Journal of Computing and Electronic Information Management
ISSN: 2413-1660 | Vol. 21, No. 2, 2026

Secrecy Analysis for a Fixed UAV-Assisted DF Relay Network with Hardware Impairments over Nakagami-m Channels

Shuiwang Niu *

Henan Polytechnic University, College of Computer Science and Technology, Jiaozuo 454000, China
*** Corresponding author:** 780929512@qq.com

Abstract: A fixed UAV-assisted decode-and-forward relay network is examined from the perspective of physical-layer security under residual transceiver distortion. The source communicates with the destination only through the UAV relay, and the eavesdropper overhears the relay transmission. Independent Nakagami-m fading is used for the three wireless links so that different UAV propagation conditions can be represented within one model. Based on the SNDRs of the two legitimate hops and the wiretap hop, expressions for SOP and SPSC are derived, and simplified finite-sum integral forms are given for integer fading parameters. The numerical study confirms the analytical results and shows how fading severity, secrecy-rate demand, eavesdropper SNR, and impairment level affect secure transmission.

Keywords: Physical layer security; UAV relay; Hardware impairments; Nakagami-m fading.

1. Introduction

Wireless signals are inherently exposed to nearby receivers, which makes confidentiality difficult to guarantee only through transmission design. Higher-layer encryption remains necessary, but PLS can add protection by exploiting differences between the legitimate and eavesdropping channels [1-7].

PLS evaluates whether the intended channel can provide a secrecy advantage over the wiretap channel. Since the classical wiretap-channel results [1,2], secrecy metrics have been studied under many fading models, including Rayleigh, Rician, and Nakagami-m fading [8,22,23]. This paper uses SOP to measure failure to satisfy a target secrecy rate and SPSC to measure the chance of obtaining positive secrecy capacity.

Relaying is widely used to improve coverage and reliability when the direct link is blocked or severely attenuated. UAV relays are attractive because they can be quickly deployed and often provide favorable air-to-ground propagation. Nevertheless, the relay-forwarding phase is also exposed to nearby eavesdroppers, and the high position of a UAV may further enlarge the region in which the signal can be overheard. In addition, UAV radio platforms are constrained by payload, power budget, calibration accuracy, and hardware cost, so residual transmitter and receiver impairments cannot be neglected. Secure cooperative transmission has therefore been studied under AF/DF protocols, relay selection, cooperative beamforming, artificial noise, and diversity techniques [9-13,15,21,24].

The Nakagami-m model is adopted here because it provides a flexible description of different fading severities while remaining mathematically tractable. This is useful for UAV-assisted links: some paths may be dominated by line-of-sight components, while others may still suffer from obstruction, scattering, and user-location-dependent fading. By changing the fading parameter, the same analytical framework can represent heterogeneous link qualities. Related studies have also shown that antenna configuration, fading severity, secrecy-rate requirement, and eavesdropper capability can strongly influence secrecy metrics [16-18], while practical issues such as imperfect CSI, hardware impairments, UAV links, and reflecting surfaces introduce additional performance limitations [14,19,20].

Although many secrecy models have been reported, a concise analysis for a fixed DF UAV relay system with both generalized fading and residual hardware distortion remains useful. Hardware distortion grows with signal power and can create an SNDR ceiling, so increasing transmit SNR alone may not continuously improve secrecy. Studying this baseline model helps clarify the interaction among legitimate-link quality, eavesdropping strength, target secrecy demand, and hardware impairment level, and it can support later extensions such as relay selection, artificial noise, trajectory optimization, imperfect CSI, and multi-antenna processing.

The present study focuses on a baseline fixed DF UAV relay system in which generalized fading and hardware distortion act together. Since distortion may cap the SNDR at high SNR, the model highlights when better transmit power, better channel quality, or better hardware is most influential.

This paper makes the following contributions:

1). A four-node UAV relay wiretap model is built for the case without a direct source-destination link, and the SNDRs are formulated under half-duplex DF relaying with residual hardware distortion.

2). SOP and SPSC are derived from the equivalent end-to-end SNDR, with finite-sum integral forms further obtained for integer Nakagami-m parameters.

3). Simulations verify the analysis and compare the effects of fading, secrecy-rate threshold, eavesdropper SNR, and impairment coefficient.

Sections 2-5 present the model, secrecy analysis, numerical results, and conclusions, respectively.

