Secrecy performance analysis for the mixed RF/VLC cooperative relaying systems

Wenwu Xie1 | Jianwu Liao1 | Jinxia Yang1 | Peng Zhu1 | Liang Yang2

1 Department of Information Science and Engineering, Hunan Institute of Science and Technology, Yueyang, China
2 College of Computer Science and Electronic Engineering, Hunan University, Changsha, China

Correspondence
Liang Yang, College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China. Email: liangy@hnu.edu.cn

Funding information
National Natural Science Foundation of China, Grant/Award Number: 61671160; Outstanding Youth Project of Hunan Provincial Education Department, Grant/Award Numbers: 20B267, 20B269; Open Fund of IPOC(BUPT); Hunan Natural Science Foundation, Grant/Award Number: 2020JJ4341

Abstract
In this work, the authors consider the security performance for the mixed radio frequency link and visible-light link cooperative relaying system, where the relay has the energy collection ability and can extract the direct current part existing in the visible-light signal. Then, the relay uses the collected energy to demodulate the received visible-light signal and retransmit it through the radio frequency link. With this equipment, some analytical expressions of the average secrecy capacity and the secrecy outage probability are derived. Furthermore, the asymptotic expression is also derived to examine the influence of the various configuration parameters on the secrecy performance of the mixed relaying system. At last, some numerical and simulation results are given to verify the theoretical analysis.

1 | INTRODUCTION

Visible light communication (VLC) has recently received considerable attention as a promising technique in the 5G/6G wireless communication [1]. With the increasing demand for the wireless communication networks and limited spectrum resources, light emitting diodes (LEDs) are used as sources, and an optical signal operated in a visible light band with a large bandwidth is used as a carrier of information source to realize the information transmission. VLC has both lighting and communication functions, and achieves an effective, green, and promising technology to realize the last mile of wireless communication. VLC has been widely used in short-distance, small-scale, and indoor wireless communication. Due to the above mentioned characteristics of VLC, the scope of VLC application is limited [2, 3]. Fortunately, the wireless relay can solve these problems well. Meanwhile, the VLC-based relaying system can obtain larger link capacity and better coverage.

Recently, the researchers have considerable interest in physical layer security (PLS). The concept of PLS was initially discussed by Wyner in [4]. Later, some classical techniques are used to improve secrecy performance. In particular, the authors in [5–7] investigated PLS for the radio frequency (RF) cooperative diversity systems. Until now, research on PLS for traditional RF communication systems has been very mature. However, there are few research results on the PLS under the VLC scenarios. The authors in [8] investigated the PLS under the influence of multi-path in VLC, where eavesdroppers were assumed to be deployed randomly. Under multi-user scenario, the security sum-rate performance of the VLC systems equipped with multiple transmit antennas and single receive antenna was studied in [9]. More recently, a novel optical jamming aided secrecy enhancement policy was proposed in [10]. The author in [11] proposed a modified Monte Carlo ray tracing model to account for both the specular and the diffusive reflections. Two new VLC PLS techniques based on generalized space shift keying (GSSK) modulation with spatial constellation design (SCD) and
non-orthogonal multiple access (NOMA) cooperative relaying are introduced in [12].

As another optical communication technology, free-space optical (FSO) has also received considerable attention. The author in [13] present and analyse a transmission scheme for the hybrid FSO/RF communication system based on RIS. A multi-user mixed hybrid FSO and RF system is considered, which introduced potential low complexity diversity gain-based massive MIMO schemes [14]. FSO technology is suitable for secure and high-speed data transmission rates for long distances for a point-to-point communication method. while it is not suitable for inner space communication networks. Then, in our paper, we consider an indoor downlink mixed RF/VLC relaying communication system.

Energy harvesting (EH) can convert the weak energy, such as weak light energy and weak kinetic energy, into electric energy, which is supplied to the sensor nodes for wireless transmission. The scheme that the nodes with EH are used as the cooperative relays, which is a promising and effective solution in the cooperative relaying systems. So far, the RF communication with EH has been studied extensively in [15–18]. However, optical wireless communication with EH has not been studied well. The receiver can capture energy by using the direct current (DC) part of the visible-light signal [19]. The mixed RF/VLC communication system with EH was first proposed in [20], which can collect the DC component in the optical signal. Then, the collected energy is used to demodulate the received signal and forward the remodulated signal at the relay. The authors in [21] designed a low-complexity and effective EH scheme, and proposed a self-reverse–biased solar panel optical receiver in the VLC system with EH.

