Analysis of intercept events in hybrid satellite-terrestrial relay network in the presence of an eavesdropper

Aleksandra Cvetković, Jelena Anastasov, Dejan Milić, Daniela Milović, and Goran Đorđević

Abstract – **In this paper, we analyse the physical layer security of hybrid satellite-terrestrial relay networks (HSTRN). The HSTRN interconnects a satellite and destination node over decode-and-forward relay in the presence of an eavesdropper which tries to overhear satellite-relay communication. The satellite-relay link as well as satellite-eavesdropper link is subjected to shadowed-Rician fading while the terrestrial relay-destination link is corrupted by Rician fading. According to the existence of the line of sight component between relay and destination, eavesdropper is ineffective in intercepting of relay-destination transmission. Under given system scenario, we evaluate the probability of intercept and analyse the impact of various fading/shadowing channel conditions and other system parameters on secrecy performance. Monte Carlo simulations are also presented to confirm derived analytical expression.**

Keywords– **Decode-and-forward relay, Eavesdropper, Hybrid satellite-terrestrial relay network, Intercept probability.**

I. Introduction

The application of land-mobile satellite (LMS) communication is widely spread for broadcasting, navigation and rescue, in both the civil and military areas [1]. The nature and large area of LMS systems coverage makes it vulnerable for eavesdropping attack by illegitimate terrestrial nodes [2]. Due to the fact that the line-of-sight (LoS) links between the satellite and terrestrial destination nodes are often blocked by bad weather conditions or surrounding obstacles, the usage of relay between satellites and intended users is required. Thus, the advances in enhancing LMS communication are recently investigated in the context of hybrid satellite-terrestrial relay network (HSTRN) security issues.

Traditionally, cryptographic technology provides a certain level of security transmission imposing additional system complexity. This is beneficial when eavesdropper is computationally limited. Alternatively, an eavesdropper with unlimited computing power can easily decrypt cryptogram due to the *brute force attack* [3] and thus increase the system's security risk.

Apart from upper layer cryptographic techniques, physical layer security (PLS) can strengthen the secure wireless transmission by exploring dynamic nature of propagation channels [4]. The PLS of satellite-terrestrial communication has been widely explored in literature. In [5], secrecy outage probability of typical wiretapped satellite communication network is analysed. The LMS secrecy performance, where satellite employs the spot beam technique, and both the terrestrial user and eavesdropper [6] or eavesdroppers [7], are equipped with multiple antennas and utilize maximal ratio combining to receive the confidential message, is investigated.

In [8-12], a relay or even multiple relays are employed to enhance the PLS of satellite-terrestrial communication. A multi-antenna amplify-and-forward (AF) relay has been adopted in [8] to increase the secrecy capacity of HSTRN in the presence of an eavesdropper. System model in [8] refers to the scenario where user and eavesdropper are out of exclusion region. Authors in [9] employed both the AF and decode and forward (DF) relay protocols to evaluate ergodic secrecy rate in the presence of multiple eavesdropping attack. Typically, the satellite-relay channel is modeled by shadowed-Rician fading model [6-12], while the relay-destination link was treated as Rayleigh fading model [8], [9], or even as Gamma-gamma turbulence model in hybrid satellite-FSO system [10]. In addition, the PLS of HSTRN was also investigated in [11], [12] by employing different relay selection methods.

In this paper, we derive a novel expression for intercept probability of HSTRN. The information is transmitted to the destination via a DF relay and an eavesdropper tries to intercept satellite-relay signal transmission. The impact of channel condition parameters, the relay and eavesdropper antennas surface area ratio, and the average SNR values on the overall system secrecy performance, is shown. Independent Monte Carlo simulations confirm accuracy of presented analytics.

II. Problem Formulation

The system model we analysed in this paper is shown in the Fig. 1. A communication between the satellite (S) and the destination user (D) can not be performed directly but only via DF relay (R). This refers to a real military scenario for special security issues. For this purpose, a relay is equipped by a large dimensional antenna and relay-destination transmission is highly directional. An eavesdropper tries to intercept transmitted data from the satellite to intended user. Due to the fact that R-D communication is directed, eavesdropper (E) is incapable of overhearing R-D transmission phase but only S-R transmission phase. Typically, the eavesdropping attack should be hidden and therefore we assume that eavesdropper antenna's dimensions are noticeable smaller.