2. System Model

The considered network consists of a source, a fixed hovering UAV relay, a legitimate destination, and an eavesdropper. Because the source-destination path is

unavailable, the UAV forwards the confidential signal. The eavesdropper is assumed to monitor this forwarding phase, so the system follows a relay-wiretap structure [1,11,12,16].

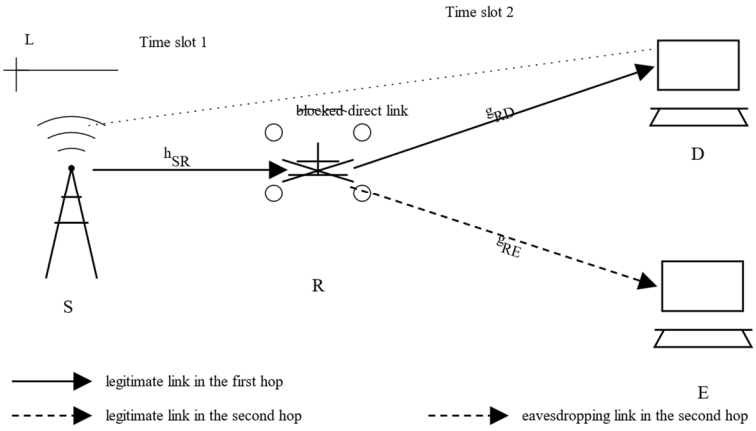

Figure 1. System model

Let the three link distances be defined for the source-relay, relay-destination, and relay-eavesdropper paths. The large-scale path loss is written as

$$\bar{g}_{ij} = C_0 d_{ij}^{-\eta_{ij}}, ij \in \{SR, RD, RE\}, \quad (1)$$

where C_0 is the reference path-loss constant and η_{ij} is the path-loss exponent.

The small-scale gains of all links are independent Nakagami-m random variables. This model is adopted because UAV links may range from strong line-of-sight paths to more variable obstructed paths. The corresponding channel-power gain is Gamma distributed as

$$|h_{ij}|^2 \sim \text{Gamma}\left(m_{ij}, \frac{\Omega_{ij}}{m_{ij}}\right), \quad (2)$$

where m_{ij} is the Nakagami-m fading parameter and $\Omega_{ij} = \mathbb{E}[|h_{ij}|^2]$ is the average channel power gain.

The source and relay transmit powers and the receiver noise power define the normalized transmit SNRs as

$$\rho_S = \frac{P_S}{N_0}, \rho_R = \frac{P_R}{N_0}. \quad (3)$$

Transmission uses two half-duplex DF slots.

During the first slot, the source sends the confidential symbol to the UAV relay, and the received signal is

$$y_R = \sqrt{P_S \bar{g}_{SR}} h_{SR}(x_s + \eta_{SR}) + n_R, \quad (4)$$

The first-hop noise and residual distortion lead to the following SNDR:

$$\gamma_{SR} = \frac{\rho_S \bar{g}_{SR} |h_{SR}|^2}{1 + \kappa_{SR}^2 \rho_S \bar{g}_{SR} |h_{SR}|^2}. \quad (5)$$

During the second slot, the relay forwards the decoded signal to the destination, while the same signal may be overheard by the eavesdropper. The received signals are

$$y_D = \sqrt{P_R \bar{g}_{RD}} h_{RD}(x_r + \eta_{RD}) + n_D, \quad (6)$$

$$y_E = \sqrt{P_R \bar{g}_{RE}} h_{RE}(x_r + \eta_{RE}) + n_E, \quad (7)$$

Thus, the second-hop and wiretap SNDRs are

$$\gamma_{RD} = \frac{\rho_R \bar{g}_{RD} |h_{RD}|^2}{1 + \kappa_{RD}^2 \rho_R \bar{g}_{RD} |h_{RD}|^2}, \quad (8)$$

$$\gamma_{RE} = \frac{\rho_R \bar{g}_{RE} |h_{RE}|^2}{1 + \kappa_{RE}^2 \rho_R \bar{g}_{RE} |h_{RE}|^2}. \quad (9)$$

Secrecy is determined by the useful two-hop relay path relative to the relay-eavesdropper path. The UAV improves connectivity, but its forwarding operation also creates the main leakage opportunity.

