEEE Transactions on Vehicular Technology*, IEEE V.67, no. 12, p. 11511−11524, 2018.

[29] Zhang, C. and Chen, Y., "Wireless Power Transfer Strategies for Cooperative Relay System to Maximize Information Throughput," in *IEEE Access*, IEEE V.5, p. 2573−2582, 2017.

[30] El Shafie, A., Mabrouk, A., Tourki, K., Al-Dhahir, N. and Hamila, R., "Securing Untrusted RF-EH Relay Networks Using Cooperative Jamming Signals," in *IEEE Access*, IEEE V.5, p. 24353−24367, 2017.

[31] Yao, R., Lu, Y., Tsiftsis, T. A., Qi, N., Mekkawy, T. and Xu, F., "Secrecy Rate-Optimum Energy Splitting for an Untrusted and Energy Harvesting Relay Network," in *IEEE Access*, IEEE V.6, p. 19238−19246, 2018.

[32] Mabrouk, A., El Shafie, A., Tourki, K. and Al-Dhahir, N., "AN-aided relay-selection scheme for securing untrusted RF-EH relay systems," in *IEEE Transactions on Green Communications and Networking*, IEEE V.1, no. 4, p. 481−493, 2017.

[33] Kalamkar, S. S. and Banerjee, A., "Secure communication via a wireless energy harvesting untrusted relay," in *IEEE Transactions on Vehicular Technology*, IEEE V.66, no. 3, p. 2199−2213, 2016.

[34] Shi, H., Cai, Y., Chen, D., Hu, J., Yang, W. and Yang, W., "Physical layer security in an untrusted energy harvesting relay network," in *IEEE Access*, IEEE V.7, p. 24819−24828, 2019.

[35] Egashira, E. N., Olivo, E. E. B. and Osorio, D. P. M., "Desempenho de outage de sigilo para redes AF com relay não confiável usando WET e jamming baseados no destino," in *XXXVII Simpósio Brasileiro de Telecomunicações (SBrT)*, p. 1−5, 2019.

[36] ©2019 IEEE. Reprinted, with permission, from Egashira, E. N., Olivo, E. E. B., Osorio, D. P. M., and Alves, H., "Secrecy Performance of Untrustworthy AF Relay Networks using Cooperative Jamming and SWIPT," in *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, p. 1−6, 2019.

[37] Guo, J., Durrani, S., Zhou, X. and Yanikomeroglu, H., "Outage probability of ad hoc networks with wireless information and power transfer," in *IEEE Wireless Communications Letters*, IEEE V.4, no. 4, p. 409−412, 2015.

[38] Rappaport, T. S., Comunicações Sem Fio: Princípios e Práticas. São Paulo, SP, Brasil, Pearson, 2008.

[39] Xing, H., Chu, Z., Ding, Z., and Nallanathan, A., "Harvest-and-jam: Improving security for wireless energy harvesting cooperative networks," in Proc. *IEEE GLOBECOM*, p. 3145−3150, 2014.

[40] Chen, Z., Cai, L. X., Cheng, Y., and Shan, H., "Sustainable Cooperative Communication

in Wireless Powered Networks With Energy Harvesting Relay," in *IEEE Trans. Wireless Commun.*, IEEE V.16, no. 12, p. 8175−8189, 2017.

[41] Ding, Z., Krikidis, I., Sharif, B., and Poor, H. V., "Impact of channel state information on wireless energy harvesting cooperative networks with spatially random relays," in Proc. *IEEE ICC*, p. 4072−4076, 2014.

[42] Gradshteyn, I.S. and Ryzhik, I.M. Table of Integrals, series and products. New York, NY, USA, Elsevier, 2007