11th International Conference on Electrical, Electronics and Computer Engineering (IcETRAN), Nis, 3-6 June 2024

Intercept Probability Analysis of Ground-to-UAV Link Attacked by Ground Eavesdropper

Jelena Anastasov
Department of Telecommunications
University of Niš, Faculty of Electronic Engineering
Niš, Serbia
jelena.anastasov@elfak.ni.ac.rs & https://orcid.org/0000-0002-8200-4130

Nenad Milošević
Department of Telecommunications
University of Niš, Faculty of Electronic Engineering
Niš, Serbia
nenad.milosevic@elfak.ni.ac.rs & https://orcid.org/0000-0001-9045-4804

Dejan Milić
Department of Telecommunications
University of Niš, Faculty of Electronic Engineering
Niš, Serbia
dejan.milic@elfak.ni.ac.rs & https://orcid.org/0000-0001-6472-2027

Daniela Milović
Department of Telecommunications
University of Niš, Faculty of Electronic Engineering
Niš, Serbia
daniela.milovic@elfak.ni.ac.rs & https://orcid.org/0000-0003-0615-7853

Aleksandra Panajotović
Department of Telecommunications
University of Niš, Faculty of Electronic Engineering
Niš, Serbia
aleksandra.panajotovic@elfak.ni.ac.rs & https://orcid.org/0000-0003-2865-7357

***Abstract*— In this paper, particular study of security of ground-to-unmanned aerial vehicle (UAV) communication link, on physical layer, in the presence of a ground eavesdropper is given. We characterize the UAV as data collector, which is distributed randomly in a horizontal plane of certain cylindrical region, while a ground user that sends data up to UAV, is located in the centre of cylinder's base. Furthermore, we assume that the eavesdropper is randomly located within a circle which defines the base of the cylindrical region. The main (user-to-UAV) channel is characterized as severely corrupted by the path loss effect, while the wiretap (source-to-eavesdropper) channel is subjected to Fisher-Snedecor fading. Under aforementioned system/channel scenario, the probability of intercept events is investigated. In more details, throughout numerical results, the impact of the predefined cylinder's height and its base's radius, as well as the impact of the fading depth and shadowing severity of the ground wiretap channel, on the intercept probability, is analysed. Related concluding remarks are also given.**

Keywords—physical layer security, fading, unmanned aerial vehicle, eavesdropper

I. Introduction

Unmanned aerial vehicles (UAVs) play a crucial role in a range of applications within smart environments, smart agriculture, and other Internet of Things (IoT) contexts, as well as in military operations, environmental monitoring, surveillance, and emergency response scenarios [1]. Given their widespread use, the study of UAV-assisted communications is increasingly important for both academic research and industrial applications.

UAVs can function as relays, routers, base stations, data collectors or energy suppliers, when integrated with ground or aerial networks. Their capability to facilitate communication or restore connections in disaster-affected areas or power-limited scenarios is enhanced by their rapid deployment [2].

However, UAV-assisted wireless systems often encounter significant security challenges. The communication channels between ground and UAVs, or vice versa, are particularly susceptible to jamming and eavesdropping due to the inherently open nature of wireless broadcasting [3]. Moreover, UAVs frequently operate in a cooperative manner when monitoring wireless networks [2], which complicates the ability to detect and prevent unauthorized interception. In today's extensive wireless network landscape, ensuring that sensitive data remains accessible only to authorized users is essential.

Physical layer security (PLS) approach is regarded as a feasible complement to traditional cryptographic methods [4]. Traditional data transmission security usually involves the use of computationally intensive cryptographic techniques at the network and higher layers [5]. Ciphers once deemed secure are now vulnerable due to the rapid increase in computational capabilities, which could potentially be exploited by malicious etities to compromise transmissions.

The principle of PLS leverages the inherent randomness of the propagation channel along with the stochastic nature of noise, fading, and shadowing. Specifically, PLS enhances the security of confidential data transmission by making decryption more challenging and enabling the secure distribution of secret keys over the physical channel [6]. Unlike traditional cryptography, the effectiveness of PLS does not depend on the eavesdropper’s computational power or their knowledge of the network's parameters.

