Desempenho de Outage de Sigilo para Redes AF com Relay não Confiável usando WET e Jamming Baseados no Destino

Edson Nobuyuki Egashira, Edgar Eduardo Benitez Olivo e Diana Pamela Moya Osorio

***Resumo*— Neste trabalho, o desempenho em termos da probabilidade de *outage* de sigilo para uma rede cooperativa composta por uma fonte, um destino e um *relay* que opera sob o protocolo amplifica-e-encaminha é investigado. O *relay* é considerado como não confiável e, potencialmente, pode tentar decodificar a informação proveniente da fonte para seu próprio benefício. Além disso, uma técnica de transferência de energia sem fio é considerada, em que o *relay* é energizado através do sinal enviado pelo destino, e, para tanto, o protocolo de comutação no tempo (*time switching*) é usado. Nesse sistema é adotado um esquema de *jamming* baseado no destino para prevenir que o *relay* não confiável obtenha informação a partir da mensagem da fonte. Os resultados mostram o impacto de diferentes parâmetros-chave do sistema no desempenho de sigilo, como o fator de alocação de tempo entre as fases de transferência de informação e de energia, o fator de alocação de potência entre a fonte e o destino, para a transmissão do sinal de informação e de jamming, respectivamente, e a posição do *relay*. Para o modelo proposto, uma expressão analítica aproximada em forma integral e uma expressão assintótica compacta em forma fechada no regime de alta relação sinal-ruído são derivadas. A acurácia das expressões obtidas é verificada por meio de simulações de Monte Carlo, considerando distintos casos ilustrativos.**

***Palavras-Chave*— *Jamming* baseado no destino, probabilidade de *outage* de sigilo, *relay* não confiável, segurança na camada física, transferência de energia sem fio.**

***Abstract*— In this paper, the secrecy outage performance of a cooperative network consisting of a source, a destination and a relay operating under the amplify-and-forward protocol is investigated. The relay is assumed to be untrustworthy, and, potentially can decode the information from the source for its own benefit. Furthermore, a wireless energy transfer technique is considered, whereby the relay is energized from the destination, and, for this purpose, a time switching protocol is used. In this system, a cooperative-destination-based jamming scheme is adopted to prevent the relay from obtaining information of the source's message. The results show the impact of key system parameters on the secrecy performance, such as the time allocation factor between the information and energy transfer phases, the power allocation factor between the source and destination, for the transmission of information and jamming signals, and the relay position. For the proposed system, an approximate analytical expression in integral form and a compact closed-form asymptotic expression at high signal-to-noise ratio are derived. The accuracy of the performed analysis is corroborated by Monte Carlo simulations, considering different illustrative cases.**

Edson Nobuyuki Egashira e Edgar Eduardo Benitez Olivo, Universidade Estadual Paulista (UNESP), Câmpus de São João da Boa Vista, São João da Boa Vista-SP, Brasil. E-mails: edson.egashira@unesp.br, edgar.olivo@unesp.br. Diana Pamela Moya Osorio, Departamento de Engenharia Elétrica, Centro de Ciências Exatas e de Tecnologia, Universidade Federal de São Carlos (UFSCar), São Carlos-SP, Brasil. E-mail: dianamoya@ufscar.br. Este trabalho foi financiado parcialmente pela CAPES - código de financiamento 001 e pelo CNPq (421850/2018-3 e 428649/2016-5).

***Keywords*— Destination based *jamming*, secrecy outage probability, untrustworthy *relay*, physical layer security, wireless energy transfer.**

I. Introdução

Nas redes de quinta geração e de gerações futuras (5GB, *5G and beyond*), uma das maiores preocupações é a segurança da informação e a privacidade, uma vez que um grande volume de dados confidenciais serão transportados por estas redes. A partir dos fundamentos da teoria da informação, uma nova abordagem tem emergido de forma a fortalecer a segurança das redes [1]. Esta abordagem é conhecida como segurança na camada física (PLS, *physical layer security*), cuja ideia básica consiste em aproveitar as propriedades físicas do canal sem fio, de modo a oferecer um nível adicional de proteção além dos esquemas de criptografia e segurança de camada superior existentes [2].

Nesse sentido, as técnicas de comunicação cooperativa baseadas em *relays* têm sido exploradas para melhorar o desempenho em termos da segurança de uma rede sem fio [3]. Apesar de todas as vantagens das comunicações cooperativas, por vezes os *relays* podem, eventualmente, vazar informação para seu próprio beneficio, tornando-se possíveis espiões na comunicação entre fonte e destino. A fim de contornar esse problema e melhorar o sigilo da comunicação no sistema, a técnica de *jamming* baseado no destino (DBJ, *destination-based jamming*) pode ser explorada [4]. De acordo com essa técnica, o destino envia um ruído artificial ao *relay* de forma que este não consiga recuperar a informação.

