<table>
<thead>
<tr>
<th>Item Type</th>
<th>Article</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authors</td>
<td>Pattanayak, Dipti R.; Dwivedi, Vivek K.; Karwal, Vikram; Ansari, Imran Shafique; Lei, Hongjiang; Alouini, Mohamed-Slim</td>
</tr>
<tr>
<td>Eprint version</td>
<td>Pre-print</td>
</tr>
<tr>
<td>DOI</td>
<td>10.1109/LWC.2020.2979442</td>
</tr>
<tr>
<td>Publisher</td>
<td>Institute of Electrical and Electronics Engineers (IEEE)</td>
</tr>
<tr>
<td>Journal</td>
<td>IEEE Wireless Communications Letters</td>
</tr>
<tr>
<td>Rights</td>
<td>(c) 2020 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other users, including reprinting/ republishing this material for advertising or promotional purposes, creating new collective works for resale or redistribution to servers or lists, or reuse of any copyrighted components of this work in other works.; This file is an open access version redistributed from: <a href="http://arxiv.org/pdf/1907.03117">http://arxiv.org/pdf/1907.03117</a></td>
</tr>
<tr>
<td>Download date</td>
<td>2023-11-01 04:57:26</td>
</tr>
<tr>
<td>Link to Item</td>
<td><a href="http://hdl.handle.net/10754/662111">http://hdl.handle.net/10754/662111</a></td>
</tr>
</tbody>
</table>
On the Physical Layer Security of a Decode and Forward Based Mixed FSO/RF Cooperative System

Dipti R. Pattanayak, Student Member, IEEE, Vivek K. Dwivedi, Member, IEEE, Vikram Karwal, Senior Member, IEEE, Imran Shafique Ansari, Member, IEEE, Hongjiang Lei, Member, IEEE, and Mohamed-Slim Alouini, Fellow, IEEE

Abstract—In this letter, the secrecy performance of a mixed free space optics (FSO) and radio frequency (RF) system is analyzed from physical layer security (PHY) perspective. In this scenario, one or more eavesdroppers are trying to intercept the confidential signal in a mixed FSO/RF system. The faded FSO links are modeled by Málaga ($\mathcal{M}$) distribution and RF link is characterized by Nakagami-$m$ distribution. Exact closed form expressions for secrecy performance metrics such as secrecy outage probability and strictly positive secrecy capacity are derived and analyzed for the proposed system in terms of Fox's $H$-function. Furthermore, the asymptotic expressions for these performance metrics are analyzed. Finally, all the results are verified by Monte-Carlo simulations.

Index Terms—Physical layer security (PHY), Mixed FSO/RF, Málaga, Nakagami-$m$, secrecy outage probability (SOP), strictly positive secrecy capacity (SPSC).

I. INTRODUCTION

Physical Layer Security and protection have progressively become issues of interest in wireless communication network [1-9]. Wireless communication is more vulnerable to eavesdropping because of its broadcast nature. An enormous amount of classified and sensitive data e.g. budget information, client documents, military information, healthcare records, etc. are transmitted by means of wireless channel. The inherent openness of wireless medium permits anyone inside the scope to track the signal, which makes the data security one of the most critical and troublesome issues in wireless systems. Traditionally the data security is handled by cryptographic approach (used in Application layer (layer 7), network layer (layer 3), and data-link layer (layer 2)) [2]. Generally, cryptographic approach is based on the data encryption method. Because of advancement in breaking of encrypted algorithms, this method is always vulnerable for security. Subsequently, new security approaches are incorporated based on the information theory fundamentals i.e. focusing on the secrecy capacity of the channel. This is termed as physical layer security (PHY) and it is handled in the physical layer [3-7]. PHY solution is basically achieved by using different methods such as code based, signalling based, and physical layer encryption based methods.