To the best of our knowledge, we found that a few researchers studied the PLS for the mixed VLC/RF communication systems. The tradeoff between the secrecy capacity (SC) and the harvested energy (HE) is investigated in VLC system, which receiver is employed to coordinate the information decoding and the EH using simultaneous wireless information and power transfer in [22]. A cooperative hybrid VLC/RF system with spatially random terminals is considered in [23]. But it does not take into account energy harvesting technology. The authors in [24] considered PLS for the mixed VLC/RF communication systems. However, they assumed that eavesdropper only exists in the RF link and the PLS for the VLC link was not considered. But, the security problem in VLC systems is still a risk due to the broadcast characteristics. Motivated by the above background, we consider the PLS for the mixed RF/VLC relaying systems where eavesdropping happens in both VLC and RF links. Furthermore, we assume that the direct links from the source to the legitimate user and the eavesdropper are not blocked, which is different from the assumption in [24]. Based on this model, the major contributions of our work are summarized as follows: (1) We consider the PLS for the mixed RF/VLC relaying systems where eavesdropping happens in both VLC and RF links. Furthermore, we assume that the direct links from the source to the legitimate user and the eavesdropper are not blocked. (2) The relay can capture energy by using the DC part of the visible-light signal, which is a novel energy harvesting policy in optical communication. (3) Some analytical expressions for the security outage probability (SOP) and average security capacity (ASC) are derived, and also the corresponding asymptotic analysis is presented. Finally, our analysis expressions are verified by the numerical results and simulations.

The article is organized as follows. In Section 2, we discuss the proposed VLC-RF system model and give the modelling of the VLC link modelling of RF link. In section 3, we evaluate the security performance, such as ASC and SOP of the mixed RF/VLC cooperative relaying system. Moreover, the asymptotic analysis is provided. In section 4, the derived expressions of SOP and ASC are verified by Monte Carlo simulation, and a simple analysis on how the parameters influence the performance is given. Finally the conclusion part is given in Section 5.

2 | SYSTEM AND CHANNEL MODELS

Consider an indoor downlink mixed RF/VLC relaying communication system, which contains an LED transmitter (S), a legitimate user (D), a relay (R), and a passive eavesdropper (E). All receivers are equipped with photo-detectors (PD), which can convert the optical signal into an electrical signal. S transmits visible-light signals to R and D through VLC links, the DC bias is added to the optical signal to ensure the optical intensity must satisfy the non-negativity constraint. Meanwhile, E also can receive optical signals owing to the broadcast characteristics of the wireless communication system. Then, R uses the collected DC bias from the received optical signal and applies the decode-and-forward (DF) scheme to transmit the signal to D. Simultaneously, E tries to eavesdrop the signal from R. We assume R-D channel experiences independent and distributed identically Rayleigh fading, as well as R-E. The system model for this mixed RF/VLC system is shown in Figure 1.

2.1 Modelling of the VLC link

During the \( T_1 \) time slot, the S transmits visible-light signals \( X(t) = N P_{LED} [D_c + x(t)] \) to R and D through VLC links, where \( N \) represents the quantity of LED in the transmitter terminal, \( P_{LED} \) is the rated luminous power of a single standard LED lamp, \( D_c \) is the DC offset used to ensure that the generated optical signal is positive, and \( x(t) \) is the electric modulation signal. Similarly, E also can receive optical signals from S due to the broadcast characteristics of wireless communication.
Then, R receives the visible-light signal from S and transforms it into electric signal, which can be expressed as

\[ i_r(t) = \eta \cdot H_{SR} \cdot S(t) + n(t) = I_{DC} + i(t) + w(t), \]

where \( i(t) \) represents an AC signal, \( H_{SR} \) represents the channel impulse response (CIR) of the VLC link, \( \eta \) is the PD conversion rate, and \( n(t) \) denotes the thermal noise and/or the background noise modelled as the additive white gaussian noise (AWGN). From [1], the line-of-sight (LOS) propagation link \( H \) is given by