Por outro lado, junto aos requerimentos exigentes em questão da segurança para as redes 5G, a implementação de redes de comunicação do tipo máquina (MTC, *machine-type communication*), que deverão suportar um número massivo de dispositivos pequenos e de baixo custo, traz a importância de dotar de sustentabilidade energética a estas redes. Nesse contexto, a técnica referida como *energy harvesting* (EH) tem-se mostrado promissora para atingir esses requisitos de eficiência energética. EH consiste na captação de energia a partir de fontes externas e sua conversão em energia elétrica [5]. Dentre essas fontes, a transferência de energia por sinais de radiofrequência (RF) a partir de dispositivos remotos, conhecida como transferência de energia sem fio (WET, *wireless energy transfer*), pode ajudar a atender os requisitos de qualidade de serviço das redes do tipo MTC.

A implementação de um sistema de comunicação baseado em WET implica na divisão do sinal recebido em duas partes:

uma para EH e outra para a transmissão de informação (IT, information transmission), resultando em um esquema de transferência sem fio simultânea de informação e potência (SWIPT, simultaneous wireless information and power transfer). Assim, uma das técnicas principais para a implementação de SWIPT é referida como comutação no tempo (TS, *time switching*), que consiste na alocação de um intervalo de tempo para EH e outro para IT. Considerando isto, esquemas SWIPT têm sido estudados em cenários de comunicação cooperativa onde os *relays* são energizados apenas por sinais RF, como em [6], em que diversas estratégias de alimentação do *relay* são analisadas, sendo uma delas através do destino (D-WPT). Já em [7], foi proposto um esquema cooperativo com um *relay* não confiável e um nó externo, onde ambos são energizados pela fonte e pelo destino utilizando a técnica TS. Nesse trabalho, o desempenho em termos da probabilidade de *outage* e da probabilidade de interceptação é comparado, para estratégias distintas de *jamming*. Em [8], foi analisada a capacidade de sigilo ergódica e a probabilidade de *outage* de sigilo de uma rede cujo *relay* não confiável é energizado via protocolo TS. Também, o desempenho foi comparado com esquema SWIPT por de divisão de potência (PS, *power splitting*).

No presente trabalho, pretende-se contribuir com o estudo do desempenho em termos de segurança para redes cooperativas de dois saltos (*dual hop*), onde o *relay* é energizado via sinais RF a partir do destino. Para tanto, o protocolo TS é adotado, sendo, nesse caso, o destino o encarregado de transmitir um sinal RF para energizar o *relay* durante a fase de EH e, posteriormente, a fonte é responsável por transmitir o sinal de informação na fase de IT. Assim, a energia armazenada pelo *relay* durante a fase de EH é utilizada para retransmitir a informação ao destino. Além disso, um esquema DBJ é considerado, onde o destino envia um sinal de *jamming* para impedir que o *relay*, considerado como não confiável, consiga decodificar e vazar a informação proveniente da fonte. O desempenho deste sistema é avaliado em termos da probabilidade de *outage* de sigilo, para o qual uma expressão analítica aproximada em forma integral e uma expressão assintótica compacta em forma fechada são obtidas. Essas expressões são validadas por simulações de Monte Carlo, considerando casos ilustrativos.

Notação: $f_A(\cdot)$ e $F_A(\cdot)$ denotam a função densidade de probabilidade (PDF, *probability density function*) e a função distribuição acumulada (CDF, *cumulative distribution function*) de uma variável aleatória A, respectivamente, $\mathrm{E}\{\cdot\}$ é o operador esperança, $\Pr(\cdot)$ denota probabilidade, $\mathcal{CN}(a,b)$ denota a distribuição Gaussiana complexa e circularmente simétrica de média a e variância b e $[c]^+ \triangleq \max\{0,c\}$.

II. Modelo do Sistema

A Fig. 1 ilustra uma rede cooperativa com uma fonte S, um destino D e um *relay* R do tipo amplifica-e-encaminha (AF, *amplify-and-forward*) operando em modo de transmissão *half duplex* (HD). Todos os nós da rede são considerados dispositivos de antena única e operam por meio de acesso múltiplo por divisão de tempo (TDMA, *time division multiple access*). Além disso, assume-se que o enlace direto S→D se encontra severamente atenuado, de modo que a comunicação entre S e D é possível unicamente através do enlace de retransmissão.

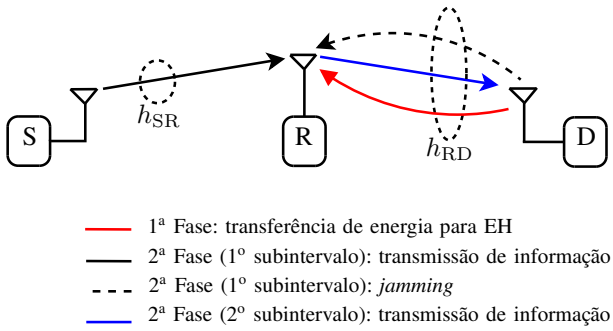

Fig. 1. Modelo do sistema.