The S-R and S-E links are subjected to shadowed-Rician fading while the terrestrial R-D link is corrupted by Rician fading due to the existence of LoS component.

[1] Aleksandra M. Cvetković, Jelena A. Anastasov, Daniela M. Milović, Dejan N. Milić and Goran T. Đorđević are with the University of Niš, Faculty of Electronic Engineering, Aleksandra Medvedeva 14, 18000 Nis, Serbia, E-mails: {aleksandra.cvetkovic, jelena.anastasov, daniela.milovic, dejan.milic, goran.t.djordjevic}@elfak.ni.ac.rs.

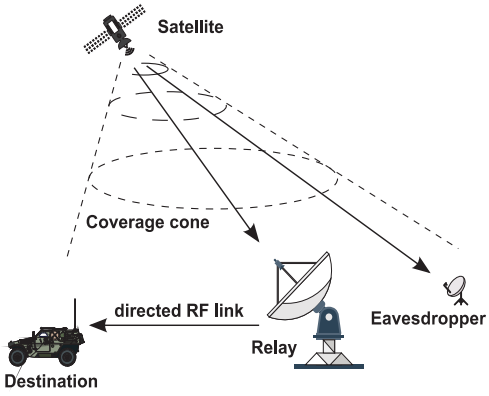

Fig. 1. System model

A. Satellite-terrestrial channels

The shadowed-Rician distribution was proposed in [13] for modeling signal amplitude over LMS channel and the probability density function (PDF) of the instantaneous signal-to-noise ratio (SNR) at the relay/eavesdropper node, $\gamma_* = E_s|h_*|^2/\sigma^2$, is

$$p_{\gamma_*}(x) = \frac{\alpha_*}{E_s/\sigma^2}\exp\left(-\frac{\beta_* x}{E_s/\sigma^2}\right){}_1F_1\left(m_*,1,\frac{\delta_* x}{E_s/\sigma^2}\right). \quad (1)$$

Where $*=\{SR,SE\}$ denotes parameters of S-R and S-E communication. In Eq. (1), ${}_1F_1(.;.;.)$ is the confluent hypergeometric function [14, Eq. (9.210.1)], E_s denotes the satellite average energy and σ^2 is variance of additive white Gaussian noise (AWGN). The parameters α_*, β_* and δ_* can be calculated as

$$\alpha_* = \frac{1}{2b_*}\left(\frac{2b_*m_*}{2b_*m_*+\Omega_*}\right)^{m_*},\ \beta_* = \frac{1}{2b_*},\ \delta_* = \frac{\Omega_*}{2b_*(2b_*m_*+\Omega_*)}, \quad (2)$$

wherein $2b_*$ is the average power of the multipath components, Ω_* is average power of the LoS component and m_* is Nakagami-m parameter in shadowed-Rician links. For integer values of the fading parameter m_*, ${}_1F_1(.;.;.)$ can be simplified using [15, Eq. (07.20.03.0009.01)] and [15, Eq. (05.02.06.0005.01)] and thus (1) can be rewritten as

$$p_{\gamma_*}(\gamma) = \frac{\alpha_*}{E_s/\sigma^2}e^{-\frac{\beta_*-\delta_*}{E_s/\sigma^2}\gamma}\sum_{k=0}^{m_*-1}\frac{1}{k!}\binom{m_*-1}{m_*-1-k}\left(\frac{\delta_*}{E_s/\sigma^2}\right)^k\gamma^k. \quad (3)$$

Based on Eq. (3), the complementary cumulative density function (CCDF) can be determined using [14, Eq. (3.351.2)]

$$\bar{F}_*(\gamma) = \frac{\alpha_*}{\beta_*-\delta_*}\sum_{k=0}^{m_*-1}\sum_{l=0}^{k}\frac{1}{l!}\binom{m_*-1}{m_*-1-k} \times\left(\frac{\delta_*}{\beta_*-\delta_*}\right)^k\left(\frac{\beta_*-\delta_*}{E_s/\sigma^2}\right)^l e^{-\frac{\beta_*-\delta_*}{E_s/\sigma^2}\gamma}\gamma^l. \quad (4)$$