\[ H = \frac{(m+1)A_{PD}}{2\pi d_i^2} \cos^m(\varphi_i) \cos(\theta_i) (i \in SR, SE, SD), \]

where \( A_{PD} \) represents the physical area of the photoelectric converter, \( m = -\ln \left( \frac{2}{\ln \left( \frac{\cos(\varphi_i/2)}{1/2} \right)} \right) \) is the Lambert exponent corresponding to the half-angle, \( d_i \) is the distance from the source S to the relay R, E, or D. \( \varphi \) represents the incidence angle, and \( \varphi \) is the irradiance angle.

The instantaneous signal-noise ratio (SNR) expressions for the VLC links are given by [1]

\[ \gamma_i = \frac{(\eta H_i N P_{LED} A)^2}{\sigma_i^2}, i \in (SR, SE, SD), \]

where \( A \) denotes the crest value of \( x(t) \), and \( \sigma_i^2 \) denotes the power spectrum density (PSD) of \( n(t) \). For notation simplicity, assuming that \( \sigma_{SR}^2 = \sigma_{SE}^2 = \sigma_{SD}^2 = \sigma^2 \), namely,

\[ \sigma^2 = qI W, \]

where \( I \) represents the faradic current of PD, \( W \) denotes effective noise bandwidth, and \( q = 1.6 \times 10^{-19} \) is the electronic charge. \( A \) can be defined as follows [20]

\[ A = \begin{cases} B - I_L, & B < \frac{I_{HI} + I_L}{2} \\ I_{HI} - B, & B \geq \frac{I_{HI} + I_L}{2} \end{cases}, \]

where \( I_L \) represents the minimal input-offset current and \( I_{HI} \) is the maximal input-offset current.

The DC component, which is added for producing the positive signal, can be extracted at the PD from the visible-light signal. Then, the maximum collected energy at R can be expressed as [20]

\[ E_{R} = 0.75 I_{DC} V_{OC} \left( T_1 + T_2 \right), \]

where \( T_1 \) and \( T_2 \) represent the duration of the first and the second time slot, respectively. \( V_{OC} \) denotes the open-circuit voltage of PD [24],

\[ V_{OC} = V_t \ln \left( \frac{I_{DC}}{I_0} + 1 \right), \]

where \( V_t \approx 25 \text{ mV} \) denotes the thermal voltage, and \( I_0 \) is the dark-saturation current of PD.

### 2.2 Modelling of RF link

During the \( T_2 \) period, R uses the HE to send the data to D and E through the RF links. Here two assumptions are given as follows: (1) at R, the energy for receiving and transmitting data is little compared with the HE; (2) the RF channels undergo independently identically distribution (IID) complex AWGN with \( N(0, 1) \). Then, the SNR expressions of the RF links are given by [1],

\[ \gamma_i = \frac{|b_i|^2 E h_i}{T_2 G_i \sigma_i^2}, i \in (RE, RD), \]

where \( b_i \) is CIR of the RF links, R-D or R-E, \( \sigma_i^2 \) denotes the noise variance, and \( G_i \) represents the path loss given by

\[ G_i = \left( \frac{4\pi d_i}{\lambda} \right)^2 \left( \frac{d_i}{d_0} \right)^{\chi} i \in (RD, RE), \]

where \( d_0 = 1 \) is the reference range, \( \lambda \) is the wavelength, \( d_i \) is the range from the relay R to the eavesdropper E or the legitimate user D, and \( \chi \) indicates the path loss coefficient. If \( b_i \) undergoes the rayleigh fading, the probability density function (PDF) of \( \gamma_i \) can be obtained as [3],

\[ f_{\gamma_i}(\gamma) = \frac{1}{\bar{\gamma}_i} e^{-\gamma / \bar{\gamma}_i}, i \in (RD, RE), \]

where \( \bar{\gamma}_i = E_{\gamma_i} / (T_2 G_i \sigma_i^2) \) represents the average SNR.