Nesse sistema, o *relay* é energizado por sinais RF provenientes de D, seguindo um protocolo TS com a técnica D-WPT. Portanto, o processo de comunicação entre S e D, realizado em um intervalo de tempo igual a T, é dividido em duas fases: (i) fase de transferência de energia para EH e (ii) fase de IT. De acordo com o protocolo TS, as duas fases são realizadas em intervalos de tempo distintos cuja duração depende de um fator de alocação de tempo $\alpha \in (0,1)$. Na fase de EH, D energiza R durante o intervalo de tempo αT. Já a fase de IT tem uma duração de $(1-\alpha)T$ e, por sua vez, divide-se em duas subfases de duração igual a $(1-\alpha)T/2$. Durante a primeira subfase, S envia o sinal da informação para R, enquanto D envia um sinal de *jamming*, para interferir o próprio *relay*. Na segunda subfase, R retransmite uma versão amplificada do sinal recebido de S, combinado ao sinal de *jamming*, utilizando toda a energia armazenada durante a fase de EH. Na recepção, assume-se que D consegue cancelar eficazmente o sinal de jamming, uma vez que o sinal é perfeitamente conhecido por D.

Adicionalmente, nesse sistema considera-se que todos os canais estão sujeitos a desvanecimento quase-estático e plano do tipo Rayleigh e a a ruido aditivo gaussiano e branco (AGWN) com potência média N_0. Consequentemente, os coeficientes de canal correspondentes aos enlaces S→R e R→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, $h_i \sim \mathcal{CN}(0,\Omega_i)$, em que $\Omega_i = \mathrm{E}\{|h_i|^2\}$ é o ganho médio do canal. Assim, $g_{\mathrm{SR}} \triangleq |h_{\mathrm{SR}}|^2$ e $g_{\mathrm{RD}} \triangleq |h_{\mathrm{RD}}|^2$ denotam os ganhos instantâneos do canal. Portanto, as relações sinal-ruído (SNRs, *signal-to-noise ratios*) transmitidas nos enlaces S→R e R→D são dadas por $\gamma_{\mathrm{S}}{=}P_{\mathrm{S}}/N_0$ e $\gamma_{\mathrm{R}}{=}P_{\mathrm{R}}/N_0$, em que P_{S} e P_{R} são as potências transmitidas em S e R, respectivamente. Além da consideração de desvanecimento quase-estático, assume-se que existe reciprocidade nos enlaces R→D e D→R. Considera-se ainda que a SNR transmitida em D é dada por $\gamma_{\mathrm{D}}{=}P_{\mathrm{D}}/N_0$. Nesse sistema, considera-se que a potência transmitida total durante a fase de EH e a 1ª subfase de IT é igual a P, sendo portanto, a SNR transmitida do sistema dada por $\gamma_{\mathrm{P}} = P/N_0$. Dessa maneira, durante a primeira subfase de IT é necessário dividir a potência P entre S e D, considerando, para tanto, um fator de alocação

de potência $\delta \in (0,1)$. Assim, $P_{\rm S} = \delta P$ e $P_{\rm D} = (1-\delta)P$. Por outro lado, a energia armazenada em R a partir do sinal vindo de D, durante a fase de EH, é dada por

$$E_{\rm R} = \eta\alpha T P g_{\rm RD}, \tag{1}$$

onde $\eta \in (0,1]$ é o fator de eficiência de conversão de energia. Portanto, a potência transmitida em R é dada por

$$P_{\rm R} = \frac{E_{\rm R}}{(1-\alpha)T/2} \overset{(a)}{=} \frac{2\eta\alpha P g_{\rm RD}}{(1-\alpha)} \overset{(b)}{=} \theta P g_{\rm RD}, \tag{2}$$

onde no passo (a), substituiu-se $E_{\rm R}$ por (1) e no passo (b) definiu-se $\theta = 2\alpha\eta/(1-\alpha)$.

III. Modelo de Sinais

Sob as considerações expostas na seção anterior, nesta seção serão modelados os sinais recebidos em R e D, a fim de determinar as SNRs recebidas correspondentes.

Durante a primeira subfase de IT, o sinal recebido em R é dado por

$$y_{\rm R}(t) = \sqrt{P_{\rm S}} h_{\rm SR} s_{\rm I}(t) + \sqrt{P_{\rm D}} h_{\rm RD} s_{\rm J}(t) + n_{\rm R}(t), \tag{3}$$

em que $s_{\rm I}(t)$ é o sinal de informação, $s_{\rm J}(t)$ é o sinal de jamming e $n_{\rm R}(t)$ é a componente de ruido em R. Além disso, considerando o protocolo AF, o sinal recebido em D durante a segunda subfase de IT é dado por

$$y_{\rm D}(t) = \sqrt{P_{\rm R}} h_{\rm RD} \mathcal{G} y_{\rm R}(t) + n_{\rm D}(t), \tag{4}$$

em que $n_{\rm D}(t)$ é a componente de ruído em D, e $\mathcal{G}$ é o fator de amplificação inerente ao protocolo AF, dado por

$$\mathcal{G} = \sqrt{\frac{1}{P_{\rm S} g_{\rm SR} + P_{\rm D} g_{\rm RD} + N_0}}, \tag{5}$$