B. Relay-user channel

We assume that relay position enables the LoS signal component between R and D. Also, it is assumed that fading over R-D channel follows Rician distribution. The PDF of the instantaneous SNR at the destination node is

$$p_{\gamma_{RD}}(\gamma) = \frac{(K+1)e^{-K}}{\bar{\gamma}_{RD}}e^{-\frac{(K+1)\gamma}{\bar{\gamma}_{RD}}}I_0\left(2\sqrt{\frac{K(K+1)\gamma}{\bar{\gamma}_{RD}}}\right), \quad (5)$$

where K denotes the Rician K factor (K is the ratio of the power of the LoS component to the average power of the scattered component), $\bar{\gamma}_{RD} = E\left[\gamma_{RD}^2\right]$ is the average SNR at the D and $I_0(x)$ is the zero-th order modified Bessel function of the first kind [14, Eq. (8.431.1)]. By using the infinite-series representation of $I_0(.)$ [14, Eq. (8.447.1)], the CCDF of the instantaneous SNR can be written in the following form

$$\bar{F}_{RD}(\gamma) = e^{-K}e^{-\frac{K+1}{\bar{\gamma}_{RD}}\gamma}\sum_{i=0}^{\infty}\sum_{j=0}^{i}\frac{K^i}{i!\,j!}\left(\frac{K+1}{\bar{\gamma}_{RD}}\right)^j\gamma^j. \quad (6)$$

C. Satellite -user subsystem

Under the DF relay strategy, for non-identically distributed S-R and R-D link, we can determine the CDF of γ_d in the following form

$$F_{\gamma_d}(\gamma) = 1-\left(1-F_{SR}(\gamma)\right)\left(1-F_{RD}(\gamma)\right) = 1-\bar{F}_{SR}(\gamma)\bar{F}_{RD}(\gamma), \quad (7)$$

where $\gamma_d = \min\{\gamma_{SR},\gamma_{RD}\}$. By substituting Eq. (4) for $*=SR$ and Eq. (6) into Eq. (7) we get

$$F_{\gamma_d}(\gamma) = 1-\frac{\alpha_{SR}e^{-K}}{\beta_{SR}-\delta_{SR}}\sum_{k=0}^{m_{SR}-1}\sum_{l=0}^{k}\sum_{i=0}^{\infty}\sum_{j=0}^{i}\frac{K^i}{i!\,j!\,l!}\binom{m_{SR}-1}{m_{SR}-1-k} \times\left(\frac{\delta_{SR}}{\beta_{SR}-\delta_{SR}}\right)^k\left(\frac{\beta_{SR}-\delta_{SR}}{E_s/\sigma^2}\right)^l\left(\frac{K+1}{\bar{\gamma}_{RD}}\right)^j e^{-\left(\frac{\beta_{SR}-\delta_{SR}}{E_s/\sigma^2}+\frac{K+1}{\bar{\gamma}_{RD}}\right)\gamma}\gamma^{l+j}. \quad (8)$$

III. Probability of Intercept

According to the Shannon capacity formula, we can evaluate the instantaneous channel capacity of the satellite-user subsystem as

$$R_d = \log_2(1+\gamma_d). \quad (9)$$

We have already assumed a possible presence of an eavesdropper that attempts to intercept S-R transmission. Thus, the wiretap S-E channel capacity can be calculated as

$$R_e = \log_2(1+\gamma_{SE}). \quad (10)$$

The occurrence of interception event i.e. intercept probability is defined as a probability that the transmission

rate of the main link falls below the rate on the wiretap link (secrecy rate becomes non-positive), in the following way [16]

$$P_{\text{int}} = \Pr\left[R_d - R_e < 0\right] = \Pr\left[\gamma_d < \gamma_{SE}\right]. \tag{11}$$

After some mathematical manipulations, the previous formula becomes

$$\begin{aligned} P_{\text{int}} &= \int_0^{\infty}\int_0^{\gamma_e} p_d(\gamma_d)\, p_{SE}(\gamma_e)\, d\gamma_d d\gamma_e \\ &= \int_0^{\infty} F_{\gamma_d}(\gamma_e)\, p_{SE}(\gamma_e)\, d\gamma_e. \end{aligned} \tag{12}$$