The received optical signals at D and E are converted to electrical signal through PD. Then, we apply the maximal ratio combining (MRC) scheme at the legitimate user and eavesdropper to merge the signals from S and R [22]. Therefore, the final SNRs of the legitimate user and eavesdropper are given by,

\[ \gamma_D = \min(\gamma_{SR}, \gamma_{RD}) + \gamma_{SD}, \]

\[ \gamma_E = \min(\gamma_{SR}, \gamma_{RE}) + \gamma_{SE}. \]

### 3 SECURITY PERFORMANCE ANALYSIS

In this part, we evaluate the security performance, such as ASC and SOP, of the mixed RF/VLC cooperative relaying system. Moreover, the asymptotic analysis is provided.

#### 3.1 Secrecy outage probability

##### 3.1.1 Exact SOP derivation

When the instantaneous secrecy link capacity cannot achieve the predefined target capacity \( C_{\text{th}} \), a secrecy incident occurs. Then,
the secrecy performance SOP definition is formulated as [4]
\[
SOP = \Pr\{\ln\left(\frac{1 + \gamma_{RE}}{1 + \gamma_{SE}}\right) - \frac{\ln(1 + \gamma_{SD}) - \gamma_{DR}}{\gamma_{SD}} < C_{th}\}
\]
where \( C_{th} \) is the minimum target threshold of security confidentiality capacity, and \( \theta = \ell_0 \geq 1 \). In (13), \( r_{SR} > 0 \), \( I_j (j = 1, 2, 3, 4) \) are
\[
I_1 = \Pr\{1 + \gamma_{SR} + \gamma_{SD} < \frac{\theta}{1 + \gamma_{SR} + \gamma_{SE}}, \\
\gamma_{SR} < \gamma_{DR}, \gamma_{SR} < \gamma_{RE}\},
\]
\[
I_2 = \Pr\{1 + \gamma_{SR} + \gamma_{SD} < \frac{\theta}{1 + \gamma_{SR} + \gamma_{SE}}, \\
\gamma_{SR} < \gamma_{DR}, \gamma_{SR} > \gamma_{RE}\},
\]
\[
I_3 = \Pr\{1 + \gamma_{SR} + \gamma_{SD} < \frac{\theta}{1 + \gamma_{SR} + \gamma_{SE}}, \\
\gamma_{SR} > \gamma_{DR}, \gamma_{SR} > \gamma_{RE}\},
\]
\[
I_4 = \Pr\{1 + \gamma_{SR} + \gamma_{SD} < \frac{\theta}{1 + \gamma_{SR} + \gamma_{SE}}, \\
\gamma_{SR} > \gamma_{DR}, \gamma_{SR} > \gamma_{RE}\}.
\]

Since \( r_{SR} > 0 \), \( I_j (j = 1, 2) \) can reduce to
\[
I_1 = \Pr\{1 + \gamma_{SR} + \gamma_{SD} < \frac{\theta}{1 + \gamma_{SR} + \gamma_{SE}}, \\
\gamma_{SR} < \gamma_{DR}, \gamma_{SR} < \gamma_{RE}\},
\]
\[
= \left\{\begin{array}{ll}
e^{-\frac{\gamma_{SR}+\gamma_{DR}+\theta}{\gamma_{RE}}} & , \quad p_1 \\
0 & , \quad p_2
\end{array}\right.
\]

where \( p_1 = 1 + \gamma_{SR} + \gamma_{SD} < \frac{\theta}{1 + \gamma_{SR} + \gamma_{SE}} \) and \( p_2 = 1 + \gamma_{SR} + \gamma_{SD} \geq \frac{\theta}{1 + \gamma_{SR} + \gamma_{SE}} \), and
\[
I_2 = \Pr\{1 + \gamma_{SR} + \gamma_{SD} < \frac{\theta}{1 + \gamma_{SR} + \gamma_{SE}}, \\
\gamma_{SR} < \gamma_{DR}, \gamma_{SR} > \gamma_{RE}\},
\]
\[
= e^{-\frac{\gamma_{SR}+\gamma_{DR}+\theta}{\gamma_{RE}}} - e^{-\frac{\gamma_{SR}}{\gamma_{RE}}}, \quad p_1
\]