Many researchers put their effort to analyze the secrecy performance from RF perspective by analyzing the secrecy performance for various fading channels. The performance of a wiretap channel was first introduced by Wyner [1] in which a source is trying to communicate with the destination in the presence of an external eavesdropper. Based on the nature of the propagation channel, researchers focused on various fading distributions to mitigate the piracy such as: generalized $K$ [2], $\alpha$-$\mu$ [3], generalized Gamma [4] etc. On the other side due to channel scattering, atmospheric turbulence, pointing deflection and optical beam divergence [5], there is a possibility of eavesdropping of confidential data. Therefore authors in [6] pointed out the data eavesdropping due to optical beam divergence and turbulence effect. The analysis in [6] also concludes that a eavesdropper can be able to overhear the data if it is very close to the legitimate node. Then in [7], it is investigated that the information can be overheard from outside the laser beam converging area through an non-line of sight (NLOS) scattering channel. In [8] it is highlighted that the eavesdropping also possible, if the beam is reflected by a small particle or blocked by a suitable obstacle. Then some efforts have been devoted to analyze the FSO link from PHY perspective such as: in [9], authors explore the PHY for a FSO channel characterized by Málaga ($\mathcal{M}$) distribution and analysed the secrecy outage probability (SOP), strictly positive secrecy capacity (SPSC) and average secrecy capacity (ASC) as a performance metrics.

Moreover, the research was extended for cooperative relaying based approach to achieve the secure communication [9]. Such relaying approach is mainly used in mixed FSO/RF environments to get the benefits of FSO to the end user level. Authors in [10] considered a mixed RF/FSO (uplink) environment by analysing the performance metrics such as: SOP and ASC, where the RF link is modeled by Nakagami-$m$ distribution and FSO link is characterized by Gamma-Gamma (GG) distribution. During analysis the eavesdropper is considered to be located in th RF link, modelled by Nakagami-$m$ distribution. Furthermore, in [11], the outage probability, average symbol error rate, channel capacity and intercept probability for a mixed RF/FSO system were analysed from RF security perspective. Similarly in [12], the PHY analysis is done for a hybrid satellite-FSO co-operative system where the satellite link is modelled by the shadowed Rician distribution and FSO link is assumed to be Gamma-Gamma fading distribution. Security analysis was further extended for downlink RF/FSO system i.e. FSO/RF system in [13]. The FSO/RF system has the advantage to serve multiple RF users with different data rates [14]. However, reported works in RF/FSO and FSO/RF scenarios are limited to the secrecy performance analysis for the RF side eavesdroppers only. This motivates to explore the PHY performance for a FSO/RF system, where an optical eavesdropper at relay is trying to interrupt the
communication. The main contributions of this work are:

1) So far no literature on PHY analysis is available in the context of information overhearing from RF based eavesdropper as well as FSO based eavesdropper simultaneously in a mixed FSO/RF system. More specifically during analysis, we have considered the worst case scenario by assuming that the confidential data is intercepted in each hop of the system i.e. eavesdroppers are trying to intercept the signal from FSO as well as RF links simultaneously.

2) The closed form expressions for secrecy performance metrics such as SOP and SPSC in wide range of fading severity (i.e. moderate, and strong regions) is derived under the impact of pointing error and different FSO data detection methods.

3) The SOP and SPSC expressions are obtained in terms of Meijer’s-function and bivariate Fox’s H-function (i.e. EGBFHF).

4) Further, the derived closed form results are expressed asymptotically to validate the proposed work and finally all the results are validated through Monte-Carlo simulation.

II. SYSTEM AND CHANNEL MODELS

A mixed FSO/RF wireless scenario is considered in which the source (S) transmits its private data to the legitimate destination node (D) through a trusted relay (R). During transmission, two unauthorized receivers (E1 and E2) are trying to decode the data using a photo detector at the relay and a RF antenna at the destination respectively. In this model, the FSO Link-1 (i.e. S–R) and FSO Link-2 (i.e. S–E1) are assumed to follow Málaga ($\mathcal{M}$) distribution. The relay is connected to the destination through a RF link that is modelled by Nakagami-m distribution. The channel between relay and eavesdropper (E2) is also assumed to follow the Nakagami-m distribution. A decode and forward (DF) based relay is considered that decodes the incoming signal and retransmits to the destination. The relay has a photo detector to receive the optical signal from the source and has a RF antenna to retransmit the RF signal to the destination.