For DF relaying, the legitimate end-to-end SNDR is limited by the weaker hop:

$$\gamma_D = \min(\gamma_{SR}, \gamma_{RD}), \quad (10)$$

and the eavesdropper SNDR is

$$\gamma_E = \gamma_{RE}. \quad (11)$$

Equation (10) shows the bottleneck effect of DF relaying. Hardware distortion further limits the attainable SNDR, so secrecy may saturate even when transmit power is increased.

Before including distortion, define the ideal instantaneous SNR of each link as

$$\tilde{\gamma}_{ij} = \rho_i \bar{g}_{ij} |h_{ij}|^2, \quad (12)$$

and its corresponding average value is

$$\bar{\gamma}_{ij} = \rho_i \bar{g}_{ij} \Omega_{ij}, \quad (13)$$

The corresponding PDF and CDF are

$$f_{\tilde{\gamma}_{ij}}(x) = \frac{\alpha_{ij}^{m_{ij}}}{\Gamma(m_{ij})} x^{m_{ij}-1} e^{-\alpha_{ij} x}, x \geq 0, \quad (14)$$

$$F_{\tilde{\gamma}_{ij}}(x) = 1 - \frac{\Gamma(m_{ij}, \alpha_{ij} x)}{\Gamma(m_{ij})}, \quad (15)$$

where

$$\alpha_{ij} = \frac{m_{ij}}{\bar{\gamma}_{ij}}. \quad (16)$$

The distorted SNDR is related to the ideal SNR by

$$\gamma_{ij} = \frac{\tilde{\gamma}_{ij}}{1 + \kappa_{ij}^2 \tilde{\gamma}_{ij}}, \quad 0 \leq \gamma_{ij} < \frac{1}{\kappa_{ij}^2}. \quad (17)$$

The support of this SNDR is

$$\mathcal{S}_{ij} = \begin{cases} 0, \infty), & \kappa_{ij} = 0, \\ 0, 1/\kappa_{ij}^2), & \kappa_{ij} > 0. \end{cases} \quad (18)$$

Within this support, the distribution is obtained by variable transformation:

$$F_{\gamma_{ij}}(x) = F_{\tilde{\gamma}_{ij}}\left(\frac{x}{1 - \kappa_{ij}^2 x}\right), \quad (19)$$

$$\bar{F}_{\gamma_{ij}}(x) = \bar{F}_{\gamma_{ij}}\left(\frac{x}{1 - \kappa_{ij}^2 x}\right), \quad (20)$$

$$f_{\gamma_{ij}}(x) = \frac{1}{(1 - \kappa_{ij}^2 x)^2} \times f_{\tilde{\gamma}_{ij}}\left(\frac{x}{1 - \kappa_{ij}^2 x}\right). \quad (21)$$

Outside the support, the CDF equals one and the complementary CDF/PDF vanish. When the impairment coefficient is zero, the ideal-hardware SNR is recovered.

The model uses four simplifying assumptions: no direct source-destination link, half-duplex DF relaying, eavesdropping only in the forwarding slot, and independent fading. These assumptions keep the secrecy analysis tractable.

The same framework can be extended to relay selection,

multi-antenna processing, imperfect CSI, asymmetric impairments, or mobile UAV deployment.

Lemma 1. The CDF of the end-to-end legitimate SNDR $\gamma_D = \min(\gamma_{SR}, \gamma_{RD})$ is

$$F_{\gamma_D}(x) = 1 - \bar{F}_{\gamma_{SR}}(x)\bar{F}_{\gamma_{RD}}(x), \tag{22}$$

where $\bar{F}_{\gamma_{ij}}(x) = 1 - F_{\gamma_{ij}}(x)$.

Proof. the definition of the minimum random variable,

$$\begin{aligned} F_{\gamma_D}(x) &= Pr(\gamma_D \le x) \\ &= 1 - Pr(\gamma_{SR} > x, \gamma_{RD} > x). \end{aligned} \tag{23}$$

Since γ_{SR} and γ_{RD} are independent,

$$\begin{aligned} F_{\gamma_D}(x) &= 1 - Pr(\gamma_{SR} > x)Pr(\gamma_{RD} > x) \\ &= 1 - \bar{F}_{\gamma_{SR}}(x)\bar{F}_{\gamma_{RD}}(x). \end{aligned} \tag{24}$$

This completes the proof.