que é obtido ao se considerar sinais com potência unitária normalizada, ou seja, $\mathrm{E}\{|s_{\rm I}(t)|^2\}=\mathrm{E}\{|s_{\rm J}(t)|^2\}=1$, e o fato que $\mathrm{E}\{|\mathcal{G} y_{\rm R}(t)|^2\}=1$. Assim, substituindo (3) em (4) e considerando que D é capaz de cancelar efetivamente o sinal de jamming, tem-se que o sinal recebido em D pode ser expresso como

$$\begin{aligned} y_{\rm D}(t_2) = \sqrt{P_{\rm R}} \mathcal{G} h_{\rm RD} \big[\sqrt{P_{\rm S}} h_{\rm SR} s_{\rm I}(t_1) \\ + \sqrt{P_{\rm D}} h_{\rm RD} s_{\rm J}(t_1) + n_{\rm R}(t_1) \big] + n_{\rm D}(t_2). \end{aligned} \tag{6}$$

Portanto, de (6), a SNR fim-a-fim recebida no enlace legítimo é dada por

$$\Gamma_\ell = \frac{P_{\rm R} g_{\rm RD} \mathcal{G}^2 P_{\rm S} g_{\rm SR}}{P_{\rm R} g_{\rm RD} \mathcal{G}^2 N_0 + N_0} \overset{(c)}{=} \frac{\gamma_{\rm S}\gamma_{\rm R} g_{\rm SR} g_{\rm RD}}{\gamma_{\rm R} g_{\rm RD} + \gamma_{\rm S} g_{\rm SR} + \gamma_{\rm D} g_{\rm RD} + 1}, \tag{7}$$

onde, no passo (c), substitui-se o ganho $\mathcal{G}$ por (5) e realizou-se algumas manipulações algébricas. Note a partir de (2) que $\gamma_{\rm R}$ é uma função do ganho de canal $g_{\rm RD}$, referente ao enlace R→D.

A SNR recebida no enlace de escuta pelo *relay* não confiável durante a primeira subfase de IT pode ser obtido a partir de (3) como

$$\Gamma_e = \frac{P_{\rm S} g_{\rm SR}}{P_{\rm D} g_{\rm RD} + N_0} = \frac{\gamma_{\rm S} g_{\rm SR}}{\gamma_{\rm D} g_{\rm RD} + 1}. \tag{8}$$

IV. Probabilidade de outage de sigilo

Nesta seção, a probabilidade de *outage* de sigilo para o sistema com *relay* não confiável sob estudo é analisada. Para tanto, da definição de capacidade de sigilo, C_s, como a taxa máxima de transmissão que pode ser alcançada para uma comunicação segura, dada pela diferença entre a capacidade do canal legítimo C_ℓ e a capacidade do canal de escuta (nesse caso, o primeiro salto do canal de *relaying*) C_e, tem-se que

$$C_s = [C_\ell - C_e]^+ = \frac{1}{2}\log_2\left(\frac{1+\Gamma_\ell}{1+\Gamma_e}\right). \tag{9}$$

Assim, a probabilidade de *outage* de sigilo define-se como a probabilidade da capacidade de sigilo em (9) ser menor que uma dada taxa de sigilo alvo $\mathcal{R}$. Portanto, de (7) e (8), segue que

$$\begin{aligned} P_{\rm sout} &= \Pr\left(\frac{1}{2}\log_2\left(\frac{1+\Gamma_\ell}{1+\Gamma_e}\right) < \mathcal{R}\right), \\ &= \Pr\left(\frac{1+\frac{\gamma_{\rm S}\gamma_{\rm R} g_{\rm SR} g_{\rm RD}}{\gamma_{\rm R} g_{\rm RD} + \gamma_{\rm S} g_{\rm SR} + \gamma_{\rm D} g_{\rm RD} + 1}}{1+\frac{\gamma_{\rm S} g_{\rm SR}}{\gamma_{\rm D} g_{\rm RD}+1}} < 2^{2\mathcal{R}} \triangleq \tau\right). \end{aligned} \tag{10}$$

De (10), uma análise exata da probabilidade de *outage* de sigilo para o sistema considerado resulta ser um problema intrincado. A seguir, uma aproximação em forma de integrais simples e uma expressão em forma fechada derivada de uma análise assintótica para o regime de alta SNR são obtidas nas Proposições 1 e 2, respectivamente.