The probability density function (PDF) and the cumulative distribution function (CDF) of the instantaneous SNR ($\gamma_{Sk}: k \in \{R, E_1\}$) for Málaga fading channels are expressed as [15]

$$F_{\gamma_{Sk}}(\gamma) = \frac{A\xi^2}{2r-\gamma} \sum_{m=1}^{\beta} b_m G_{1,0}^3 \left[ B \left( \frac{\gamma}{\mu_r}, \frac{\xi^2 + 1}{\alpha, m} \right) \right],$$

$$F_{\gamma_{Sk}}(\gamma) = \frac{A\xi^2}{2r} \frac{\xi^2 + 1}{(2\pi)^r} \sum_{m_1=1}^{\beta} c_m G_{1,3r+1,3r+1} \left[ E \left( \frac{\gamma}{\mu_r}, \frac{1, K_1}{K_2, 0} \right) \right].$$

where $r = 1$ and $r$ represents the average SNR for heterodyne (HD) and intensity modulation with direct detection (IM/DD) techniques respectively with

$\mu_1 = \gamma_{Sk}$ and $\mu_2 = \frac{\xi(1+\xi^2)\xi^2(2\xi^2+\gamma+\Omega^2)}{\alpha r(1+\xi^2)\xi^2(\gamma+\Omega^2)\xi^2(1+\xi^2)}.$

A $= \frac{2a_2}{g(\xi^2+r)^2} \left[ \frac{\xi^2(\gamma+\Omega^2)^{\beta+2}}{(\xi^2+1)^{(\gamma+\Omega^2)}} \right]^2$, $B = \frac{\xi^2a_2(\gamma+\Omega^2)^{\beta+2}}{(\xi^2+1)^{(\gamma+\Omega^2)}}$,

$$b_m = a_m \left[ \frac{\xi^2(\gamma+\Omega^2)^{\beta+2}}{(\xi^2+1)^{(\gamma+\Omega^2)}} \right], c_m = b_m \alpha m r^{\alpha m}, a_m = \left( \frac{\beta - 1}{m - 1} \right) \left( \frac{\xi(\gamma+\Omega^2)^{\beta+2}}{(\xi^2+1)(\xi^2+1)} \right), E = \frac{b_m}{\alpha r^2}.$$

The parameter $\alpha$ is a positive number related to effective number of large scale cells of the scattering process, and $\beta$ shows the fading severity of the channel. From [15], $\gamma = 2b_0 (1-\rho)$, denotes the average power of the scattering component received by off-axis eddies, $2b_0$ is the average power of the total scattering components. The parameter $\rho$ denotes amount of scattering power coupled to the line-of-sight (LOS) component with $0 \leq \rho \leq 1$, $\Omega = \Omega+2b_0\rho+2\sqrt{2b_0\rho}c_{G,sk}$ represents the average power from coherent contributions, $\Omega$ is the average power of the LOS component, and $\phi_A$ and $\phi_{B}$ are the deterministic phases of the LOS and the coupled-to-LOS scatter items, respectively [15]. Parameter $r$ represents the scheme of detection at the photo receiver. $\xi$ is the measure of pointing deflection between transmitter and receiver. $\gamma_{Sk}$ and $\gamma_{RD}$ are the electrical and average SNRs for the respective links.