3. Secrecy Performance Analysis

For the impaired half-duplex DF relay, the legitimate and wiretap capacities are

$$C_D = \frac{1}{2}\log_2(1 + \gamma_D), \tag{25}$$

$$C_E = \frac{1}{2}\log_2(1 + \gamma_E). \tag{26}$$

Thus, the instantaneous secrecy capacity is

$$\begin{aligned} C_s &= [C_D - C_E]^+ \\ &= \left[\frac{1}{2}\log_2\left(\frac{1+\gamma_D}{1+\gamma_E}\right)\right]^+, \end{aligned} \tag{27}$$

where $[x]^+ = \max(x, 0)$.

Thus, secrecy depends on the capacity gap between the bottlenecked legitimate path and the wiretap path, with both fading and hardware distortion shaping the gap.

3.1. Secrecy Outage Probability

For a target secrecy rate, SOP is

$$P_{\text{SOP}} = \Pr(C_s < R_s). \tag{28}$$

Let

$$\tau = 2^{2R_s}. \tag{29}$$

Then,

$$\begin{aligned} P_{\text{SOP}} &= Pr\left(\frac{1+\gamma_D}{1+\gamma_E} < \tau\right) \\ &= Pr(\gamma_D < \tau(1 + \gamma_E) - 1). \end{aligned} \tag{30}$$

The wiretap-SNDR support is denoted by

Theorem 1. For positive Nakagami-m parameters and feasible impairment levels, SOP is

$$P_{\text{SOP}} = \int_{S_E} F_{\gamma_D}\left(\tau\left(1+y\right)-1\right) f_{\gamma_E}(y)\, dy. \tag{31}$$

Proof. From the definition of SOP,

$$P_{\text{SOP}} = \Pr(\gamma_D < \tau(1 + \gamma_E) - 1). \tag{32}$$

Conditioning on $\gamma_E = y$ yields

$$P_{\text{SOP}} = \int_{S_E} \Pr\left(\gamma_D < \tau\left(1+y\right)-1 \mid \gamma_E = y\right) f_{\gamma_E}(y)\, dy. \tag{33}$$

Using the CDF of γ_D, we obtain

$$P_{\text{SOP}} = \int_{S_E} F_{\gamma_D}\left(\tau\left(1+y\right)-1\right) f_{\gamma_E}(y)\, dy. \tag{34}$$

This completes the proof.

By substituting the distribution of the end-to-end legitimate SNDR into the above result, the SOP can also be rewritten as

$$P_{\text{SOP}} = 1 - \int_{S_E} \bar{F}_{\gamma_{SR}}(X)\bar{F}_{\gamma_{RD}}(X) f_{\gamma_E}(y)\, dy, \tag{35}$$

where

$$X = \tau(1 + y) - 1. \tag{36}$$

This form separates the contributions of the two legitimate hops, the eavesdropping hop, and the impairment coefficients.

When m_{SR}, m_{RD}, and m_{RE} are positive integers, the complementary CDF of the ideal Nakagami -m SNR can be expressed as

$$\bar{F}_{\tilde{\gamma}_{ij}}(x) = e^{-\alpha_{ij}x} \sum_{n=0}^{m_{ij}-1} \frac{(\alpha_{ij}x)^n}{n!}. \tag{37}$$

After applying the SNDR mapping in Section 2, the corresponding finite-series terms are inserted into the SOP integral.

$$\begin{aligned} f_{\gamma_E}(y) &= \frac{1}{(1-\kappa_{RE}^2 y)^2} \\ &\times f_{\tilde{\gamma}_{RE}}\left(\frac{y}{1-\kappa_{RE}^2 y}\right), \end{aligned} \tag{38}$$

This substitution gives the finite-sum integral form below.

Theorem 2. For positive integer-valued m_{SR}, m_{RD}, and m_{RE}, the SOP admits the following equivalent finite-sum integral representation:

$$\begin{aligned} P_{\text{SOP}} &= 1 - \frac{\alpha_{RE}^{m_{RE}}}{\Gamma(m_{RE})} \sum_{k=0}^{m_{SR}-1} \sum_{l=0}^{m_{RD}-1} \frac{\alpha_{SR}^k \alpha_{RD}^l}{k!l!} \\ &\times \int_{S_E} \Psi_{k,l}(y)\, dy, \end{aligned} \tag{39}$$

where

$$\begin{aligned} \Psi_{k,l}(y) &= \left(\frac{X}{1-\kappa_{SR}^2 X}\right)^k \left(\frac{X}{1-\kappa_{RD}^2 X}\right)^l \\ &\times \frac{y^{m_{RE}-1}}{(1-\kappa_{RE}^2 y)^{m_{RE}+1}} \\ &\times exp\left(-\alpha_{SR}\frac{X}{1-\kappa_{SR}^2 X} - \alpha_{RD}\frac{X}{1-\kappa_{RD}^2 X} - \alpha_{RE}\frac{y}{1-\kappa_{RE}^2 y}\right) \end{aligned} \tag{40}$$

where $X = \tau(1 + y) - 1$.

