

Análise de Sigilo de Sistemas sem Fio Assistidos por RIS sob Desvanecimento $\kappa-\mu$

Mariani Sfredo Da Luz, Henry Ramiro Carvajal Mora, Henrique Calefi e Evelio M. Garcia Fernandez

Resumo— Este trabalho analisa o desempenho de sigilo de um sistema de escuta assistido por superfícies inteligentes reconfiguráveis (RIS) em canais com desvanecimento $\kappa-\mu$, considerando a estatística da fase do canal. A RIS fornece alinhamento de fase perfeito no receptor legítimo, enquanto o enlace de escuta apresenta alinhamento imperfeito. Expressões aproximadas em forma fechada para a função densidade de probabilidade (PDF) e a função de distribuição cumulativa (CDF) da relação sinal-ruído (SNR) do enlace legítimo são obtidas via Teorema do Limite Central (CLT). A SNR do enlace de escuta é caracterizada por aproximação Gama. A probabilidade de outage de sigilo (SOP) e a probabilidade de outage de sigilo generalizada (GSOP) são obtidas e validadas por simulações de Monte Carlo.

Palavras-Chave— Superfícies Inteligentes Reconfiguráveis (RIS), Distribuição $\kappa-\mu$, Alinhamento Perfeito de Fase, Alinhamento Imperfeito de Fase, Probabilidade de Outage de Sigilo (SOP), Probabilidade de Outage de Sigilo Generalizada (GSOP).

Abstract— This work analyzes the secrecy performance of an RIS-assisted wiretap system over $\kappa-\mu$ fading channels, accounting for the channel-phase behavior. The RIS provides perfect phase alignment at the legitimate receiver, whereas the eavesdropping link experiences imperfect phase alignment. Closed-form approximations for the PDF and CDF of the legitimate-link SNR are derived using the central limit theorem (CLT), while the eavesdropping-link SNR is approximated by a Gamma distribution. Based on these results, the secrecy outage probability (SOP) and generalized secrecy outage probability (GSOP) are obtained. Monte Carlo simulations validate the analysis and show the impact of phase misalignment on secrecy performance.

Keywords— Reconfigurable Intelligent Surfaces, $\kappa-\mu$ fading, Imperfect Phase Alignment, Phase Alignment, Secrecy Outage Probability (SOP), Generalized Secrecy Outage Probability (GSOP).

I. INTRODUÇÃO

A segurança na camada física (PLS) tem emergido como uma abordagem eficiente para aprimorar o sigilo em sistemas assistidos por superfícies inteligentes reconfiguráveis (RIS) [1], [2], [3]. Ao controlar o ambiente de propagação por meio de elementos refletivos quase passivos, a RIS pode fortalecer o enlace legítimo e degradar o sinal recebido pelo espião, desde que os deslocamentos de fase sejam precisos: nesse caso, os componentes refletidos se combinam construtivamente no receptor, aumentando a SNR [4], [5], [6], [7]. Na prática, contudo, o alinhamento perfeito é difícil de manter, sobretudo em cenários de ondas milimétricas (mmWave), onde variações geométricas, mobilidade e erros de estimação de canal

degradam a compensação de fase e exigem reconfigurações frequentes da RIS [8], [9], reduzindo o ganho coerente e tornando as estatísticas da SNR dependentes do modelo de desvanecimento adotado [10].

O desvanecimento $\kappa-\mu$ tem sido adotado na modelagem de sistemas mmWave assistidos por RIS, pois representa o comportamento não uniforme da fase estatisticamente acoplado à envoltória, aspecto relevante para a compensação de fase [11], [12], [13], [14]. Além disso, medições demonstraram sua melhor aderência em relação a modelos clássicos de desvanecimento [15]. Como as condições de desvanecimento influenciam a qualidade relativa dos enlaces legítimo e de escuta, a probabilidade de outage de sigilo (SOP) tem sido amplamente empregada para avaliar a ocorrência de falhas de sigilo em sistemas assistidos por RIS [16], [17], [18].

Embora a SOP caracterize a ocorrência de falhas de sigilo, ela não quantifica diretamente a parcela de informação comprometida. Essa limitação torna-se mais evidente no pior cenário, em que a capacidade do canal legítimo é inferior à capacidade do canal do intruso, pois a SOP apenas indica a ocorrência do outage, sem medir o nível de comprometimento da mensagem. Nesse contexto, a probabilidade de outage de sigilo generalizada (GSOP) incorpora a equivocação fracionária e permite avaliar a probabilidade de que o vazamento de informação exceda um limiar predefinido [19], [20], [21], [22], [23]. Entretanto, a caracterização conjunta da SOP e da GSOP em sistemas RIS sob desvanecimento $\kappa-\mu$, considerando a fase não uniforme e o alinhamento assimétrico entre os enlaces legítimo e de escuta, permanece pouco explorada.