Proposição 1: Uma expressão analítica aproximada para a probabilidade de *outage* de sigilo de uma rede cooperativa com o *relay* AF não confiável, utilizando DBJ e D-WPT via protocolo TS é dada por

$$\begin{aligned} &P_{\rm sout} \\ &= F_{g_{\rm SR}}(g_{\rm SR1}) + \int_{g_{\rm SR1}}^{g_{\rm SR2}} F_{g_{\rm RD}}\Bigg(\frac{1}{2}\Bigg(\frac{(1-\delta)^4\tau^2}{(1-\delta)^2\theta^2(\delta x\gamma_P-\tau)^2} \\ &+ \frac{4\delta^2(1-\delta)^2\theta\tau x^2\gamma_P + \delta^2\theta^2\tau^2x^2 - 2\delta(1-\delta)^2\theta\tau^2 x}{(1-\delta)^2\theta^2(\delta x\gamma_P-\tau)^2}\Bigg)^{\frac{1}{2}} \\ &+ \frac{-(1-\delta)^2\tau - \delta\theta\tau x}{2(1-\delta)\theta(\tau-\delta x\gamma_P)}\Bigg) f_{g_{\rm SR}}(x)dx + \int_{g_{\rm SR2}}^{\infty} F_{g_{\rm RD}}\Bigg(\Bigg(\frac{\delta}{(1-\delta)} \\ &\times \frac{\tau x}{2\theta\gamma_P} + \left(\frac{\delta^2\tau^2x^2}{4(1-\delta)^2\theta^2\gamma_P^2} - \frac{\tau^3}{27\theta^3\gamma_P^3}\right)^{\frac{1}{2}}\Bigg)^{\frac{1}{3}} + \frac{\tau}{3\theta\gamma_P} \\ &\times \left(\frac{\delta\tau x}{2(1-\delta)\theta\gamma_P} + \left(\frac{\delta^2\tau^2x^2}{4(1-\delta)^2\theta^2\gamma_P^2} - \frac{\tau^3}{27\theta^3\gamma_P^3}\right)^{\frac{1}{2}}\right)^{-\frac{1}{3}}\Bigg) \\ &\times f_{g_{\rm SR}}(x)dx, \end{aligned} \tag{11}$$

em que

$$\begin{aligned} g_{\rm SR1} &= \frac{\tau}{\gamma_P\delta}, \\ g_{\rm SR2} &= \frac{\theta\tau^2 + 5(1-\delta)^2\tau\gamma_P}{2\delta(1-\delta)^2\gamma_P^2} + \frac{1}{2}\Bigg(\frac{\theta^3\tau^4 + 8(1-\delta)^6\tau\gamma_P^3}{\delta^2(1-\delta)^4\theta\gamma_P^4} \\ &\quad + \frac{17(1-\delta)^4\theta\tau^2\gamma_P^2 + 10(1-\delta)^2\theta^2\tau^3\gamma_P}{\delta^2(1-\delta)^4\theta\gamma_P^4}\Bigg)^{\frac{1}{2}}. \end{aligned}$$

Demonstração: Vide Apêndice I. ∎

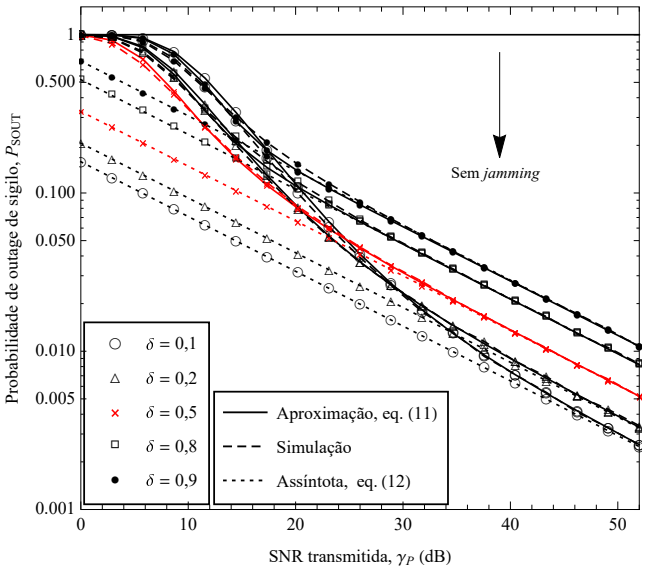

Fig. 2. Probabilidade de outage de sigilo em função da SNR transmitida γ_P, para diferentes valores de δ, considerando $\alpha = 0{,}5$.

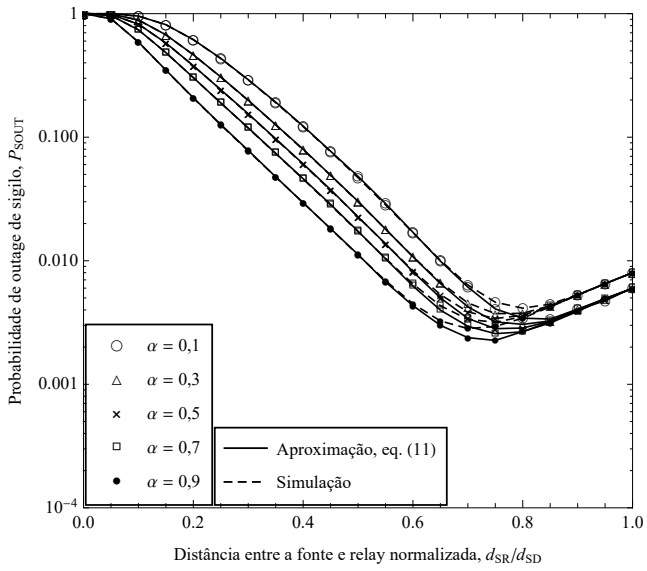

Fig. 3. Probabilidade de outage de sigilo em função da distância entre a fonte e o *relay* $d_{\text{SR}}/d_{\text{SD}}$, para diferentes valores de α, considerando $\delta = 0{,}5$ e $\gamma_P = 30$ dB.