Similar to formula (18), we can obtain
\[
I_3 = \Pr\{\gamma_{RD} < \min\left(\frac{\theta}{1 + \gamma_{SR} + \gamma_{SE}} - \gamma_{SD}, 1\right), \\
\gamma_{SR}, \gamma_{SR} < \gamma_{RE}\},
\]
\[
= \left\{\begin{array}{ll}
e^{-\frac{\gamma_{SR}}{\gamma_{RE}}} & , \quad p_1 \\
\left(1 - e^{-\frac{\gamma_{SR}}{\gamma_{RE}}\gamma_{RD}}\right) & , \quad p_2
\end{array}\right.
\]

Finally, \( I_4 \) can be rewritten as
\[
I_4 = \Pr\{\gamma_{RD} < \min\left(\frac{\theta}{1 + \gamma_{SR} + \gamma_{SE}} - \gamma_{SD}, 1\right), \\
\gamma_{SR}, \gamma_{SR} > \gamma_{RE}\},
\]
\[
= \Pr\{\gamma_{RD} < \min\left(\frac{\theta}{1 + \gamma_{SR} + \gamma_{SE}} - \gamma_{SD}, 1\right), \\
\gamma_{SR}, \gamma_{SR} > \gamma_{RE}\},
\]
where \( \min\left(\frac{\theta}{1 + \gamma_{SR} + \gamma_{SE}} - \gamma_{SD}, 1\right) \) can be expressed as
\[
= \left\{\begin{array}{ll}
e^{-\frac{\gamma_{SR}+\gamma_{DR}+\theta}{\gamma_{RE}}} & , \quad p_1 \\
e^{-\frac{\gamma_{SR}+\gamma_{DR}+\theta}{\gamma_{RE}}} - e^{-\frac{\gamma_{SR}}{\gamma_{RE}}\gamma_{RD}} & , \quad p_2
\end{array}\right.
\]

Finally, substituting \( I_1, I_2, I_3, \) and \( I_4 \) into (13) yields the final secrecy outage probability expression.

### 3.1.2 Asymptotic SOP analysis

To obtain explicit analytical results, we consider the asymptotic analysis and assume that \( \gamma_{RD} \) tends to infinity and \( \gamma_{RE} \) is fixed, which corresponds to the scenario where the legitimate user is very close to the relay, while the eavesdropper is far away from R. Assuming that \( \gamma_{RE} \) is a constant and \( \gamma_{RD} \) tends infinity, the asymptotic SOP expression can be expressed as
\[
SOP \rightarrow \left\{\begin{array}{ll}
e^{-\frac{\gamma_{SR}+\gamma_{DR}}{\gamma_{RE}}} & , \quad p_1 \\
e^{-\frac{\gamma_{SR}+\gamma_{DR}}{\gamma_{RE}}} - e^{-\frac{\gamma_{SR}}{\gamma_{RE}\gamma_{RD}}} & , \quad p_2
\end{array}\right.
\]
From (24), it shows that the asymptotic SOP expression is not related to \( \bar{\gamma}_{RD} \). If \( \gamma_{SR} \) and \( \gamma_{SD} \) increase, SOP can be reduced. While decreasing \( \gamma_{RE} \) and \( \gamma_{SE} \), SOP increases. Furthermore, \( \gamma_{SR} \) and \( \gamma_{SE} \) are related to the VLC link parameters \( N \) and \( P_{LED} \). By increasing the number of LED lamp arrays or using a higher power LED lamp, the relay can obtain higher energy collection, which enhances the SOP performance.

### 3.2 Average secrecy capacity

#### 3.2.1 Exact ASC derivation

The ASC is also one of the important indicators for evaluating secrecy performance. ASC is the average security rate defined as [9],

\[
\bar{C}_i = \int_0^\infty \frac{F_{\bar{\gamma}}(\gamma)}{1+\gamma} \{1 - F_{\gamma_0}(\gamma)\}d\gamma.
\]

(25)

The cumulative distribution function (CDF) \( F_{\bar{\gamma}} \) of \( \gamma_E \) is

\[
F_{\bar{\gamma}}(\gamma) = \Pr(\gamma_{RE} + \gamma_{SE} < \gamma) = \begin{cases} \Pr(\gamma_{RE} + \gamma_{SE} < \gamma), & \gamma < \gamma_{SR} + \gamma_{SE} \\ 1, & \gamma > \gamma_{SR} + \gamma_{SE}. \end{cases}
\]