There are certain investigations on PLS of ground user-to UAV or vice versa transmissions, in the presence of ground eavesdroppers. An overview of emerging techniques designed to counteract eavesdropping and jamming in UAV wireless communication systems is provided in [7]. The performance of the security on physical layer, over Rice and Rayleigh fading channels in IoT, with UAV acting as data collector, is analyzed in [8]. Research in [9] focuses on evaluating the intercept probability and ergodic secrecy capacity to enhance security between two ground nodes, with the support of a UAV serving as a relay. Furthermore, the PLS analysis of a UAV-aided relay connecting an aerial base station and a ground node is detailed in [10].

In this paper, we analyse the intercept probability of the ground-to-aerial transmission in the presence of a ground

ISBN 978-86-6200-001-9 ©2024 AM & ETRAN

https://doi.org/10.69994/11Ic24038

eavesdropper. The analysis is performed assuming that the UAV as aerial node is randomly distributed within a circular horizontal plane. Also, the location of the eavesdropper is assumed to be randomly distributed in circular plane on the ground. The source of confidential data is in the center of the base of cylindrical region. Under a certain geometric system model, theoretical and numerical results are presented in order to highlight the impact of different system and channel parameters on the intercept probability.

II. System and Channel Model

The system model under consideration is shown in Fig.1. The ground node (GN) is a source of confidential information that should be collected by the UAV. We assume that the UAV is initially launched in a 3D space of cylindrical geometry with radius R and height H above the ground plane. The GN is located at the center of the base of this cylindrical region. An eavesdropper (E) tries to overhear the GN-to-UAV communication. It is assumed to be located on the ground within a circle area that defines the base of the cylindric.

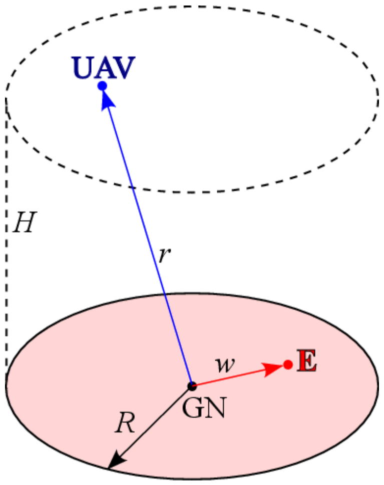

Fig. 1. *System model*

A. Main channel

The GN-to-UAV link is denoted as the main channel (blue line in Fig. 1). The distance r from GN to UAV, when UAV makes spatial excursions in a horizontal circle plane of radius R, at height H, can be defined by the following probability density function (pdf) [11, eq. (11)]

$$p_r(r)=\begin{cases}\dfrac{2r^2}{R^2H}, \text{ for } 0\le r<H\\ \dfrac{2r}{R^2}, \text{ for } H\le r<R\\ \dfrac{2r}{R^2}-\dfrac{2r\sqrt{r^2-R^2}}{R^2H}, \text{ for } R\le r\le\sqrt{R^2+H^2},\end{cases} \tag{1}$$

when $R>H$.

The instantaneous signal-to-noise ratio (SNR) of the main channel, γ_{M}, can be defined as $\gamma_{\mathrm{M}}=\dfrac{P}{\sigma_{\mathrm{M}}^2 r^{\xi_{\mathrm{M}}}}=\dfrac{\overline{\gamma}_{\mathrm{M}}}{r^{\xi_{\mathrm{M}}}}$, where P denotes the transmitting power of GN, σ_{M}^2 denotes variance of the zero-mean additive white Gaussian noise, $\overline{\gamma}_{\mathrm{M}}$ is the average SNR and parameter ξ_{M} is the path loss exponent. Relying on (1) and by some basic variable transformations, we derive the pdf of γ_{M} in the following form