Further, by substituting Eq. (8) and Eq. (3) for $* = SE$ in Eq. (12) and assuming that relay-eavesdropper antenna's surface area ratios is denoted by λ, we get

$$\begin{aligned} P_{\text{int}} = 1 - \frac{\alpha_{SR} e^{-K}}{\beta_{SR} - \delta_{SR}} \frac{\alpha_{SE}}{E_s/\lambda/\sigma^2} \sum_{k=0}^{m_{SR}-1} \sum_{l=0}^{k} \sum_{i=0}^{\infty} \sum_{j=0}^{i} \sum_{r=0}^{m_{SE}-1} \frac{K^i}{i!\, j!\, l!\, r!} \\ \times \binom{m_{SR}-1}{m_{SR}-1-k} \binom{m_{SE}-1}{m_{SE}-1-r} \left(\frac{\delta_{SR}}{\beta_{SR}-\delta_{SR}}\right)^k \left(\frac{\beta_{SR}-\delta_{SR}}{E_s/\sigma^2}\right)^l \\ \times \left(\frac{\delta_{SE}}{E_s/\lambda/\sigma^2}\right)^r \left(\frac{K+1}{\overline{\gamma}_{RD}}\right)^j \int_0^{\infty} \gamma^{l+j+r} e^{-\left(\frac{\beta_{SR}-\delta_{SR}}{E_s/\sigma^2} + \frac{K+1}{\overline{\gamma}_{RD}} + \frac{\beta_{SE}-\delta_{SE}}{E_s/\lambda/\sigma^2}\right)\gamma} d\gamma. \end{aligned} \tag{13}$$

The antenna's dimension has the influence of the received energy thus the relay-eavesdropper antenna's surface area ratios is equivalent to relay-eavesdropper received power ratio.

Applying [14, Eq. (8.310.1)] in Eq. (13), the intercept probability can be determined in a closed-form expression as

$$\begin{aligned} P_{\text{int}} = 1 - \frac{\alpha_{SR} e^{-K}}{\beta_{SR} - \delta_{SR}} \frac{\alpha_{SE}}{E_s/\lambda/\sigma^2} \sum_{k=0}^{m_{SR}-1} \sum_{l=0}^{k} \sum_{i=0}^{\infty} \sum_{j=0}^{i} \sum_{r=0}^{m_{SE}-1} \frac{K^i (l+j+r)!}{i!\, j!\, l!\, r!} \\ \times \binom{m_{SR}-1}{m_{SR}-1-k} \binom{m_{SE}-1}{m_{SE}-1-r} \left(\frac{\delta_{SR}}{\beta_{SR}-\delta_{SR}}\right)^k \left(\frac{\beta_{SR}-\delta_{SR}}{E_s/\sigma^2}\right)^l \\ \times \left(\frac{\delta_{SE}}{E_s/\lambda/\sigma^2}\right)^r \left(\frac{K+1}{\overline{\gamma}_{RD}}\right)^j \left(\frac{\beta_{SR}-\delta_{SR}}{E_s/\sigma^2} + \frac{K+1}{\overline{\gamma}_{RD}} + \frac{\beta_{SE}-\delta_{SE}}{E_s/\lambda/\sigma^2}\right)^{-1-l-j-r}. \end{aligned} \tag{14}$$

Approximately 20 terms are needed to bound infinity summation in Eq. (14) in order to achieve sufficient accuracy in evaluating P_{int}.

IV. Numerical Results

In this section we present numerical and simulation results for observed system. Numerical results are obtained based on the derived analytical expression (14). The satellite links are modeled as shadowed-Rician fading channels and utilized parameters that define different shadowing severity levels are: frequent heavy shadowing (b_*=0.063, m_*=1, Ω_* =8.94×10^{-4}), average shadowing (b_*=0.126, m_*=10, Ω_*=0.835), and infrequent light shadowing (b_*= 0.158, m_*= 19, Ω_*=1.29) [10].

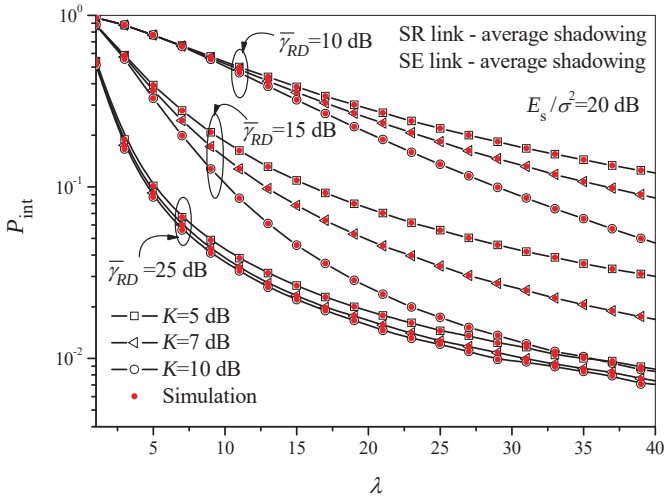

Fig. 2. Intercept probability versus the relay-eavesdropper antenna's surface area ratios