(26)

Since \( \Pr(\gamma_{RE} + \gamma_{SE} < \gamma) = \int_0^\gamma f_{\gamma_{RE}}(\gamma_{RE}) d\gamma_{RE} \), we have

\[
F_{\bar{\gamma}}(\gamma) = \begin{cases} 1 - e^{-\gamma_{SR}} \frac{e^\gamma - 1}{\bar{\gamma}_{RD}}, & \gamma < \gamma_{SR} + \gamma_{SE} \\ 1, & \gamma > \gamma_{SR} + \gamma_{SE}. \end{cases}
\]

(27)

Like \( \gamma_E \), the CDF of \( \gamma_D \) can be given by

\[
F_{\gamma_D}(\gamma) = \begin{cases} 1 - e^{-\gamma_{SD}} \frac{e^\gamma - 1}{\bar{\gamma}_{RD}}, & \gamma < \gamma_{SR} + \gamma_{SD} \\ 1, & \gamma > \gamma_{SR} + \gamma_{SD}. \end{cases}
\]

(28)

Substituting (27), (28), into (25) and using integral formula [[25], eq. (3.352.1)], we have

\[
\bar{C}_i = \int_0^\infty \frac{F_{\bar{\gamma}}(\gamma)}{1+\gamma} \{1 - F_{\gamma_0}(\gamma)\}d\gamma
\]

\[
= \frac{\gamma_{SD}+1}{\bar{\gamma}_{RD}} \left\{ E\left(-\frac{\gamma_{SR}+\gamma_{SE}+1}{\bar{\gamma}_{RD}}\right) - E\left(-\frac{1}{\bar{\gamma}_{RD}}\right) \right\} + \epsilon \frac{\gamma_{SR}+\gamma_{SE}}{\bar{\gamma}_{RD}} \left\{ E\left(-\frac{\gamma_{SR}+\gamma_{SE}}{\bar{\gamma}_{RD}}\right) - E\left(-\frac{\gamma_{SR}+\gamma_{SE}+1}{\bar{\gamma}_{RD}}\right) \right\}, \gamma_{SD} > \gamma_{SE}
\]

(29)

\[
+ \frac{\gamma_{SR}+\gamma_{SE}}{\bar{\gamma}_{RD}} \left\{ E\left(-\frac{\gamma_{SR}+\gamma_{SE}}{\bar{\gamma}_{RD}}\right) - E\left(-\frac{1}{\bar{\gamma}_{RD}}\right) \right\} + \epsilon \frac{\gamma_{SR}+\gamma_{SE}}{\bar{\gamma}_{RD}} \left\{ E\left(-\frac{\gamma_{SR}+\gamma_{SE}}{\bar{\gamma}_{RD}}\right) - E\left(-\frac{\gamma_{SR}+\gamma_{SE}+1}{\bar{\gamma}_{RD}}\right) \right\}, \gamma_{SD} < \gamma_{SE}
\]

where \( Ei(x) \) is the first-order exponential integral function defined as \( Ei(x) = \int_0^x \frac{e^t}{t} dt \).

#### 3.2.2 Asymptotic ASC derivation

Let \( \bar{\gamma}_{RE} \) and \( \bar{\gamma}_{RD} \) tend to infinity. Using Taylor expansion approximation \( Ei(x) = \int_0^x \frac{e^t}{t} dt \approx \ln(x) + \sum_{i=1}^{\infty} \frac{x^i}{i \cdot \ln(x)} \), the asymptotic ASC expression can be written as

\[
\bar{C}_i \approx \ln(\gamma_{SR} + 1 + \gamma_{SE}) - e^{\bar{\gamma}_{RD}} \left\{ E\left(-\frac{1}{\bar{\gamma}_{RE}}\right) \right\} + \epsilon \frac{\gamma_{SR}+\gamma_{SE}}{\bar{\gamma}_{RD}} \left\{ E\left(-\frac{\gamma_{SR}+\gamma_{SE}+1}{\bar{\gamma}_{RD}}\right) - E\left(-\frac{\gamma_{SR}+\gamma_{SE}}{\bar{\gamma}_{RD}}\right) \right\}, \gamma_{SD} > \gamma_{SE}
\]