Proposição 2: Uma expressão analítica assintótica compacta em forma fechada para a probabilidade de *outage* de sigilo de uma rede cooperativa com o *relay* AF não confiável, utilizando DBJ e D-WPT via protocolo TS é dada por

$$P_{\text{sout}} = \frac{\left(\frac{\delta\tau}{(1-\delta)\gamma_P\theta}\right)^{\frac{1}{3}} \Omega_{\text{SR}}^{\frac{4}{3}}\Gamma(\frac{4}{3})}{\Omega_{\text{SR}}\Omega_{\text{RD}}}. \quad (12)$$

Demonstração: Vide Apêndice II. ■

V. Resultados Numéricos e Discussões

Nesta seção, 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 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 $d_{SR} = 0{,}5$, $d_{RD} = 0{,}5$ e $d_{SD} = 1$, respectivamente. Considera-se que o ganho médio de canal de todos os enlaces é determinado pela perda de percurso, isto é, $\Omega_i = d_i^{\beta}$, para $i \in \{SR, RD\}$, em que d_i é a distância entre dois nós e $\beta = 4$ é o expoente de perda de percurso. Além disso, assume-se que a taxa de sigilo alvo é fixada em $\mathcal{R} = 1$ bps/Hz e o fator de eficiência de energia é fixado em $\eta = 0{,}5$.

Na Fig. 2 é ilustrada a probabilidade de *outage* de sigilo em função da SNR transmitida do sistema γ_P, para diferentes valores do fator de alocação de potência entre fonte e destino. As expressões analíticas aproximada e assintótica são confrontadas com os resultados obtidos por simulação, apresentando excelentes resultados. Observe que, na região de alta SNR, o desempenho do sistema melhora conforme menos potência é alocada para a fonte, enquanto que, na região de baixa SNR, uma alocação igual de potência entre fonte e destino ($\delta = 0{,}5$) fornece o melhor desempenho de sigilo do sistema. Além disso, observa-se que o uso da técnica DBJ é essencial para conseguir uma transmissão segura neste sistema, quando comparado ao caso sem *jamming*.

A Fig. 3, ilustra a probabilidade de *outage* de sigilo em função da distância normalizada de R em relação a S, $d_{\text{SR}}/d_{\text{SD}}$, para diferentes valores do fator de alocação de tempo α, com $\delta = 0{,}5$ e $\gamma_P = 30$ dB. Observa-se que o desempenho de sigilo aumenta conforme α aumenta (ou seja, mais tempo é alocado à fase de EH). Além disso, a melhor estratégia para fornecer sigilo na comunicação, usando a técnica D-WPT, é posicionar o *relay* mais próximo do destino. Observe também que a aproximação proposta caracteriza perfeitamente o comportamento do sistema para uma ampla faixa de valores da posição relativa de R, aproximadamente até $d_{SR}/d_{SD} \approx 0,7$.

VI. Conclusões

Neste trabalho, o desempenho em termos da probabilidade de *outage* de sigilo para uma rede cooperativa com um *relay* AF não confiável foi analisado. Considerou-se o uso da técnica DBJ para fornecer segurança de camada física na comunicação entre fonte e destino. Considerou-se ainda que o *relay* é energizado via protocolo TS a partir do destino. Uma aproximação em forma integral e uma expressão assintótica em forma fechada e compacta foram derivadas. A acurácia das expressões analíticas obtidas foi validada por meio de simulações de Monte Carlo. Neste sistema foi investigado o impacto do tempo de carregamento do *relay*, o fator de alocação de potência entre a fonte e o destino durante a fase de IT, assim como da posição relativa do *relay* em relação a fonte. Dos resultados foi observado que a técnica DBJ é essencial para transmitir informação de forma segura. Observou-se ainda que, no regime de baixa SNR, uma estratégia de alocação igual de potência entre fonte e destino forneceu o melhor desempenho de sigilo. Além disso, observou-se que a segurança do processo de comunicação é melhorada conforme o *relay* é posicionado mais próximo do destino.