In Fig. 2, the intercept probability versus the ratio of relay and eavesdropper's antenna surface area is shown. We assume average shadowing conditions over shadowed-Rician links and constant satellite's emitting power. As expected, for higher values of parameter λ, the probability of intercept decreases and the communication between satellite and intended user via relay is secured. Also, when signal power at R-D link increases and/or Rician K factor increases, the probabilities of intercept are lower.

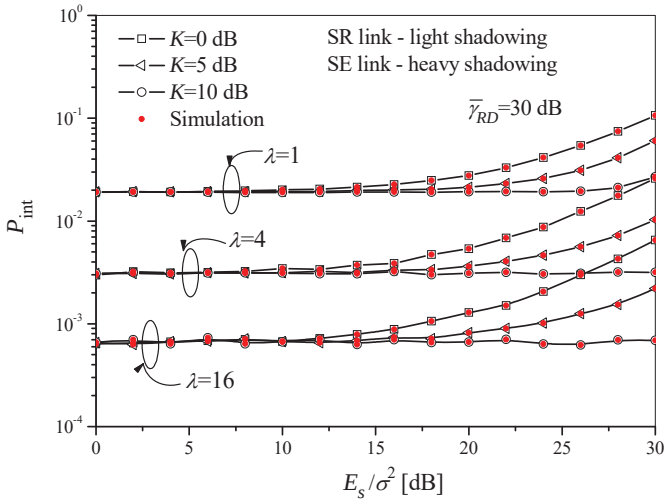

Fig. 3. Intercept probability versus the satellite emitting power for various K factors

The intercept probability dependence on the satellite's emitting power is presented in the Fig. 3. The S-R link is corrupted by light shadowing while S-E link is in heavy shadowing. We can notice that up to some specific value of satellite emitting power, the intercept probability is a constant defined by the ratio λ. For lower E_s/σ^2 values, the intercept probability depends exclusively on the S-R and S-E channel conditions and the influence of terrestrial channel conditions are marginal. Further amplification of the satellite's emitting power does not enhance the system PLS, even for favorable R-D channel conditions.

Intercept probability versus the average signal power on the R-D link for different satellite emitting power is shown in Fig. 4. It is obvious that scenario with S-E link in the heavy shadowing is beneficial for security issues. Also, we can notice that after some specific values of the average SNR, $\overline{\gamma}_{RD}$, the intercept probability tends to irreducible floor. Thus, a further variation of the system parameters don't affect security risk. In addition, the impact of satellite emitting power is more pronounced for lower-to-medium $\overline{\gamma}_{RD}$ values showing higher impact of satellite-terrestrial links.

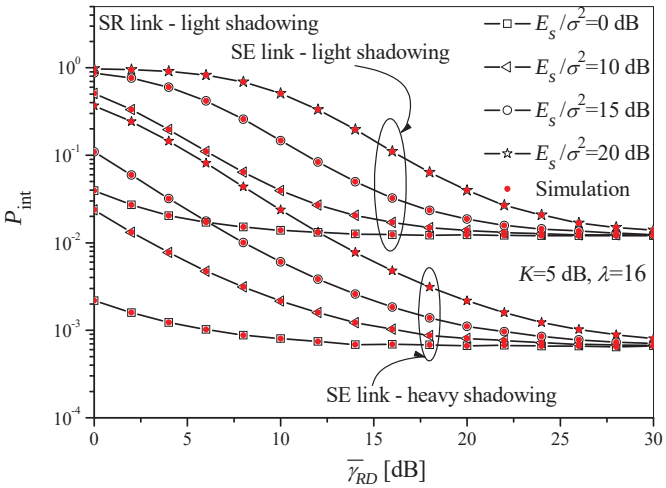

Fig. 4. Intercept probability versus the relay-destination average signal power under different shadowing conditions

In overall, the independent Monte Carlo simulations showed good agreement with analytical results presented in Figs. 2., 3. and 4.