For a DF based relaying network, the end-to-end SNR can be written as $F_{\gamma_{eq}} = \min \{F_{\gamma_{SR}}, F_{\gamma_{RD}}\}$ [17]. From [17], the CDF for $F_{\gamma_{eq}}$ is obtained as

$$F_{\gamma_{eq}}(\gamma) = 1 - P_{T}\left[ F_{\gamma_{SR}}(\gamma) > \gamma \right] P_{T}\left[ F_{\gamma_{RD}}(\gamma) > \gamma \right].$$

Using Eq.(1) and Eq.(3) in Eq.(4) and utilizing [18, Eq. (07.34.21.0085.01)], the expression for end-to-end (S-R-D) CDF is obtained as

$$F_{\gamma_{eq}}(\gamma) = 1 - \frac{A\xi^2}{(2\pi)^r} \exp \left( -\frac{m \gamma_{RD}}{\pi_{RD}} \right) \sum_{k=0}^{m_{RD}} \sum_{m=1}^{\beta} \frac{b_m}{r^m(1+\alpha-m)} \left[ \frac{m_{RD} - 1}{K_1} \right] \left[ \frac{m_{RD} \gamma_{RD}}{K_2} \right]^{k}.$$
capacity \( (C_s) \) falls below a target secrecy rate \([4]\) and it can be expressed as
\[
P_{\text{out}} (r_s) = Pr \{ C_s (\gamma_{eq}, \gamma_{SE}) \leq R_s \},
\]
where \( R_s \) is the target secrecy rate. Referring to \([4]\), the lower bound for the SOP is derived as
\[
SOP_L = \int_0^\infty F_{\gamma_{eq}} (\Theta \gamma) \, d\gamma.
\]
(8)

The expression of secrecy outage probability for FSO/RF system can be expressed as given in \([9]\), where \( \Theta = e^{R_s} \), \( v_1 = \frac{b^r}{B^r} \), \( v_2 = \frac{b^s}{B^s} \), and \( [Q]_i \) = \( Q, Q, \ldots, Q \), comprising \( i \) terms. \( H_{m_1, m_2, n_1, n_2, m_3, n_3} \) is the H-function of two variables, which can be efficiently implemented in MATLAB \([19]\).

**Proof:** See appendix A.

The SOP in Eq. (9) reduces to the SOP for Gamma-Gamma-Rayleigh (for \( m = 1 \)) special case as
\[
SOP_{L_i} = 1 - \frac{\gamma}{\gamma} H_{1,0;3r+1,0;3,0} \frac{m_{rd}}{\gamma} \frac{m_{rd}}{\gamma} \sum_{k=0}^{\infty} \sum_{m_1=1}^{\infty} \sum_{m_2=1}^{\infty} \frac{\beta_1}{\beta_2} \left( \frac{\xi^2}{2r} \right)^{k'} \left( \frac{\xi^2}{2r} \right)^{k'} \left( 1, 1 \right) \left( 1, 1 \right) \left( 1, 1 \right) \left( \xi^2, r, \alpha, r, \beta, r \right).
\]
(9)

where \( K_{i,j} \) denotes the \( j \)th term of \( K \), and \( i \in \{ 3, 4 \} \) with \( K_3 = \left[ 1 - \Delta (r, \xi^2), 1 - \Delta (r, \xi^2) \right] \) and \( K_4 = \left[ \Delta (r, \xi^2), \Delta (r, \alpha), \Delta (r, \beta) \right] \).

**B. Strictly positive secrecy capacity analysis (SPSC)**

SPSC shows the probability of existence of secrecy capacity. It can be formulated as follows \([2]\)
\[
SPSC_1 = Pr \{ C_s (\gamma_{eq}, \gamma_{SE}) > 0 \}
\]
\[
= 1 - SOP_{L_i} |_{R_S = 0}.
\]
(13)

Upon substituting \( R_S = 0 \) in (9) and then substituting in (13), the SPSC can be expressed as Eq. (14), where \( v_2 = \frac{b^r}{B^r} \).