APÊNDICE I
DEMONSTRAÇÃO DA PROPOSIÇÃO 1

Considerando o regime de média-a-alta SNR, após algumas manipulações algébricas, e aplicando a relação $\min\{X,Y\} \geq XY/(X+Y+1)$ [4], a probabilidade de *outage* de sigilo em (10) pode ser expressa como

$$\begin{aligned}
P_{\text{sout}} &= \Pr\left(\frac{\frac{\gamma_{\text{R}}}{\gamma_{\text{R}}+\gamma_{\text{D}}}}{1+\frac{\gamma_{\text{S}}g_{\text{SR}}}{\gamma_{\text{D}}g_{\text{RD}}+1}}\min\{\gamma_{\text{S}}g_{\text{SR}},(\gamma_{\text{R}}+\gamma_{\text{D}})g_{\text{RD}}\}<\tau\right)\\
&= \Pr\left(\frac{\gamma_{\text{R}}}{\gamma_{\text{R}}+\gamma_{\text{D}}}\min\{\gamma_{\text{S}}g_{\text{SR}},(\gamma_{\text{R}}+\gamma_{\text{D}})g_{\text{RD}}\}\right.\\
&\qquad \left.<\tau\left(1+\frac{\gamma_{\text{S}}g_{\text{SR}}}{\gamma_{\text{D}}g_{\text{RD}}+1}\right)\right)\\
&\overset{(d)}{=} \Pr\left(\frac{\theta\gamma_P g_{\text{RD}}}{\theta\gamma_P g_{\text{RD}}+(1-\delta)\gamma_P}\right.\\
&\qquad \times\min\{\delta\gamma_P g_{\text{SR}},[\theta\gamma_P g_{\text{RD}}+(1-\delta)\gamma_P]g_{\text{RD}}\}\\
&\qquad \left.<\tau\left(\frac{(1-\delta)\gamma_P g_{\text{RD}}+1+\delta\gamma_P g_{\text{SR}}}{(1-\delta)\gamma_P g_{\text{RD}}+1}\right)\right)\\
&= \Pr\left(\frac{\theta\gamma_P g_{\text{RD}}}{\theta g_{\text{RD}}+1-\delta}\min\{\delta g_{\text{SR}},[\theta g_{\text{RD}}+(1-\delta)]g_{\text{RD}}\}\right.\\
&\qquad \left.<\tau\left(\frac{(1-\delta)g_{\text{RD}}+\frac{1}{\gamma_P}+\delta g_{\text{SR}}}{(1-\delta)g_{\text{RD}}+\frac{1}{\gamma_P}}\right)\right)\\
&\overset{(e)}{=} \Pr\left(\min\{\delta g_{\text{SR}},[\theta g_{\text{RD}}+(1-\delta)]g_{\text{RD}}\}\right.\\
&\qquad \left.<\tau\left(\frac{(1-\delta)g_{\text{RD}}+\delta g_{\text{SR}}}{\gamma_P(1-\delta)g_{\text{RD}}}\right)\left(\frac{\theta g_{\text{RD}}+1-\delta}{\theta g_{\text{RD}}}\right)\right),
\end{aligned} \tag{13}$$

onde, no passo (d) considerou-se que $\gamma_{\text{R}} = P_{\text{R}}/N_0 = \theta P g_{\text{RD}}$, sendo θ dado em (2) e, no passo (e), os termos $1/\gamma_P$ do passo anterior foram desprezados.

As expressões referentes a probabilidade de *outage* de sigilo foram obtidas através das regiões de integração para os eventos de *outage* no argumento de $\Pr(\cdot)$ em (13). Para resolver o termo $\min\{\cdot,\cdot\}$ desta expressão, foram considerados os seguintes eventos: (i) $\delta g_{\text{SR}} < (\theta g_{\text{RD}}+1-\delta)g_{\text{RD}}$ e (ii) $\delta g_{\text{SR}} > (\theta g_{\text{RD}}+1-\delta)g_{\text{RD}}$. Para a primeira condição, a região de integração é dada por

$$\begin{aligned}
&\mathcal{R}_1\\
&= 0<g_{\text{SR}} \leq \frac{\tau}{\gamma_P\delta}\bigcap\theta\left[1-\delta+2\theta g_{\text{RD}}-\left((1-\delta)^2+4\delta\theta g_{\text{SR}}\right)^{\frac{1}{2}}\right]\\
&> 0\bigcup\left\{g_{\text{SR}} > \frac{\tau}{\gamma_P\delta}\bigcap\frac{1}{\gamma_P^2\delta(1-\delta)^2}\left\{\theta\tau\left[\left(\frac{8\tau\gamma_P(1-\delta)^2}{\theta}\right.\right.\right.\right.\\
&\left.\left.\left.\left.+\tau^2\right)^{\frac{1}{2}}+\tau\right]+\gamma_P(1-\delta)^2\left[\left(\frac{8\tau\gamma_P(1-\delta)^2}{\theta}+\tau^2\right)^{\frac{1}{2}}+5\tau\right]\right\}\right.\\
&> 2g_{\text{SR}}\bigcap\frac{\sqrt{(1-\delta)^2+4\delta\theta g_{\text{SR}}}-1+\delta}{2\theta} < g_{\text{RD}} < \left[(1-\delta)^2\tau\right.\\
&+\delta\theta\tau g_{\text{SR}}+\sqrt{\tau}\left(\gamma_P\delta g_{\text{SR}}-\tau\right)\left(\frac{4\gamma_P\delta^2(1-\delta)^2\theta g_{\text{SR}}^2}{(\tau-\gamma_P\delta g_{\text{SR}})^2}\right.\\
&\left.\left.+\frac{\tau\left[(1-\delta)^2-\delta\theta g_{\text{SR}}^2\right]}{(\tau-\gamma_P\delta g_{\text{SR}})^2}\right)^{\frac{1}{2}}\right]\left(\frac{1}{2(1-\delta)\theta(\gamma_P\delta g_{\text{SR}}-\tau)}\right)\Bigg\}.
\end{aligned} \tag{14}$$