$$p_{\gamma_M}(\gamma)=\begin{cases}\dfrac{2\overline{\gamma}^{\frac{2}{\xi_M}}\gamma^{-\frac{2}{\xi_M}-1}}{\xi_M R^2}-\dfrac{2\overline{\gamma}^{\frac{2}{\xi_M}}\gamma^{-\frac{2}{\xi_M}-1}\sqrt{\left(\dfrac{\overline{\gamma}}{\gamma}\right)^{\frac{2}{\xi_M}}-R^2}}{\xi_M R^2 H},\\ \qquad \text{for } \dfrac{\overline{\gamma}}{\left(R^2+H^2\right)^{\frac{\xi_M}{2}}}\le\gamma\le\dfrac{\overline{\gamma}}{R^{\xi_M}}\\ \dfrac{2\overline{\gamma}^{\frac{2}{\xi_M}}\gamma^{-\frac{2}{\xi_M}-1}}{\xi_M R^2}, \text{ for } \dfrac{\overline{\gamma}}{R^{\xi_M}}\le\gamma<\dfrac{\overline{\gamma}}{H^{\xi_M}}\\ \dfrac{2\overline{\gamma}^{\frac{3}{\xi_M}}\gamma^{-\frac{3}{\xi_M}-1}}{\xi_M R^2 H}, \text{ for } \dfrac{\overline{\gamma}}{H^{\xi_M}}\le\gamma<\infty\end{cases} \tag{2}$$

B. Wiretap channel

According to the information-theory, the GN-to-E channel is recognized as wiretap channel (red line in Fig.1). The distance of the ground eavesdropper from GN, w, is uniformly distributed variable within a circle of radius R. Thus, variable w, can be described by the pdf in the form that follows [12]

$$p_w(w)=\frac{2}{R^2}w. \tag{3}$$

Further, we assume that conditions in wiretap channel are such that the instantaneous SNR is defined as $\gamma_E=\dfrac{|h|^2P}{\sigma_E^2 w^{\xi_E}}$, where h refers to the fading envelope, which follows Fisher-Snedecor (F) distribution, σ_{E}^2 denotes variance of the zero-mean additive white Gaussian noise over wiretap channel, and ξ_{E} is the path loss exponent. We model the GN-to-E channel as F fading channel model regarding that this model is proposed as the best fit for device-to-device communication links, for in- and out-door environments [13].

Therefore, the pdf of γ_{E}, can be obtained in the following way

$$p_{\gamma_{\mathrm{E}}}(\gamma)=\int_0^R p_{\gamma_{\mathrm{E}}|w}(\gamma|w)\,p_w(w)\,dw, \tag{4}$$

with the conditional pdf determined relying on [14, eq. (3)], and including the path loss effect, as

$$p_{\gamma_{\mathrm{E}}|w}\left(\gamma|w\right)=\frac{G_{1,1}^{1,1}\left(\frac{mw^{\xi_{\mathrm{E}}}}{k\bar{\gamma}_{\mathrm{E}}}\gamma\left|\begin{matrix}1-k\\ m\end{matrix}\right.\right)}{\Gamma\left(m\right)\Gamma\left(k\right)\gamma}. \tag{5}$$

The parameters m and k in (5) determine the fading depth and shadowing severity, respectively, and $\bar{\gamma}_{\mathrm{E}}$ denotes the average SNR of wiretap channel. $G_{p,q}^{m,n}\left(z\left|\begin{matrix}-\\ -\end{matrix}\right.\right)$ is notation for Meijer's G function and $\Gamma\left(\cdot\right)$ is notation for Gamma function [15]. By substituting (5) and (3) in (4), and by recalling [16, eq. (26)], after some mathematical manipulations, we derive the pdf of γ_{E}, in the following way

$$p_{\gamma_{\mathrm{E}}}\left(\gamma\right)=\frac{2}{\Gamma\left(m\right)\Gamma\left(k\right)\gamma\xi_{\mathrm{E}}}G_{2,2}^{1,2}\left(\frac{mR^{\xi_{\mathrm{E}}}}{k\bar{\gamma}}\gamma\left|\begin{matrix}1-k,1-\frac{2}{\xi_{\mathrm{E}}}\\ m,-\frac{2}{\xi_{\mathrm{E}}}\end{matrix}\right.\right). \tag{6}$$

III. Intercept Probability

The instantaneous channel capacities, or the Shannon capacity over the main and wiretap channel, can be defined as [9, 17]

$$C_{*}=\log_{2}\left(1+\gamma_{*}\right), \tag{7}$$

where the subscript * denotes either the main (M), either the eavesdropper's (E) i.e. wiretap channel index.