Neste trabalho, investigamos o desempenho de sigilo de um sistema assistido por RIS sob desvanecimento $\kappa-\mu$. A RIS é configurada para proporcionar combinação coerente no receptor legítimo, enquanto o enlace do espião permanece sujeito a alinhamento imperfeito de fase. A partir da caracterização estatística de ambos os enlaces, são obtidas a SOP e a GSOP.

As principais contribuições deste trabalho são resumidas a seguir.

- Para o enlace legítimo, derivamos expressões em forma fechada para a PDF e a CDF da SNR instantânea.
- Para o enlace do espião, obtemos uma caracterização semi-analítica da PDF da SNR instantânea sob alinhamento imperfeito de fase, utilizando uma aproximação Gamma baseada em casamento de momentos para considerar o comportamento não uniforme e analiticamente intratável da fase do canal $\kappa-\mu$.
- Com base na caracterização estatística de ambos os enlaces, derivamos a SOP e a GSOP.

O restante deste artigo está organizado da seguinte forma: a Seção II apresenta o modelo do sistema e a caracterização

Mariani Sfredo Da Luz, Evelio M. Garcia Fernandez e Henrique Calefi: Departamento de Engenharia Elétrica, Universidade Federal do Paraná, Curitiba-PR, Brasil, e-mails: {sfredo, evelio, henriquecalefi} @ufpr.br; Henry Ramiro Carvajal Mora: Colegio de Ciencias e Ingenierías "El Politécnico", Universidad San Francisco de Quito USFQ, Quito, Ecuador, e-mail: hcarvajal@usfq.edu.ec.

estatística dos enlaces legítimo e do espião; a Seção III desenvolve a análise da SOP e da GSOP; a Seção IV apresenta os resultados numéricos; e a Seção V conclui o artigo.

Notação: Os operadores esperança e variância são denotados por $\mathbb{E}[\cdot]$ e $\text{var}[\cdot]$, respectivamente. As distribuições Gaussianas real e complexa são denotadas por $\mathcal{N}(\mu, \sigma^2)$ e $\mathcal{CN}(0, \sigma^2)$, respectivamente, e $\text{erf}(\cdot)$ denota a função erro.

II. MODELO DO SISTEMA

Considere um sistema de comunicação sem fio assistido por uma RIS composta por N elementos refletores passivos, um transmissor T_x , um receptor legítimo, R_B , e um espião passivo R_E , todos equipados com antena única. Assume-se que os enlaces diretos T_x - R_B e T_x - R_E estão indisponíveis ou severamente atenuados, de modo que a comunicação ocorre apenas pelos caminhos assistidos pela RIS. As distâncias dos enlaces T_x -RIS, RIS- R_B e RIS- R_E são denotadas por d_T , d_B e d_E , respectivamente. Essa configuração permite isolar o impacto da fase não uniforme do desvanecimento κ - μ e do alinhamento assimétrico da RIS.

Sejam $g_i = |g_i|e^{j\varphi_i}$, $h_i = |h_i|e^{j\varphi_i}$ e $z_i = |z_i|e^{j\psi_i}$ os coeficientes dos enlaces T_x -RIS, RIS- R_B e RIS- R_E , respectivamente, associados ao i -ésimo elemento refletor, com $i = 1, \dots, N$. Assume-se que os coeficientes são mutuamente independentes e i.i.d. em cada enlace, embora as estatísticas de desvanecimento possam diferir entre enlaces. Além disso, essa hipótese desconsidera possíveis efeitos de correlação espacial na RIS. A envoltória segue a distribuição κ - μ , enquanto a fase é não uniforme e estatisticamente acoplada à envoltória. Sem perda de generalidade, considera-se $\mathbb{E}[|g_i|^2] = \mathbb{E}[|h_i|^2] = \mathbb{E}[|z_i|^2] = 1$, $\forall i$.

Cada elemento da RIS aplica um deslocamento de fase controlável denotado por ξ_i . Portanto, os coeficientes cascata associados aos enlaces legítimo e do espião são dados por $g_i h_i e^{j\xi_i}$ para o caminho T_x -RIS- R_B e por $g_i z_i e^{j\xi_i}$ para o caminho T_x -RIS- R_E . Assim, os modelos de sinal recebido e as estatísticas da SNR resultantes em R_B e R_E são apresentados separadamente nas subseções seguintes.

A. Caracterização Estatística

Nesta seção, derivamos as estatísticas dos canais legítimo e do espião. A RIS é otimizada apenas para o enlace legítimo; portanto, o desalinhamento no enlace do espião refere-se ao descasamento efetivo entre a fase aplicada pela RIS e a fase do canal RIS- R_E , e não a erros físicos de implementação ou estimação, que afetariam ambos os enlaces.