Proof. Substitute the finite-series complementary CDFs into the general SOP expression and apply the SNDR transformation.

The result links SOP to average SNRs, fading parameters, impairment coefficients, and the secrecy-rate threshold.

3.2. Strictly Positive Secrecy Capacity

The SPSC is defined as

$$P_{\text{SPSC}} = \Pr(C_s > 0). \tag{41}$$

Since $C_s > 0$ is equivalent to $\gamma_D > \gamma_E$, we have

$$P_{\text{SPSC}} = Pr(\gamma_D > \gamma_E) = \int_{S_E} \bar{F}_{\gamma_D}(y) f_{\gamma_E}(y)\, dy \tag{42}$$

Theorem 3. For positive Nakagami-m parameters and arbitrary impairment coefficients, SPSC is

$$P_{\text{SPSC}} = \int_{S_E} \bar{F}_{\gamma_{SR}}(y)\bar{F}_{\gamma_{RD}}(y) f_{\gamma_E}(y)\, dy. \tag{43}$$

Proof. Since $C_s > 0$ is equivalent to $\gamma_D > \gamma_E$, we have

$$P_{\text{SPSC}} = \Pr(\gamma_D > \gamma_E). \tag{44}$$

Conditioning on $\gamma_E = y$ gives

$$\begin{aligned} P_{\text{SPSC}} &= \int_{S_E} \Pr(\gamma_D > y) f_{\gamma_E}(y)\, dy \\ &= \int_{S_E} \bar{F}_{\gamma_D}(y) f_{\gamma_E}(y)\, dy. \end{aligned} \tag{45}$$

Using Lemma 1,

$$\bar{F}_{\gamma_D}(y) = \bar{F}_{\gamma_{SR}}(y)\bar{F}_{\gamma_{RD}}(y), \tag{46}$$

which leads to the desired result. This completes the proof.

For integer fading parameters, the same finite-series substitution gives a finite-sum SPSC expression.

Theorem 4. For positive integer-valued m_{SR}, m_{RD}, and m_{RE}, the SPSC is equivalently represented by the following finite-sum integral representation:

$$P_{\mathrm{SPSC}} = \frac{\alpha_{RE}^{m_{RE}}}{\Gamma(m_{RE})} \sum_{k=0}^{m_{SR}-1} \sum_{l=0}^{m_{RD}-1} \frac{\alpha_{SR}^{k} \alpha_{RD}^{l}}{k!\,l!} \int_{S_E} \Phi_{k,l}(y)\, d \quad (47)$$

where

$$\Phi_{k,l}(y) = \left(\frac{y}{1-\kappa_{SR}^2 y}\right)^{k} \left(\frac{y}{1-\kappa_{RD}^2 y}\right)^{l} \times \frac{y^{m_{RE}-1}}{(1-\kappa_{RE}^2 y)^{m_{RE}+1}}$$
$$\times exp\left(-\alpha_{SR} \frac{y}{1-\kappa_{SR}^2 y} - \alpha_{RD} \frac{y}{1-\kappa_{RD}^2 y} - \alpha_{RE} \frac{y}{1-\kappa_{RE}^2 y}\right). \quad (48)$$

Proof. Insert the finite-series complementary CDFs into the SPSC integral and collect the terms.

SOP describes target-rate failure, while SPSC describes whether any positive secrecy capacity occurs. The two metrics therefore provide complementary views.

Remark 1. When $R_s = 0$, the SOP and SPSC satisfy

$$P_{\mathrm{SPSC}} = 1 - P_{\mathrm{SOP}}. \quad (49)$$

4. Numerical Results and discussion

The analytical expressions are evaluated numerically and checked by Monte Carlo simulation. Unless otherwise stated, the listed parameter values are used, solid curves represent theory, and markers represent simulations.

The simulation cases isolate four effects: fading severity, target secrecy rate, eavesdropper-link strength, and residual hardware distortion.