In PLS analysis, the difference between main channel capacity and wiretap channel capacity defines the secrecy capacity, C_s

$$C_{s}=C_{\mathrm{M}}-C_{\mathrm{E}}=\log_{2}\left(\frac{1+\gamma_{\mathrm{M}}}{1+\gamma_{\mathrm{E}}}\right), \tag{8}$$

while assuming that the channel state information are available at all nodes. According to information-theoretic security, the perfect secure communication on physical layer, can be achieved when the wiretap channel becomes degraded version of the main channel.

One of the PLS metrics is the probability of intercept events or intercept probability. This is the probability that the secrecy capacity becomes non-positive. It is defined as [14]

$$P_{\mathrm{int}}=\Pr\left[\gamma_{\mathrm{M}}<\gamma_{\mathrm{E}}\right]=\int_{0}^{\infty}\left(\int_{0}^{\gamma_{\mathrm{E}}}p_{\gamma_{\mathrm{M}}}\left(\gamma_{\mathrm{M}}\right)d\gamma_{\mathrm{M}}\right)p_{\gamma_{\mathrm{E}}}\left(\gamma_{\mathrm{E}}\right)d\gamma_{\mathrm{E}} \tag{9}$$

Thus, by substituting (2) and (6) in (9), the intercept probability can be evaluated, and from that point of view the PLS of aforementioned system model can be analysed.

IV. Numerical Results

Relying to previous theoretical analysis, the following numerical results are obtained.

In Fig.2, intercept probability versus the average SNR of the main channel, is plotted. The impact of different values of the average SNR, $\bar{\gamma}_E$, and the impact of different shadowing severity scenarios' over wiretap channel, on the PLS, is studied. One can notice more pronounced impact of the shadowing shaping factor when the average SNR $\bar{\gamma}_E$ is lower. For instance, for $\bar{\gamma}_M=20$dB when shaping factor k increases from k=1.7 to k=5.7 (the shadowing becomes lighter), the intercept probability decreases for an order of magnitude when $\bar{\gamma}_E=0$dB , and less then a half of an order of magnitude when $\bar{\gamma}_E=10$dB . In any case, when shadowing severity decreases, i.e. k factor increases, the intercept probability also decreases.

In Figs. 3 and 4., we plot the intercept probability as a function of the parameters that define cylindrical region in the system model.