1) *Enlace Legítimo:* Para o enlace legítimo, assume-se que a RIS possui conhecimento perfeito das fases do canal cascata. Consequentemente, o i -ésimo elemento é configurado como $\xi_i = -\varphi_i - \varphi_i$. Assim, o sinal recebido em R_B pode ser expresso como

$$y_B = \left[\sum_{i=1}^N |h_i| |g_i| \right] \sqrt{P_b} \cdot x + \eta, \quad (1)$$

em que $P_b = P_t c_T d_T^{-\alpha} c_R d_B^{-\alpha}$. P_t é a potência transmitida, enquanto c_T e c_R denotam as constantes de propagação associadas aos enlaces T_x -RIS e RIS- R_B , respectivamente. Além disso, α é o expoente de perda de percurso e x denota o

símbolo complexo transmitido pertencente a uma constelação com potência média normalizada, e $\eta \sim \mathcal{CN}(0, \sigma_\eta^2)$ representa o ruído branco Gaussiano aditivo (AWGN) com média zero e variância σ_η^2 .

Portanto, a SNR em R_B é obtida como

$$\gamma_B = \frac{P_b}{\sigma_\eta^2} \underbrace{\left| \sum_{i=1}^N |h_i| |g_i| \right|}_B^2. \quad (2)$$

Como B é a soma de N variáveis aleatórias independentes e identicamente distribuídas, o teorema central do limite (CLT) permite aproximar B por uma variável aleatória Gaussiana para N suficientemente grande, isto é, $B \sim \mathcal{N}(\bar{B}, \sigma_B^2)$.

Assim, a média de B é dada por

$$\bar{B} = \mathbb{E} \left[\sum_{i=1}^N |g_i| |h_i| \right] = N \mathbb{E}[|h|] \mathbb{E}[|g|]. \quad (3)$$

Utilizando a função geradora de momentos da distribuição κ - μ [12, eq. (5)], obtém-se diretamente uma expressão em forma fechada para $\bar{B}$.

Sob a mesma hipótese de independência, a variância de B pode ser obtida a partir de $\text{var}[B] = \sum_{i=1}^N \text{var}[|h_i| |g_i|]$, resultando em

$$\begin{aligned} \sigma_B^2 &= N \left(\mathbb{E}[(|h|^2 |g|^2)] - (\mathbb{E}[|h|] \mathbb{E}[|g|])^2 \right) \\ &= N \left[1 - \left(\frac{\bar{B}}{N} \right)^2 \right]. \end{aligned} \quad (4)$$

A partir de (2), observa-se que $\gamma_B = a |B|^2$, em que $a = \frac{P_b}{\sigma_\eta^2}$, é uma função de B . Assim, seguindo o procedimento usual para determinar a distribuição de probabilidade de uma função de variável aleatória, a PDF de γ_B pode ser obtida como

$$\begin{aligned} f(\gamma_B) &= \frac{1}{2a\sqrt{2\pi}\sigma_B} \sqrt{\frac{a}{\gamma_B}} \left\{ \exp \left[-\frac{1}{2\sigma_B^2} \left(\sqrt{\frac{\gamma_B}{a}} + \bar{B} \right)^2 \right] \right. \\ &\quad \left. + \exp \left[-\frac{1}{2\sigma_B^2} \left(\sqrt{\frac{\gamma_B}{a}} - \bar{B} \right)^2 \right] \right\}. \end{aligned} \quad (5)$$

Integrando (5) com o auxílio do Wolfram Mathematica, obtém-se a expressão em forma fechada para a CDF de γ_B como

$$F_{\gamma_B}(\gamma_B) = \frac{1}{2} \left[\text{erf} \left(\frac{\sqrt{\frac{\gamma_B}{a}} - \bar{B}}{\sqrt{2}\sigma_B} \right) + \text{erf} \left(\frac{\sqrt{\frac{\gamma_B}{a}} + \bar{B}}{\sqrt{2}\sigma_B} \right) \right]. \quad (6)$$

B. Enlace do Espião

Em R_E , a mesma configuração $\xi_i = -(\varphi_i + \varphi_i)$, otimizada para R_B , é aplicada pela RIS. Assim, o i -ésimo componente recebido pelo espião conserva a fase relativa $\Delta_i = \varphi_i + \psi_i + \xi_i = \psi_i - \varphi_i$, que representa o desalinhamento efetivo do enlace de escuta.