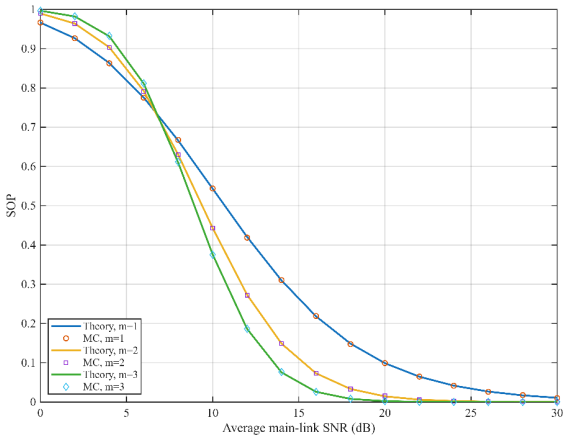

Figure 2. SOP under different Nakagami-m fading parameters

Fig. 2 shows that increasing the main-link SNR lowers SOP. Larger Nakagami-m values also reduce outage because the legitimate hops experience fewer deep fades. The analytical and simulated curves agree closely.

Physically, small m values correspond to stronger channel fluctuations, making the weaker DF hop more likely to dominate. Larger m values stabilize the legitimate channel.

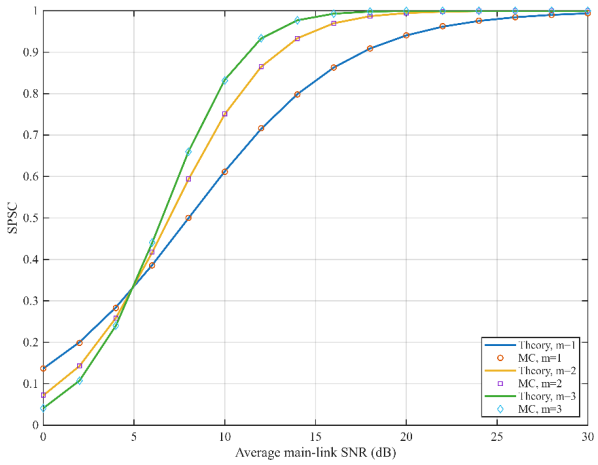

Figure 3. SPSC under different Nakagami-m fading parameters

Fig. 3 shows that SPSC increases with the main-link SNR and approaches one. Larger Nakagami-m values further improve the probability of positive secrecy capacity.

Together, Figs. 2 and 3 indicate that milder fading simultaneously improves both secrecy metrics.

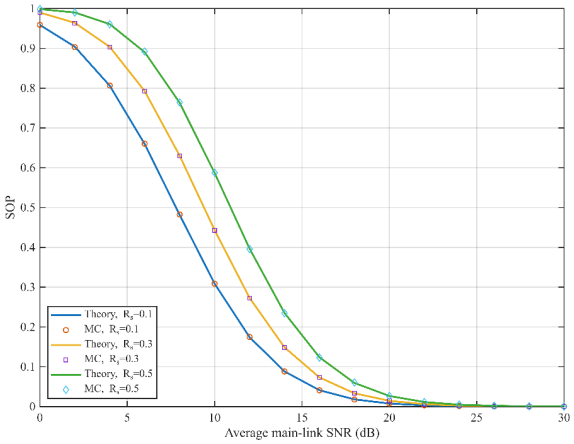

Figure 4. SOP under different target secrecy rates

Fig. 4 shows that increasing the target secrecy rate raises SOP because a larger capacity gap is required between the legitimate and wiretap links.

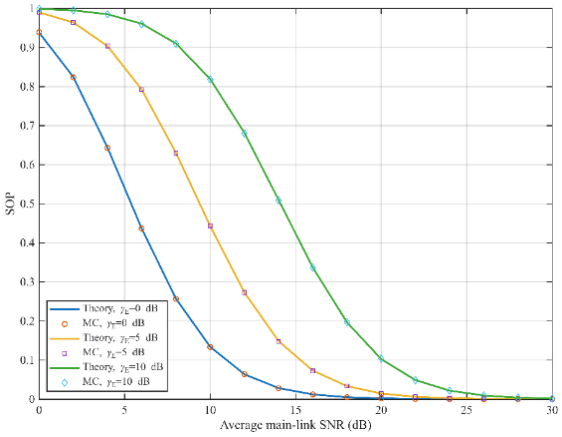

Figure 5. SOP under different eavesdroppers' signal-to-noise ratios

The target-rate effect is strongest at low and medium SNR, where the legitimate channel has limited margin.