The SPSC in Eq. (14) can be approximated at high SNR as
\[
SPSC_1 \approx 1 - SOP_{L_i} |_{R_S = 0}.
\]
(15)

Correspondingly, the asymptotic expansion for SPSC is obtained as given in Eq. (16).

**IV. EAVESDROPPING ATTACK ON BOTH FSO AND RF LINKS SIMULTANEOUSLY**

**A. Secrecy Outage Probability (SOP)**

For a DF based FSO/RF system, the instantaneous secrecy capacity can be obtained as
\[
C_{\text{Inst}} = \min \{ C_{SR}, C_{RD} \} < R_s.
\]
(17)

where, \( C_{SR} \) and \( C_{RD} \) are the instantaneous secrecy capacities of SR and RD links respectively. Now the SOP in the presence of two independent eavesdroppers can be computed as
\[
SOP_2 = Pr \{ \min \{ C_{SR}, C_{RD} \} < R_s \}
\]
\[
= 1 - Pr \{ C_{SR} < R_s \} Pr \{ C_{RD} < R_s \}.
\]
(18)

Further this can be reformulated as
\[
SOP_2 = 1 - \left( 1 - \int_0^\infty F_{SR} (\Theta \gamma_{SE} + \Theta - 1) d\gamma_{SE} \right)
\]
\[
\times \left( 1 - \int_0^\infty F_{RD} (\Theta \gamma_{RE} + \Theta - 1) d\gamma_{RE} \right).
\]
(19)

As deriving the closed form of this SOP is very difficult, therefore we can derive the lower bound as follows
\[
SOP_{L_2} \approx I_1 \times I_2
\]
(20)
\[ SPSC_1 = \frac{(m_{RD} - 1)}{\Gamma(m_{RD})} \left( \frac{\xi^2 A}{2^r} \right)^2 \frac{1}{(2r - 1)} \sum_{k'=0}^{(m_{RD} - 1)} \left( \frac{m_{RD} \theta}{\gamma} \right)^{k'} \frac{1}{k'} \sum_{m_1=1}^{\beta_1} \sum_{m_2=1}^{\beta_2} x^{\alpha+m_1} b_m x_{\gamma} b_{m_2} H_{1,0}^{0.3} r_{1+3} + 1.3, 3.0 \left[ u_1, u_2 \right] \begin{pmatrix} 1; 1, 2 \end{pmatrix} \begin{pmatrix} K_1, [1]_{K_1} \end{pmatrix}, (1, 1) \begin{pmatrix} K_2, [1]_{K_2} \end{pmatrix}, (0, 1) \begin{pmatrix} \xi^2 + 1, r \end{pmatrix} \right]. \] (14)

\[ SPSC_1^\infty \approx \frac{\beta_1}{\gamma} \sum_{m_1=1}^{\beta_1} \sum_{m_2=1}^{\beta_2} \left( \frac{\xi^2 A}{2^r (2r - 1)} \right)^2 r^{\alpha+m_1+m_2-1} c_m b_{m_2} \times \sum_{k=1}^{3r} \left( \frac{\gamma}{\gamma_{SE}} \right) K_{3,k}^{-1} \prod_{l=1}^{3r+1} \Gamma (K_{3, l} - K_{3,k}) \prod_{l=3r+1}^{3r+1} \Gamma (1 + K_{3, l} - K_{3,k}) \right) \] (16)

\[ SOP_L^2 = \left[ 1 - \left( 1 - \left( \frac{A \xi^2}{2^r (2r - 1)} \right)^2 \right) \frac{\gamma^3}{\gamma_{SE}} \right] \frac{\gamma^3}{\gamma_{SE}} \left[ \frac{\gamma_{SR}}{\gamma_{SE}} \right] \left[ \frac{1 - K_2, 1, K_1}{K_2, 0, 1 - K_1} \right] \times A \] (23)