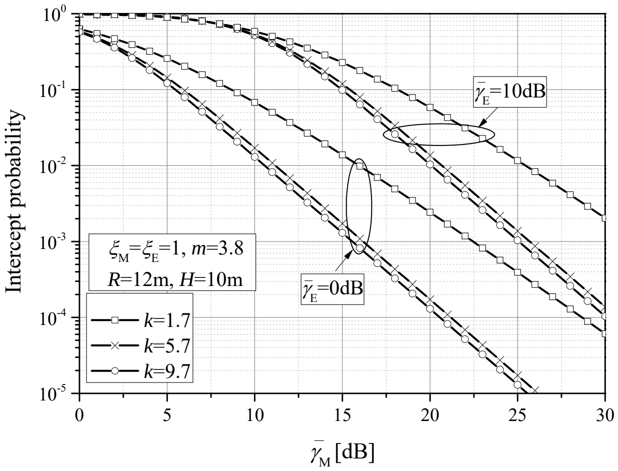

Fig. 2. *Intercept probability vs. the average SNR of main channel*

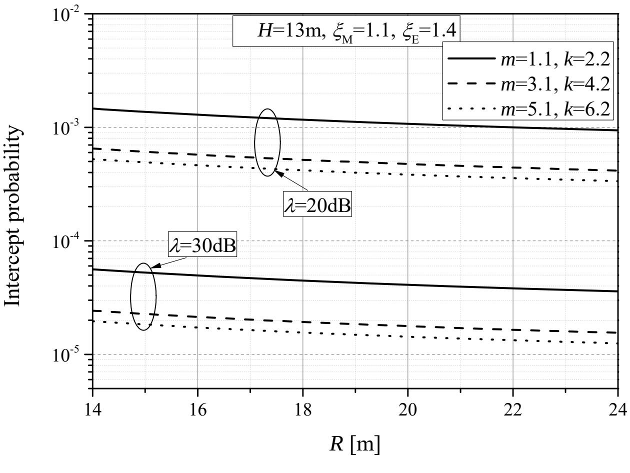

Fig. 3. *Intercept probability vs. the radius for different values of MWRs*

In Fig. 3, intercept probability dependence on the radius R is shown, for different values of the average main-to-wiretap channel power ratio (MWR), i.e. $\lambda=\frac{\bar{\gamma}_{\mathrm{M}}}{\bar{\gamma}_{\mathrm{E}}}$, and for different fading and shadowing conditions. We assume that UAV hovers in the horizontal plane, at a constant height of H=13m. A slight decrease in intercept probability can be observed with the increase in radius. The lowest intercept probabilities are obtained for the lowest fading depth and lightest shadowing severity (m=5.1, k=6.2). On the other hand, by increasing the UAV's altitude H, the intercept probability also increases i.e. the PLS deteriorates (Fig.4).

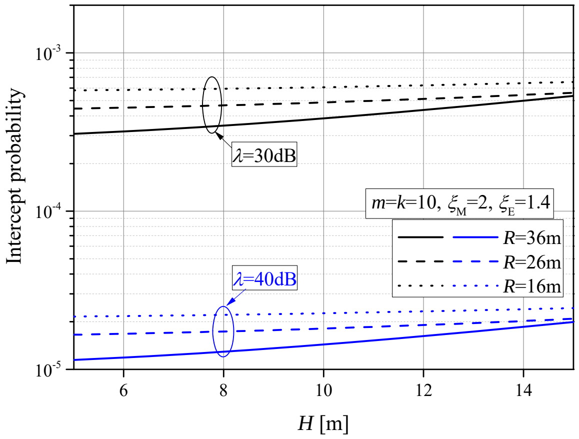

Fig. 4. *Intercept probability vs. the UAV's altitude for different values of MWRs*

The intercept probability dependence on the average SNR of wiretap channel, for different path loss exponents is illustrated in Fig. 5. The figure shows pronounced impact of path loss effects, over both, the main and wiretap channel, on the intercept probability. In this figure, we assume that the path loss exponent is the same for both links. It can be confirmed that the lowest intercept probabilities are obtained for lower path loss effects, when ξ_M=ξ_E=1.1. Also, the impact of the average SNR of main channel is more pronounced when the path loss effects are lower on both channels.

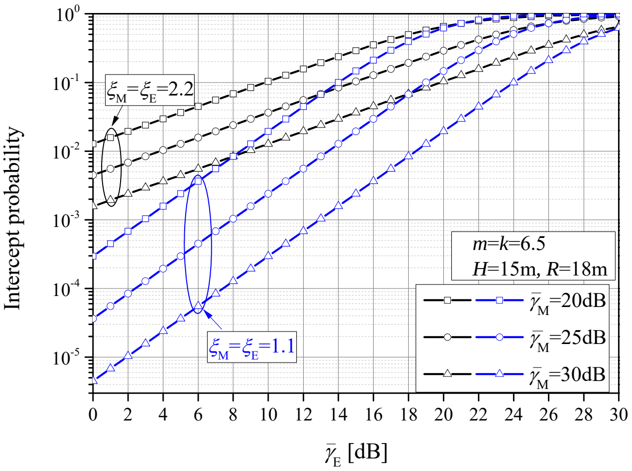

Fig. 5. *Intercept probability vs. the average SNR of wiretap channel for different path loss exponents*

V. Conclusion

In this work, analysis of the probability of intercept events in communication between ground node and UAV in the presence of a UAV eavesdropper, in specific cylindric region, was presented. The ground link was modeled as F fading channel. Obtained results indicated that increasing the average SNR of the main link and decreasing the average SNR of the wiretap link, both reduce the intercept probability. Also, the decrease in UAV height or the increase in the radius of the circle area within which the eavesdropper could be found, improved system security. In addition, the results demonstrated that less severe shadowing and/or lighter fading depth over wiretap channel enhances PLS.