Portanto, o sinal recebido no espião é expresso como

$$y_E = \left[\sum_{i=1}^N |g_i| |z_i| e^{j\Delta_i} \right] \sqrt{P_e} \cdot x + \eta, \quad (7)$$

onde $P_e = P_t c_T d_T^{-\alpha} c_R d_E^{-\alpha}$. A notação restante é definida semelhantemente no enlace legítimo. Portanto, a SNR resultante pode ser formulada como

$$\gamma_E = \frac{P_e}{\sigma_\eta^2} \left| \underbrace{\sum_{i=1}^N |g_i| |z_i| e^{j\Delta_i}}_W \right|^2, \quad (8)$$

onde W pode ser expresso como

$$W = \underbrace{\sum_{i=1}^N |g_i| |z_i| \cos \Delta_i}_{W_1} + j \underbrace{\sum_{i=1}^N |g_i| |z_i| \sin \Delta_i}_{W_2}. \quad (9)$$

Para N suficientemente grande, tanto W_1 quanto W_2 podem ser aproximados por variáveis aleatórias Gaussianas pelo CLT, uma vez que cada termo corresponde à soma de contribuições independentes. Assim,

$$W_1 \sim \mathcal{N}(\mathbb{E}[W_1], \sigma_1^2), \quad W_2 \sim \mathcal{N}(\mathbb{E}[W_2], \sigma_2^2). \quad (10)$$

Os momentos de primeira ordem de W_1 e W_2 são obtidos, respectivamente, como

$$\begin{aligned} \mathbb{E}[W_1] &= N \mathbb{E}[|g|] \mathbb{E}[|z|] \mathbb{E}[\cos(\Delta)], \\ \mathbb{E}[W_2] &= N \mathbb{E}[|g|] \mathbb{E}[|z|] \mathbb{E}[\sin(\Delta)]. \end{aligned} \quad (11)$$

Os momentos de primeira ordem da envoltória, $\mathbb{E}[|g|]$ e $\mathbb{E}[|z|]$, são obtidos a partir de [12, eq. (5)], utilizando os respectivos parâmetros κ - μ dos enlaces T_x-RIS e RIS-R_E. As esperanças dependentes da fase são calculadas como

$$\begin{aligned} \mathbb{E}[\cos(\Delta)] &= \int_{-\pi}^{\pi} \cos(\Delta) f_\Delta(\Delta) d\Delta, \\ \mathbb{E}[\sin(\Delta)] &= \int_{-\pi}^{\pi} \sin(\Delta) f_\Delta(\Delta) d\Delta. \end{aligned} \quad (12)$$

A PDF $f_\Delta(\Delta)$ não é assumida como a fase de um único canal κ - μ ; ela é induzida pela diferença circular entre as fases dos enlaces RIS-R_E e RIS-R_B. Como essa distribuição não admite forma fechada simples para μ arbitrário, os momentos trigonométricos de primeira e segunda ordem usados em (12) e nas variâncias de W_1 e W_2 são avaliados numericamente a partir das fases individuais.

Utilizando a normalização $\mathbb{E}[|g|^2] = \mathbb{E}[|z|^2] = 1$, as variâncias de W_1 e W_2 podem ser escritas como

$$\sigma_1^2 = N \mathbb{E}[\cos^2(\Delta)] - \frac{\mathbb{E}[W_1]^2}{N}, \quad (13)$$

$$\sigma_2^2 = N \mathbb{E}[\sin^2(\Delta)] - \frac{\mathbb{E}[W_2]^2}{N}. \quad (14)$$

A partir de (9), tem-se $|W|^2 = W_1^2 + W_2^2$. Como W_1 e W_2 são variáveis Gaussianas, conforme (10), seus quadrados seguem distribuições qui-quadrado não centrais escaladas, cada uma com $\nu = 1$ grau de liberdade [24]. Os respectivos parâmetros de não centralidade, λ_1 e λ_2 , são dados por

$$\lambda_1 = \frac{(\mathbb{E}[W_1])^2}{\text{var}[W_1]}, \quad \lambda_2 = \frac{(\mathbb{E}[W_2])^2}{\text{var}[W_2]}. \quad (15)$$

Portanto, o momento de primeira ordem de $|W|^2$ é dado por

$$\mathbb{E}[|W|^2] = \underbrace{\text{var}[W_1]}_{\mathbb{E}[W_1^2]} (1 + \lambda_1) + \underbrace{\text{var}[W_2]}_{\mathbb{E}[W_2^2]} (1 + \lambda_2), \quad (16)$$

e a variância correspondente por

$$\text{var}[|W|^2] = \text{var}[W_1^2] + \text{var}[W_2^2] + 2 \text{Cov}[W_1^2, W_2^2]. \quad (17)$$

em que

$$\begin{aligned} \text{var}[W_1^2] &= 2 (\text{var}[W_1])^2 (1 + 2\lambda_1), \\ \text{var}[W_2^2] &= 2 (\text{var}[W_2])^2 (1 + 2\lambda_2). \end{aligned} \quad (18)$$

O termo de covariância em (17) surge porque W_1 e W_2 compartilham as mesmas contribuições da envoltória cascata, $|g_i| |z_i|$, conforme observado em (9). Entretanto, avaliações numéricas mostraram que o coeficiente de correlação amostral entre W_1^2 e W_2^2 permanece baixo para uma ampla faixa de valores de κ e μ .