\[ SOP_L^\infty \approx 1 - \left\{ \left( 1 - \frac{3r}{\gamma_{SE, \gamma}} \right) K_{3,k}^{-1} \prod_{l=1}^{3r+1} \Gamma (K_{3, l} - K_{3,k}) \prod_{l=3r+1}^{3r+1} \Gamma (1 + K_{3, l} - K_{3,k}) \right\} A \] (24)

with

\[ I_1 = 1 - \left( 1 - \frac{r}{\gamma_{SE, \gamma}} F_{SR}(\gamma_{SE, \gamma}) f_{SE_1}(\gamma_{SE, \gamma}) d\gamma_{SE_1} \right) \] (21)

and

\[ I_2 = \left( 1 - \frac{r}{\gamma_{RD, \gamma}} F_{RD}(\gamma_{RD, \gamma}) f_{RE_2}(\gamma_{RD, \gamma}) d\gamma_{RE_2} \right) \] (22)

Using 1 and 2 in (21) and 3 and 4 in (22) and thereafter utilizing (12), the closed form expression for \( SOP_L \) is obtained as (23), where

\[ A = \sum_{k=1}^{m-1} \frac{1}{k!} \left( \frac{m \theta}{\gamma_{RD}} \right)^{k} \frac{m}{\gamma_{RE_2}} \frac{1}{m} \frac{\Gamma (m + k)}{\Gamma (m) \left( \frac{m \theta}{\gamma_{RD}} + \frac{m}{\gamma_{RE_2}} \right)^{m+k}} \]

and

\[ \omega = \left( \frac{\xi^2 A}{2^r (2r - 1)} \right)^2 \sum_{m_1=1}^{\beta_1} b_m x_{\gamma} x + m_1 - 1 \sum_{m_2=1}^{\beta_2} b_m x_{\gamma} x + m_2 - 1 \]

Proof: See appendix B.

Moreover using [15, Eq. (41)], the \( SOP_L \) can be expressed asymptotically at high SNR, as (24), with \( K_{i,j} \) denotes the \( j \)th term of \( K_i \) and \( i \in \{3, 4\} \) with \( K_3 = [1 - \Delta (r, \xi^2), 1 - \Delta (r, \alpha), 1 - \Delta (r, m_1), 1, \Delta (r, 1 + \xi^2)] \) and \( K_4 = [\Delta (r, \xi^2), \Delta (r, \alpha), \Delta (r, m_2), 0, 1 - \Delta (r, 2 - \xi^2)] \).

V. STRICTLY POSITIVE SECRECY CAPACITY ANALYSIS

SPSC shows the probability of existence of secrecy capacity. It can be formulated as follows (2)

\[ SPSC_2 = Pr \{ C_s (\gamma_{eq}, \gamma_{SE}) > 0 \} \]

\[ = 1 - SOP_L^2 | R_S = 0. \] (25)

Using (23) in (25), we obtain the SPSC as (26), where

\[ A' = \sum_{k=1}^{m-1} \frac{1}{k!} \left( \frac{m}{\gamma_{RD}} \right)^{k} \frac{m}{\gamma_{RE_2}} \frac{1}{m} \frac{\Gamma (m + k)}{\Gamma (m) \left( \frac{m}{\gamma_{RD}} + \frac{m}{\gamma_{RE_2}} \right)^{m+k}} \]

The SPSC in Eq. (26) can be obtained at high SNR as

\[ SPSC_2^\infty \approx 1 - SOP_L^\infty | R_S = 0. \] (27)

Thus using (24) in (27), we obtained the closed form expansion for SPSC at high SNR as (28).

VI. NUMERICAL RESULT

In this part, the analytical and asymptotic results are presented to analyze the secrecy performance metrics. Furthermore, we analyze the impact of pointing deflection, type of detection and, fading parameters of FSO and RF links on SOP and SPSC. In this analysis, the secrecy rate is set to 0.01 nats/sec/Hz and \( m_1 = m_2 = m \). The turbulence parameters are considered as \( \alpha = 2.296 \) and \( \beta = 2 \) for strong turbulence region and, for moderate turbulence region the values are \( \alpha = 4.2 \) and \( \beta = 3 \).