Acknowledgment

This work was supported by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia [grant number 451-03-65/2024-03/200102].

References

[1] B. Alzahrani, O. Sami Oubbati, A. Barnawi, M. Atiquzzaman, D. Alghazzawi, "UAV assistance paradigm: State-of-the-art in applications and challenges," Journal of Network and Computer Applications, vol. 166, no. 15, September 2020.

[2] N. Zhao et al., "UAV-Assisted Emergency Networks in Disasters," in IEEE Wireless Communications, vol. 26, no. 1, pp. 45-51, February 2019.

[3] M. Bloch, J. Barros, *Physical-layer security: from information theory to security engineering,* Cambridge University Press, 2011.

[4] Wang, N., Wang, P., Alipour-Fanid, A., Jiao, L., Zeng, K.: Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities. IEEE Internet of Things Journal,vol. 6, no. 5, pp. 8169-8181, 2019.

[5] Stallings, W.: Cryptography and Network Security, Principles and Practice, 7th edn. Pearson Education, Harlow, England, 2017.

[6] Zhou, X., Song, L., Zhang, Y.: Physical Layer Security in Wireless Communications. Crc Press, Boca Raton, USA 2013.

[7] Sun, X., Ng, D.W.K., Ding, Z., Xu, Y., Zhong, Z.: Physical layer security in UAV systems: Challenges and opportunities. IEEE Wireless Communications vol. 26, no. 5, pp. 40-47, 2019.

[8] Lei, H., Wang, D., Park, K.-H., Ansari, I.S., Jiang, J., Pan, G., Alouini, M.-S.: Safeguarding UAV IoT communication systems against randomly located eavesdroppers. IEEE Internet of Things Journal, vol. 7, no. 2, pp. 1230-1244, 2019.

[9] Bao, T., Yang, H.-C., Hasna, M.O.: Secrecy performance analysis of UAV-assisted relaying communication systems. IEEE Transactions on Vehicular Technology, vol. 69, no. 1, pp. 1122-1126, 2019.

[10] Yang, L., Long, X., Zhang, J.: Secrecy analysis of UAV-aided relaying systems. In: 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), pp. 1-5. IEEE, Antwerp, Belgium (2020).

[11] P. K. Sharma and D. I. Kim, "Random 3D Mobile UAV Networks: Mobility Modeling and Coverage Probability," in IEEE Transactions on Wireless Communications, vol. 18, no. 5, pp. 2527-2538, May 2019.

[12] P.K. Sharma, D. Deepthi and D. I. Kim, "Outage Probability of 3-D Mobile UAV Relaying for Hybrid Satellite-Terrestrial Networks", *IEEE Commun. Lett.*, vol. 24, pp. 418–422, 2020.

[13] S. K. Yoo, S. L. Cotton, P. C. Sofotasios, M. Matthaiou, M. Valkama and G. K. Karagiannidis, "The Fisher–Snedecor *F* Distribution: A Simple and Accurate Composite Fading Model," in IEEE Communications Letters, vol. 21, no. 7, pp. 1661-1664, July 2017.

[14] L. Kong and G. Kaddoum, "On Physical Layer Security Over the Fisher-Snedecor *F* Wiretap Fading Channels," in *IEEE Access*, vol. 6, pp. 39466-39472, 2018.

[15] I. S. Gradshteyn and I. M. Ryzhik, Table of Integrals, Series, and Products, 6th ed. San Diego, CA, USA, Academic Press, 2000.

[16] V. S. Adamchik, O. I. Marichev, "The Algorithm for Calculating Integrals of Hypergeometric Type Functions and Its Realization in Reduce System", ISSAC'90 Conference Proceedings, Tokyo, Japan, pp. 212-224, Tokyo, Japan, 1990.

[17] M. Bloch, J. Barros, M. Rodrigues and S. McLaughlin, "Wireless Information-Theoretic Security", *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515-2534, 2008.