Consequentemente, (17) pode ser reescrita como

$$\text{var}[|W|^2] = \text{var}[W_1^2] + \text{var}[W_2^2]. \quad (19)$$

A variável aleatória $|W|^2 = W_1^2 + W_2^2$, presente em (8), não segue uma distribuição padrão em forma fechada. Entretanto, ela pode ser aproximada por meio de casamento de momentos com uma distribuição Gamma, isto é,

$$|W|^2 \sim \text{Gamma}(\delta, \beta), \quad \delta = \frac{(\mathbb{E}[|W|^2])^2}{\text{var}[|W|^2]}, \quad \beta = \frac{\text{var}[|W|^2]}{\mathbb{E}[|W|^2]}. \quad (20)$$

Por fim, a SNR instantânea em R_E, dada em (8), pode ser expressa como $\gamma_E = \psi |W|^2$, $\psi = \frac{P_e}{\sigma_\eta^2}$. Assim, pela propriedade de escala da distribuição Gamma, conclui-se que $\gamma_E \sim \text{Gamma}(\delta, \psi\beta)$, com PDF dada por

$$f_{\gamma_E}(\gamma_E) = \frac{1}{(\psi\beta)^\delta \Gamma(\delta)} \gamma_E^{\delta-1} \exp\left(-\frac{\gamma_E}{\psi\beta}\right), \quad \gamma_E > 0, \quad (21)$$

onde $\Gamma(\cdot)$ denota a função Gamma [25, eq. (6.1.1)]. A aproximação constitui uma caracterização semi-analítica, pois a distribuição exata de $|W|^2$ não é obtida em forma fechada; sua validade é verificada numericamente para os cenários considerados.

III. ANÁLISE DE SIGILO

A. Probabilidade de Outage de Sigilo

A probabilidade de outage de sigilo (SOP) é definida como a probabilidade de que a capacidade instantânea de sigilo seja menor que uma taxa-alvo de sigilo R_s , isto é, [26, eq. (9)]

$$\text{SOP} = \Pr(\mathcal{C}_s < R_s), \quad (22)$$

onde a capacidade de sigilo não negativa é dada por

$$\mathcal{C}_s = \begin{cases} \mathcal{C}_B - \mathcal{C}_E, & \gamma_B > \gamma_E, \\ 0, & \gamma_B \leq \gamma_E, \end{cases} \quad (23)$$

com $\mathcal{C}_B = \log_2(1 + \gamma_B)$ e $\mathcal{C}_E = \log_2(1 + \gamma_E)$ denotando as capacidades dos canais de R_B e de R_E, respectivamente. Portanto, substituindo (6) e (21) em (22) e (23), obtém-se

$$\text{SOP} = \int_0^\infty F_{\gamma_B}(2^{R_s}(1 + \gamma_E) - 1) f_{\gamma_E}(\gamma_E) d\gamma_E. \quad (24)$$

B. Probabilidade de Outage de Sigilo Generalizada

A probabilidade de outage de sigilo generalizada (GSOP) quantifica a probabilidade de que a equivocação fracionária $\Lambda = \min\{C_s/R_s, 1\}$ seja inferior ao limiar θ , ou, equivalentemente, de que a razão de vazamento $1 - \Lambda$ exceda $1 - \theta$ [27],

$$\text{GSOP} = \Pr(\Lambda < \theta), \quad (25)$$

onde $0 < \theta \leq 1$.

Condicionando em relação a γ_E e utilizando a CDF de γ_B em (6) e a PDF de γ_E em (21), a GSOP pode ser expressa como

$$\text{GSOP} = \int_0^\infty F_{\gamma_B}(2^{\theta R_s}(1 + \gamma_E) - 1) f_{\gamma_E}(\gamma_E) d\gamma_E. \quad (26)$$

IV. RESULTADOS NUMÉRICOS

Esta seção apresenta resultados numéricos para validar a probabilidade de outage de sigilo de um sistema de escuta sob as duas condições de alinhamento de fase consideradas. As expressões analíticas são comparadas com simulações de Monte Carlo no MATLAB, usando 1×10^6 realizações independentes do canal.

Para todos os enlaces, consideram-se $\alpha = 2,5$, $c_T = c_R = -30$ dB, $\sigma_\eta^2 = -90$ dBm, $P_t = 15$ dBm e $R_s = 1$ bps/Hz. Salvo indicação em contrário, adota-se $d_T = 20$ m, $d_B = 30$ m e $d_E = 40$ m, representando enlaces mmWave de curto alcance com parâmetros usuais de perda de percurso [28], [29], [30].