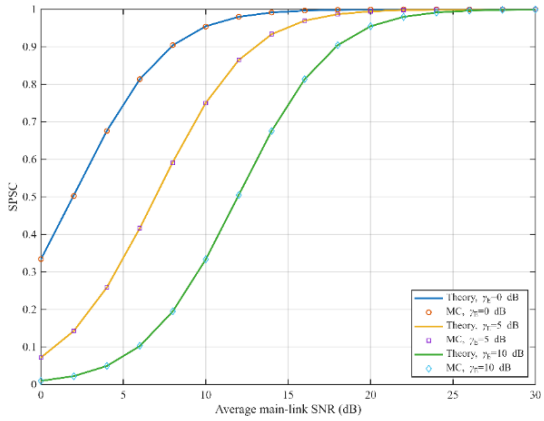

Figure 6. SPSC versus the average main-link SNR for different eavesdropper SNRs

Figs. 5 and 6 show that a stronger eavesdropper link increases SOP and lowers SPSC, confirming that the relay-eavesdropper path is a key limiting factor.

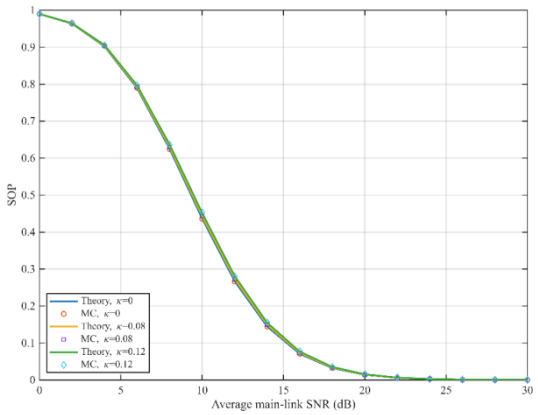

Figure 7. SOP versus the average main-link SNR for different hardware impairment levels

A higher eavesdropper SNR narrows the legitimate-wiretap capacity gap, which explains the observed degradation.

Fig. 7 shows that stronger hardware impairment increases SOP. Distortion reduces the effective legitimate SNDRs and creates earlier saturation, so the ideal-hardware case performs best.

Overall, secrecy improves with better legitimate links and larger Nakagami-m parameters, but degrades with stronger eavesdropping, stricter secrecy-rate requirements, and larger impairment coefficients.

5. Conclusion

This paper studied a fixed DF UAV relay wiretap system with residual hardware impairments over independent Nakagami-m fading links. SOP and SPSC were derived from the equivalent SNDR distributions, and finite-sum integral forms were obtained for integer fading parameters. The results show that secrecy is improved by stronger legitimate links and milder fading, but reduced by a stronger eavesdropper, a higher target rate, and more severe hardware distortion.

The analysis offers a baseline for secure UAV relay design with non-ideal transceivers. Future extensions may consider imperfect CSI, unequal impairments, antenna arrays, artificial noise, relay selection, or UAV mobility.

References

[1] Wyner, A. D. (1975). The wire-tap channel. Bell System Technical Journal, 54(8), 1355-1387.

https://doi.org/10.1002/j.1538-7305.1975.tb02040.x

[2] Leung-Yan-Cheong, S. K., & Hellman, M. E. (1978). The Gaussian wire-tap channel. IEEE Transactions on Information Theory, 24(4), 451-456.

https://doi.org/10.1109/TIT.1978.1055917

[3] Bloch, M., & Barros, J. (2011). Physical-layer security: From information theory to security engineering. Cambridge University Press.

[4] Shiu, Y. S., Chang, S. Y., Wu, H. C., Huang, S. C. H., & Chen, H. H. (2011). Physical layer security in wireless networks: A tutorial. IEEE Wireless Communications, 18(2), 66-74. https://doi.org/10.1109/MWC.2011.5751298

[5] Mukherjee, A., Fakoorian, S. A. A., Huang, J., & Swindlehurst, A. L. (2014). Principles of physical layer security in multiuser wireless networks: A survey. IEEE Communications Surveys & Tutorials, 16(3), 1550-1573.

https://doi.org/10.1109/SURV.2014.012314.00178

[6] Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. Proceedings of the IEEE, 104(9), 1727-1765. https://doi.org/10.1109/JPROC.2016.2558521