V. Conclusion

In this paper, the probability of intercept of HSTRN with the DF relay in the presence of an eavesdropping attack is analyzed. Analytical expression for intercept probability is derived for integer fading parameter value of shadowed LoS component over satellite channels. The obtained results are in excellent agreement with the simulation results which were performed independently.

We showed that employment of dimensionally larger antenna at the relay brings benefits in the system PLS. Strengthen domination of LoS component at the R-D link also enhances the overall system performance. Lower intercept probability values are obtained when the wiretapped S-E link is in heavy shadowing, as expected.

Acknowledgement

This work was supported by Ministry of science and technology development of Republic of Serbia (grants III-44006 and TR-32051).

References

[1] A. Vanelli-Coralli et al., "Satellite Communications: Research Trends and Open Issues", IWSSC 2007, Conference Proceedings, pp. 71-75, Salzburg, Austria, 2007.

[2] A. Roy-Chowdhury, J. S. Baras, M. Hadjitheodosiou, and S. Papademetriou, "Security Issues in Hybrid Networks with a Satellite Component", IEEE Wireless Commun., vol. 12, no. 6, pp. 50-61, 2005.

[3] F. Gandino, B. Montrucchio and M. Rebaudengo, "Key Management for Static Wireless Sensor Networks with Node Adding," IEEE Trans. Industrial Informatics, vol. 10, no. 2, pp. 1133-1143, 2014.

[4] G. Zheng, P.-D. Arapoglou and B. Ottersten, "Physical Layer Security in Multibeam Satellite Systems", IEEE Trans. Wireless Commun., vol. 11, no. 2, pp. 852-863, 2012.

[5] K. An, M. Lin, T. Liang, J. Ouyang, C. Yuan and W. Lu "Secrecy Performance Analysis of Land Mobile Satellite Communication Systems over Shadowed-Rician Fading Channels", WOCC 2016, Conference Proceedings, Chengdu, China, 2016.

[6] K. An, T. Liang, X. Yan and G. Zheng, "On the Secrecy Performance of Land Mobile Satellite Communication Systems", IEEE Access, vol. 6, pp. 39606-39620, 2018.

[7] Y. Li, K. An, T. Liang and X. Yan, "Secrecy Performance of Land Mobile Satellite Systems With Imperfect Channel Estimation and Multiple Eavesdroppers", IEEE Access, vol. 7, pp. 31751-31761, 2019.

[8] K. An, M. Lin, T. Liang, J. Ouyang, C. Yuan and Y. Li, "Secure Transmission in Multi-antenna Hybrid Satellite-Terrestrial Relay Networks in the Presence of Eavesdropper", WCSP 2015, Conference Proceedings, Nanjing, China, 2015.

[9] Q. Huang, M. Lin, K. An, J. Ouyang and W.-P. Zhu, "Secrecy Performance of Hybrid Satellite Terrestrial Relay Networks in the Presence of Multiple Eavesdroppers", IET Commun., vol. 12 , no. 1, pp. 26-34, 2018.

[10] Y. Ai, A. Mathur, M. Cheffena, M. R. Bhatnagar and H. Lei, "Physical Layer Security of Hybrid Satellite-FSO Cooperative Systems", IEEE Photonics J., vol.11, no. 1, 2019.

[11] V. Bankey, P. K. Upadhyay, "Physical Layer Security of Multiuser Multirelay Hybrid Satellite-Terrestrial Relay Networks", IEEE Trans. Veh. Technol., vol. 68, no. 3, pp. 2488-2501, 2019.

[12] W. Cao, Y. Zou, Z. Yang and J. Zhu, "Relay Selection for Improving Physical-Layer Security in Hybrid Satellite-Terrestrial Relay Networks", IEEE Access, vol. 6, pp. 65275-65285, 2018.

[13] A. Abdi, W. Lau, M.-S. Alouini, and M. Kaveh, "A New Simple Model for Land Mobile Satellite Channels: First and Second Order Statistics", IEEE Trans. Wireless Commun., vol. 2, no. 3, pp. 519–528, 2003.

[14] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. San Diego, CA, USA: Academic, 2007.

[15] The Wolfarm Functions Site, 2008. [Online] Available: http://functions.wolfram.com/

[16] N. Milošević, J. Anastasov, A. Cvetković, D. Milović and D. Milić, "On the Intercept Probability of DF Relaying Wireless Communication", Wireless Pers. Commun., vol. 104, no. 4, pp 1523–1533, 2019.