A concordância entre análise e simulação nas faixas de N consideradas, inclusive para os menores valores avaliados, confirma a precisão prática das aproximações baseadas no CLT e no casamento de momentos nos cenários simulados.

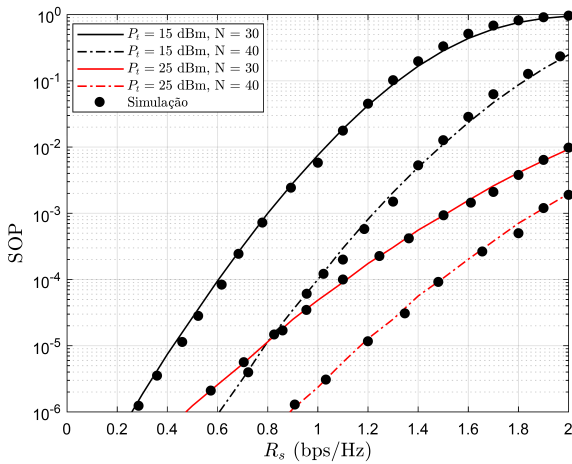


Fig. 1: SOP em função de R_s parametrizada por diferentes valores de P_t e N .

A Fig. 1 apresenta a SOP em função do limiar de capacidade de sigilo para diferentes valores de P_t e N . Observa-se que, para todas as configurações consideradas, a SOP aumenta à medida que R_s cresce, uma vez que limiares de sigilo mais elevados exigem uma maior vantagem instantânea do enlace legítimo em relação ao enlace do espião. Assim, o sistema torna-se mais sensível às flutuações da envoltória equivalente e

aos efeitos do desalinhamento de fase, pois pequenas reduções na vantagem instantânea do canal legítimo podem resultar em falha de sigilo.

Além disso, a SOP é reduzida com o aumento de P_t ou de N ao longo de toda a faixa de R_s , e não apenas em uma região específica. Esse comportamento indica que o ganho de potência transmitida e o ganho de combinação coerente proporcionado pela RIS contribuem para ampliar a diferença entre os enlaces legítimo e de interceptação.

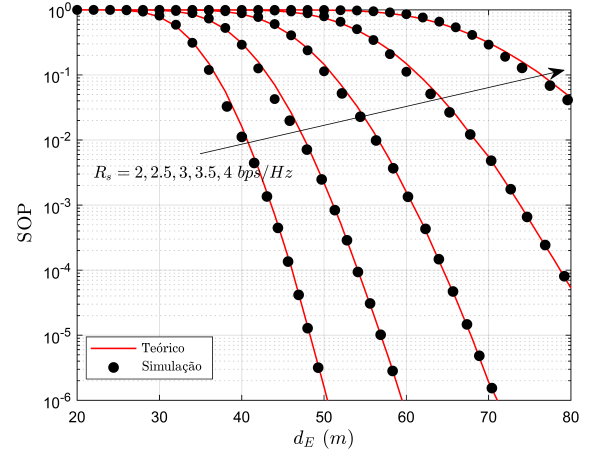


Fig. 2: SOP em função de d_E parametrizada por diferentes valores de R_s .

A Fig. 2 apresenta a SOP em função de d_E , parametrizada por diferentes valores de R_s . À medida que R_s aumenta, o requisito de sigilo torna-se mais rigoroso, e uma mesma distância de R_E deixa de garantir baixa SOP. Assim, maiores valores de R_s exigem maior separação entre a RIS e o espião para que a atenuação do enlace desalinhado compense o aumento do limiar de sigilo.

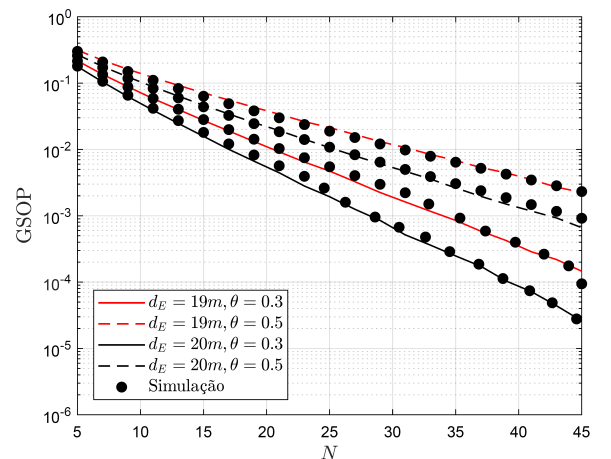


Fig. 3: GSOP em função de N parametrizado por diferentes valores de d_E e θ . Os parâmetros restantes são: $d_T = 2$ m, $d_B = 20$ m.