Para a segunda condição, a região de integração é dada por

$$\begin{aligned}
&\mathcal{R}_2\\
&= \left\{g_{\text{RD}}<\left[\frac{\tau\delta g_{\text{SR}}}{2(1-\delta)\theta\gamma_P}\left(\frac{\delta^2 g_{\text{SR}}^2\tau^2}{4\theta^2\gamma_P^2(1-\delta)^2}-\frac{\tau^3}{27\gamma_P^3\theta^3}\right)^{\frac{1}{2}}\right]^{\frac{1}{3}}\right.\\
&+\frac{\tau}{3\theta\gamma_P}\left[\frac{\tau\delta g_{\text{SR}}}{2(1-\delta)\theta\gamma_P}\left(\frac{\delta^2 g_{\text{SR}}^2\tau^2}{4\theta^2\gamma_P^2(1-\delta)^2}-\frac{\tau^3}{27\gamma_P^3\theta^3}\right)^{\frac{1}{2}}\right]^{-\frac{1}{3}}\\
&\bigcap\frac{1}{\gamma_P^2\delta(1-\delta)^2}\left\{\theta\tau\left[\left(\frac{8\tau\gamma_P(1-\delta)^2}{\theta}+\tau^2\right)^{\frac{1}{2}}+\tau\right]\right.\\
&\left.+\gamma_P(1-\delta)^2\left[\left(\frac{8\tau\gamma_P(1-\delta)^2}{\theta}+\tau^2\right)^{\frac{1}{2}}+5\tau\right]\right\}<2g_{\text{SR}}\Bigg\}\\
&\bigcup\left\{0<g_{\text{RD}}<\frac{1}{2}\sqrt{\frac{(1-\delta)^2+4\delta\theta g_{\text{SR}}}{\theta^2}}-\frac{1-\delta}{2\theta}\right.\\
&\bigcap\frac{1}{\gamma_P^2\delta(1-\delta)^2}\left\{\theta\tau\left[\left(\frac{8\tau\gamma_P(1-\delta)^2}{\theta}+\tau^2\right)^{\frac{1}{2}}+\tau\right]\right.\\
&\left.\left.+\gamma_P(1-\delta)^2\left[\left(\frac{8\tau\gamma_P(1-\delta)^2}{\theta}+\tau^2\right)^{\frac{1}{2}}+5\tau\right]\right\}\geq 2g_{\text{SR}}\right\}.
\end{aligned} \tag{15}$$

Desta forma, após a solução das integrais definidas a partir das regiões dadas em (14) e (15), uma aproximação para a probabilidade de *outage* de sigilo é obtida como em (11).

APÊNDICE II
DEMONSTRAÇÃO DA PROPOSIÇÃO 2

Considerando que os termos proporcionais a $1/\gamma_P$ e $1/\gamma_P^2$ em (11) tendem a zero no regime de alta SNR, e usando a aproximação assintótica para a função exponencial baseada nas séries de Maclaurin, em que $e^{-x} \simeq 1-x$, para $x \to 0$ [9, eq. (0.318.2)], após a solução das integrais resultantes, uma expressão assintótica em forma fechada para a probabilidade de *outage* de sigilo é obtida como em (12).

REFERÊNCIAS

[1] A. Mukherjee, "Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints," *Proc. IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.

[2] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, pp. 1–1, 2018.

[3] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[4] D. P. Moya Osorio, E. E. Benitez Olivo, and H. Alves, "Secrecy performance for multiple untrusted relay networks using destination-based jamming with direct link," in *IEEE PIMRC*, Sep. 2018, pp. 1–5.

[5] J. Huang, C. C. Xing, and C. Wang, "Simultaneous wireless information and power transfer: Technologies, applications, and research challenges," *IEEE Commun. Mag.*, vol. 55, no. 11, pp. 26–32, Nov. 2017.

[6] C. Zhang and Y. Chen, "Wireless power transfer strategies for cooperative relay system to maximize information throughput," *IEEE Access*, vol. 5, pp. 2573–2582, 2017.

[7] M. T. Mamaghani and R. Abbas, "Security and reliability performance analysis for two-way wireless energy harvesting based untrusted relaying with cooperative jamming," *IET Communications*, vol. 13, no. 4, pp. 449–459, 2019.

[8] S. S. Kalamkar and A. Banerjee, "Secure communication via a wireless energy harvesting untrusted relay," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2199–2213, March 2017.

[9] I. Gradshteyn and I. Ryzhik, *Table of Integrals, series and products*. New York, NY: Elsevier, 2007.