Fig. 2 shows the SOP versus \( \gamma_{RD} \) for different values of \( r, \xi, \alpha \) and \( \beta \). During analysis, the system is considered to be attacked by FSO based eavesdropping in the first hop. This figure reveals that the secrecy outage probability is improved with increasing in \( \gamma_{RD} \). It also concludes that the heterodyne detection scheme leads better secrecy performance than IM/DD scheme for different values of \( \xi \). Moreover, the high pointing accuracy (i.e. high value of \( \xi \)) leads to better secrecy performance. From turbulence severity point of view, larger value of \( \alpha \) and \( \beta \) leads to better performance (i.e. smaller SOP), since the severity of the atmospheric turbulence gets lower. Fig. 3 demonstrates the effect of turbulence severity and
Fig. 1. Secrecy outage probability versus average SNR with \( m_{\text{RD}} = 2 \).

Fig. 2. Secrecy outage probability versus average SNR for Gamma-Gamma special case with \( m_{\text{RD}} = 1 \) and \( \xi = 1.1 \).

Fig. 3. Strictly positive secrecy capacity versus average SNR with \( m_{\text{RD}} = 2 \).

Fig. 4. Strictly positive secrecy capacity versus average SNR for Gamma-Gamma special case with \( m_{\text{RD}} = 1 \) and \( \xi = 1.1 \).

V. III. CONCLUSION

In this work, the analysis is done for two different scenarios such as: primarily it is assumed that an eavesdropper is
After mathematical simplification, Eq. (A.1) can further be expanded as

\[
SOP_L = 1 - \frac{A\xi^{2}}{2^{r}(2\pi)^{r-1}} \sum_{m_1=1}^{\beta} b_{m_1} \frac{A\xi^{2} \beta}{2^{r}(2\pi)^{r-1}} \sum_{m_2=1}^{\beta} b_{m_2} \int_{0}^{\infty} \gamma^{1} \exp\left(-\frac{\Theta_{\gamma}}{\pi_{RD}} G^{3r+1.0}_{r+1.3r+1} \right) B^{r}\gamma \frac{K_{1}}{\pi^{2}r_{SR}} K_{2,0}^{} \left(1,1\right) \left(0,1\right) \gamma B^{r}\gamma \frac{K_{1}}{\pi^{2}r_{SR}} K_{2,0}^{} \left(1,1\right) \left(0,1\right) d\gamma \tag{A.2}
\]

By expressing \(exp(\cdot)\) and \(G^{m,p,q}_{m,n}{}[\cdot]\) functions in their corresponding H-function representations using the identity [17, Eq. (07.34.26.0008.01)], the integral in terms of Fox’s H-functions is obtained as

\[
SOP_L = 1 - \frac{A\xi^{2}}{2^{r}(2\pi)^{r-1}} \sum_{m_1=1}^{\beta} b_{m_1} \frac{A\xi^{2} \beta}{2^{r}(2\pi)^{r-1}} \sum_{m_2=1}^{\beta} b_{m_2} \int_{0}^{\infty} \gamma^{1} \exp\left(-\frac{\Theta_{\gamma}}{\pi_{RD}} G^{3r+1.0}_{r+1.3r+1} \right) B^{r}\gamma \frac{K_{1}}{\pi^{2}r_{SR}} K_{2,0}^{} \left(1,1\right) \left(0,1\right) \gamma B^{r}\gamma \frac{K_{1}}{\pi^{2}r_{SR}} K_{2,0}^{} \left(1,1\right) \left(0,1\right) d\gamma \tag{A.3}
\]

Now, using the formula [15, Eq. (2.3)], Eq. (A.3) can be expressed as Eq. (9).