[7] Poor, H. V., & Schaefer, R. F. (2017). Wireless physical layer security. Proceedings of the National Academy of Sciences of the United States of America, 114(1), 19-26. https://doi.org/10.1073/pnas.1618130114

[8] Barros, J., & Rodrigues, M. R. D. (2006). Secrecy capacity of wireless channels. In Proceedings of the IEEE International Symposium on Information Theory (ISIT) (pp. 356-360). IEEE. https://doi.org/10.1109/ISIT.2006.261589

[9] Goel, S., & Negi, R. (2008). Guaranteeing secrecy using artificial noise. IEEE Transactions on Wireless Communications, 7(6), 2180-2189.

https://doi.org/10.1109/TWC.2008.060848

[10] Zhou, X., & McKay, M. R. (2010). Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation. IEEE Transactions on Vehicular Technology, 59(8), 3831-3842.

https://doi.org/10.1109/TVT.2010.2056893

[11] Dong, L., Han, Z., Petropulu, A. P., & Poor, H. V. (2010). Improving wireless physical layer security via cooperating relays. IEEE Transactions on Signal Processing, 58(3), 1875-1888. https://doi.org/10.1109/TSP.2009.2036937

[12] Zou, Y., Wang, X., & Shen, W. (2013). Optimal relay selection for physical-layer security in cooperative wireless networks. IEEE Journal on Selected Areas in Communications, 31(10), 2099-2111. https://doi.org/10.1109/JSAC.2013.131016

[13] Kim, J., Ikhlef, A., & Schober, R. (2012). Combined relay selection and cooperative beamforming for physical layer security. Journal of Communications and Networks, 14(4), 364-373. https://doi.org/10.1109/JCN.2012.00053

[14] Mukherjee, A. (2015). Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints. Proceedings of the IEEE, 103(10), 1747-1761. https://doi.org/10.1109/JPROC.2015.2466548

[15] Shetty, N. V., So, D. K. C., & Hamdi, K. A. (2015). Physical layer security in wireless cooperative relay networks: State of the art and beyond. IEEE Communications Magazine, 53(12), 32-39. https://doi.org/10.1109/MCOM.2015.7355582

[16] Jia, P., Ma, X., & Sun, J. (2024). Security performance analysis of SIMO relay networks over wireless fading channels. Radio Engineering, 54(3), 543-549.

[17] Ren, T., Li, G., & Cheng, Y. (2019). Security performance analysis of relay systems with multi-relay and multi-user selection. Telecommunications Science, 35(8), 111-119. https://doi.org/10.11959/j.issn.1000-0801.2019153

[18] Ye, S., Ji, X., & Li, W. (2022). Research on physical layer security of full-duplex UAV relaying. Journal of System Simulation, 34(4), 788-796.

https://doi.org/10.16182/j.issn1004731x.joss.20-0674

[19] Wang, J., Wang, X., Gao, R., Lei, C., Feng, W., Ge, N., Jin, S., & Quek, T. Q. S. (2022). Physical layer security for UAV communications: A comprehensive survey. China Communications, 19(9), 77-115.

https://doi.org/10.23919/JCC.2022.09.007

[20] Sun, X., Ng, D. W. K., Ding, Z., Xu, Y., & Zhong, Z. (2019). Physical layer security in UAV systems: Challenges and opportunities. IEEE Wireless Communications, 26(5), 40-47. https://doi.org/10.1109/MWC.2019.1800487

[21] Krikidis, I., Thompson, J. S., McLaughlin, S., & Goertz, N. (2009). Max-min relay selection for legacy amplify-and-forward systems with interference. IEEE Transactions on Wireless Communications, 8(6), 3016-3027.

https://doi.org/10.1109/TWC.2009.080788

[22] Liang, Y., Poor, H. V., & Shamai, S. (2008). Secure communication over fading channels. IEEE Transactions on Information Theory, 54(6), 2470-2492.

https://doi.org/10.1109/TIT.2008.921678

[23] Oggier, F., & Hassibi, B. (2011). The secrecy capacity of the MIMO wiretap channel. IEEE Transactions on Information Theory, 57(8), 4961-4972.

https://doi.org/10.1109/TIT.2011.2158484

[24] Zhang, X., Zhou, X., & McKay, M. R. (2013). On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels. IEEE Transactions on Vehicular Technology, 62(5), 2170-2181.

https://doi.org/10.1109/TVT.2013.2247771