A Fig. 3 apresenta a GSOP em função de N para diferentes valores de d_E e θ . A aproximação de R_E à RIS aumenta a GSOP, enquanto maiores valores de d_E favorecem o sigilo.

Além disso, $\theta = 0,5$ impõe requisito mais rigoroso que $\theta = 0,3$, pois caracteriza outage quando o vazamento excede 50% da mensagem, em vez de 70%. Esse efeito é parcialmente compensado pelo ganho de combinação associado ao aumento de N .

V. CONCLUSÕES

Este trabalho analisou a SOP e a GSOP em sistemas assistidos por RIS sob desvanecimento $\kappa-\mu$, considerando explicitamente a fase não uniforme do canal. Os resultados mostraram que a modelagem proposta permite capturar o efeito do desalinhamento residual de fase no enlace de escuta, enquanto o alinhamento perfeito no enlace legítimo produz ganho coerente com o aumento de N . Assim, a RIS mostrou-se efetiva para melhorar o sigilo quando sua configuração favorece o enlace legítimo e limita a combinação coerente no espião. Além disso, a boa concordância entre análise e simulação indica que a modelagem estatística é adequada para representar o impacto da fase na avaliação da PLS em sistemas mmWave assistidos por RIS.

Como trabalhos futuros, sugere-se incluir erros práticos de configuração da RIS, correlação espacial entre elementos, enlaces diretos residuais e comparações com modelos alternativos de desvanecimento. Também se pretende estender a análise às métricas AFE (Equivocação Fracionária Média) e AILR (Taxa Média de Vazamento de Informação).

AGRADECIMENTOS

Este trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) - Código de Financiamento 001, e da Universidad San Francisco de Quito USFQ, Equador, Grant PoliGrants 41991.