\[
\text{APPENDIX B}
\]

\[
\text{DERIVATION OF } I_1 \text{ AND } I_2
\]

In this appendix, we derive \(I_1\) and \(I_2\) as follows:

\[
I_1 = 1 - \int_{0}^{\infty} F_{SR} \left(\Theta_{\gamma} \gamma_{E1}\right) I_{SE} \left(\gamma \gamma_{E1}\right) d\gamma_{E1} \tag{B.1}
\]

Herein we only solved the integral part of \(I_1\). Thus using [1] and [2] in the above integral, the obtained expression is written as

\[
I_1 = 1 - \omega \int_{0}^{\infty} G^{3r+1}_{r+1.3r+1} \left(\frac{E_{\gamma}}{\mu_{SR}}\right) \frac{K_{1}}{K_{2,0}^{} \left(1,1\right) \left(0,1\right)} \gamma B^{r}\gamma \frac{K_{1}}{\pi^{2}r_{SR}} K_{2,0}^{} \left(1,1\right) \left(0,1\right) d\gamma \tag{B.2}
\]

By utilizing [17, Eq.(07.34.21.0013.01)] in the above integral, we obtain the closed form solution for \(I_1\) as

\[
I_1 = 1 - \left(\frac{A\xi^{2}}{2^{r}(2\pi)^{r-1}} \frac{A\xi^{2} \beta}{2^{r}(2\pi)^{r-1}} \sum_{m_1=1}^{\beta} b_{m_1} \frac{A\xi^{2} \beta}{2^{r}(2\pi)^{r-1}} \sum_{m_2=1}^{\beta} b_{m_2} \int_{0}^{\infty} \gamma^{1} \exp\left(-\frac{\Theta_{\gamma}}{\pi_{RD}} G^{3r+1.0}_{r+1.3r+1} \right) B^{r}\gamma \frac{K_{1}}{\pi^{2}r_{SR}} K_{2,0}^{} \left(1,1\right) \left(0,1\right) \gamma B^{r}\gamma \frac{K_{1}}{\pi^{2}r_{SR}} K_{2,0}^{} \left(1,1\right) \left(0,1\right) d\gamma \tag{B.3}
\]

\[
\text{SIMILARLY, FOR } I_2 \text{ CAN BE FORMULATED AS}
\]

\[
I_2 = \left(1 - \int_{0}^{\infty} F_{RD} \left(\Theta_{\gamma} \gamma_{E2}\right) I_{RE} \left(\gamma \gamma_{E2}\right) d\gamma_{E2}\right) \tag{B.4}
\]

Utilizing [3] and [4], the integral part of the can be written as

\[
I_2 = 1 - \int_{0}^{\infty} \left\{1 - \sum_{k=0}^{m-1} \frac{1}{k!} \left(\frac{m_{\Theta_{\gamma}}}{\pi_{RD}}\right)^{k} \exp\left(-\frac{m_{\Theta_{\gamma}}}{\pi_{RD}}\right)\right\} \times \left(\frac{m_{\Theta_{\gamma}}}{\pi_{RE}}\right)^{m} \frac{m_{\gamma}^{m-1}}{\Gamma(m)} \exp\left(-\frac{m_{\gamma}}{\pi_{RE}}\right) d\gamma \tag{B.4}
\]
Thus utilizing \[ \int_0^\infty x^{\alpha-1} \exp(-\mu x) \, dx = \frac{\Gamma(\alpha)}{\mu^\alpha} \] in the above expression, the solved closed for expression is obtained as

\[
I_2 = \sum_{k=1}^{m-1} \frac{1}{k!} \left( \frac{m\Theta}{\tau_{RD}} \right)^k \left( \frac{m}{\tau_{RE}} \right)^m \frac{1}{\Gamma(m)} \Gamma(m + k) \left( \frac{m\Theta}{\tau_{RD}} + \frac{m}{\tau_{RE}} \right)^{m+k}
\]

(B.5)

REFERENCES