REFERÊNCIAS

- [1] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Communications Letters*, vol. 8, no. 5, pp. 1410–1414, 2019.
- [2] X. Yu, D. Xu, and R. Schober, "Enabling Secure Wireless Communications via Intelligent Reflecting Surfaces," in *2019 IEEE Global Communications Conference (GLOBECOM)*, 2019, pp. 1–6.
- [3] J. Chen, Y.-C. Liang, Y. Pei, and H. Guo, "Intelligent Reflecting Surface: A Programmable Wireless Environment for Physical Layer Security," *IEEE Access*, vol. 7, pp. 82 599–82 612, 2019.
- [4] Q. Wu and R. Zhang, "Towards Smart and Reconfigurable Environment: Intelligent Reflecting Surface Aided Wireless Network," *IEEE Communications Magazine*, vol. 58, no. 1, pp. 106–112, 2020.
- [5] E. Basar, M. Di Renzo, J. De Rosny, M. Debbah, M.-S. Alouini, and R. Zhang, "Wireless Communications Through Reconfigurable Intelligent Surfaces," *IEEE Access*, vol. 7, pp. 116 753–116 773, 2019.
- [6] I. Isabel Salazar Argoti, E. M. G. Fernandez, H. Ramiro Carvajal Mora, and A. Camponogara, "On the Performance of RIS-Assisted Wireless Communications Over Generalized Multi-Cluster Fluctuating Two-Ray Fading Channels," *IEEE Access*, vol. 13, pp. 217 929–217 938, 2025.
- [7] E. G. Gomes, H. R. C. Mora, and E. E. B. Olivo, "Performance of STAR-RIS-Aided RSMA Networks: Impact of Correlated Fading Channels and SIC Imperfections," *IEEE Access*, vol. 13, pp. 39 826–39 839, 2025.
- [8] T. S. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G. N. Wong, J. K. Schulz, M. Samimi, and F. Gutierrez, "Millimeter Wave Mobile Communications for 5G Cellular: It Will Work!" *IEEE Access*, vol. 1, pp. 335–349, 2013.
- [9] T. S. Rappaport, G. R. MacCartney, M. K. Samimi, and S. Sun, "Wideband Millimeter-Wave Propagation Measurements and Channel Models for Future Wireless Communication System Design," *IEEE Transactions on Communications*, vol. 63, no. 9, pp. 3029–3056, 2015.
- [10] D. Li, "Ergodic Capacity of Intelligent Reflecting Surface-Assisted Communication Systems With Phase Errors," *IEEE Communications Letters*, vol. 24, no. 8, pp. 1646–1650, 2020.
- [11] U. S. Dias and M. D. Yacoub, "The $\kappa-\mu$ Phase-Envelope Joint Distribution," *IEEE Transactions on Communications*, vol. 58, no. 1, pp. 40–45, 2010.
- [12] M. D. Yacoub, "The $\kappa-\mu$ distribution and the $\eta-\mu$ distribution," *IEEE Antennas and Propagation Magazine*, vol. 49, no. 1, pp. 68–81, 2007.
- [13] C. A. da Silva, M. D. Yacoub, and G. Fraidenraich, " $\alpha-\mu$, $\kappa-\mu$, and $\eta-\mu$ Mixed Products: Exact and Approximate Results With Applications to RIS-Assisted Systems," *IEEE Transactions on Vehicular Technology*, 2024.
- [14] H. R. C. Mora, N. V. O. Garzón, F. D. A. García, J. D. V. Sánchez, and O. L. A. López, "Secure Transmission for Uplink SCMA Systems Over $\kappa-\mu$ Fading Channels," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 1, pp. 754–770, 2024.
- [15] S. K. Yoo, N. Simmons, S. L. Cotton, P. C. Sofotasios, M. Matthaiou, M. Valkama, and G. K. Karagiannidis, "The $\kappa-\mu$ /Inverse Gamma and $\eta-\mu$ /Inverse Gamma Composite Fading Models: Fundamental Statistics and Empirical Validation," *IEEE Transactions on Communications*, vol. 69, no. 8, pp. 5514–5530, 2021.
- [16] Z. Xie, Y. Liu, W. Yi, X. Wu, and A. Nallanathan, "Physical Layer Security for STAR-RIS-NOMA: A Stochastic Geometry Approach," *IEEE Transactions on Wireless Communications*, vol. 23, no. 6, pp. 6030–6044, 2024.
- [17] A. Salem, K.-K. Wong, and C.-B. Chae, "Impact of Phase-Shift Error on the Secrecy Performance of Uplink RIS Communication Systems," *IEEE Transactions on Wireless Communications*, vol. 23, no. 7, pp. 7376–7391, 2024.
- [18] N. Bhargava, S. L. Cotton, and D. E. Simmons, "Secrecy Capacity Analysis Over $\kappa-\mu$ Fading Channels: Theory and Applications," *IEEE Transactions on Communications*, vol. 64, no. 7, pp. 3011–3024, 2016.
- [19] S. Allipuram, P. Mohapatra, and S. Chakrabarti, "Secrecy performance of an artificial noise assisted transmission scheme with active eavesdropper," *IEEE Communications Letters*, vol. 24, no. 5, pp. 971–975, 2020.
- [20] G. Sharma and A. Singh, "Secrecy performance of diffusion based molecular timing channels," *IET Communications*, vol. 15, no. 2, pp. 289–304, 2021.
- [21] B. He, X. Zhou, and A. L. Swindlehurst, "On Secrecy Metrics for Physical Layer Security Over Quasi-Static Fading Channels," *IEEE Transactions on Wireless Communications*, vol. 15, no. 10, pp. 6913–6924, 2016.
- [22] D. P. M. Osorio, H. Alves, and E. E. B. Olivo, "On the Secrecy Performance and Power Allocation in Relaying Networks With Untrusted Relay in the Partial Secrecy Regime," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2268–2281, 2020.
- [23] H. Ramiro Carvajal Mora, N. Verónica Orozco Garzón, F. Darío Almeida García, J. David Vega Sánchez, F. Grijalva, and E. Eduardo Benitez Olivo, "Partial Secrecy Analysis in Wireless Systems: Diversity-Enhanced PLS Over Generalized Fading Channels," *IEEE Access*, vol. 13, pp. 164 723–164 741, 2025.
- [24] A. Ferrari, "A note on sum and difference of correlated chi-squared variables," *arXiv preprint arXiv:1906.09982*, 2019.
- [25] M. Abramowitz, *Handbook of Mathematical Functions, With Formulas, Graphs, and Mathematical Tables*,. USA: Dover Publications, Inc., 1974.
- [26] H. Lei, C. Gao, Y. Guo, and G. Pan, "On Physical Layer Security Over Generalized Gamma Fading Channels," *IEEE Communications Letters*, vol. 19, no. 7, pp. 1257–1260, 2015.
- [27] B. He, X. Zhou, and A. L. Swindlehurst, "On Secrecy Metrics for Physical Layer Security over Quasi-Static Fading Channels," *IEEE Transactions on Wireless Communications*, vol. 16, no. 1, pp. 475–488, 2017.
- [28] A. Al-Rimawi and A. Al-Dweik, "On the Performance of RIS-Assisted Communications with Direct Link over $\kappa-\mu$ Shadowed Fading," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 2314–2328, 2022.
- [29] T. S. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. Upper Saddle River, NJ: Prentice Hall PTR, 2002.
- [30] 3rd Generation Partnership Project (3GPP), "Study on Channel Model for Frequencies from 0.5 to 100 GHz," 3rd Generation Partnership Project (3GPP), Technical Report TR 38.901, Nov. 2020, Version 16.1.0, Release 16.