\[
+ \epsilon \frac{\gamma_{SR}+\gamma_{SE}}{\bar{\gamma}_{RD}} \left\{ E\left(-\frac{\gamma_{SR}+\gamma_{SE}}{\bar{\gamma}_{RD}}\right) - E\left(-\frac{1}{\bar{\gamma}_{RD}}\right) \right\} + \epsilon \frac{\gamma_{SR}+\gamma_{SE}}{\bar{\gamma}_{RD}} \left\{ E\left(-\frac{\gamma_{SR}+\gamma_{SE}}{\bar{\gamma}_{RD}}\right) - E\left(-\frac{\gamma_{SR}+\gamma_{SE}+1}{\bar{\gamma}_{RD}}\right) \right\}, \gamma_{SD} < \gamma_{SE}
\]

(30)

From (30), it shows that the asymptotic ASC is only related to \( \bar{\gamma}_{RE} \) and \( \gamma_{SR} \). On increasing \( \gamma_{SR} \) or decreasing \( \gamma_{RE} \), the ASC performance can be improved.

### 4 NUMERICAL AND SIMULATION RESULTS

In this part, the derived expressions of SOP and ASC are verified by Monte Carlo simulation. The simulation parameter values are used as follows [20] and [24]: \( P_{LED} = 20 \text{ mW/A} \), \( N = 10, \delta_{1/2} = 15 \text{ deg}, \phi_1 = 20 \text{ deg}, \phi_2 = 20 \text{ deg}, d_1 = 1 \text{ m}, d_2 = 1 \text{ mA}, I_H = 16 \text{ mA}, I_T = 1 \text{ mW}, C_{th} = 0.02, q = 1.6 \times 10^{-19}, W = 1 \times 10^6 \text{ Hz}, I = 5.84 \text{ mA}, \eta = 0.4 \).

Figure 2 plots the SOP of the legitimate user versus SNR with the distance from the source to the relay. The semi-angler varies from 10 to 60. For this configuration, it is notable that the SOP in the VLC link can acquire the optimal SOP for the semi-angle value around 20. We choose the paper value for the parameters in the next simulation.

In Figure 3, we take the DC offset as the horizontal ordinate and draw the secrecy outage probability for various distance \( d_{SR} \). It shows that the theoretical analysis is fit well to the simulation results. Along with the DC offset increasing, we can observe that the SOP decreases. This is due to the fact that bigger DC can achieve a larger EH and guarantees more reliable service for legitimate user. In addition, it shows that increasing the distance \( d_{SR} \) leads to a higher SOP and the reason is that increasing the distance \( d_{SR} \) causes the EH becoming weak. Thus, overall secrecy performance is affected.

SOP versus the distance \( d_{SE} \) and \( d_{RD} \) for various values \( d_{SR} \) is plotted in Figure 4. We can observe that the simulation results are fit well to our analytical results. It can be observed that increasing the path of eavesdropper will improve the safety
performance, the reason is that far distance will reduce the quality of the eavesdropping signal. Furthermore, larger $d_{SR}$ results in worse SOP performance. This comes from the fact that long transmission distance causes a worse energy collection and in turn affects the system performance. This also shows from a deeper level that communication security is relative. It is a game process that depends on the channel status of eavesdropping users and legitimate users, and does not depend on one party.

In Figure 5 and 6, we use $\bar{\gamma}_{RD}$ as the horizontal ordinate to draw SOP and ASC for various $\gamma_{SR}$. Again, it shows that the theoretical analysis results are well close to the numerical simulations results. A bigger $\bar{\gamma}_{RD}$ value can make both the SOP and ASC performance better. Finally, the asymptotic ASC and SOP curves get tight while $\bar{\gamma}_{RD}$ increase. As expected, both ASC and SOP converge to a constant at high $\bar{\gamma}_{RD}$. In this latter case, $\bar{\gamma}_{RD}$ too high indicates that the distance of relay and users is
wirelessly close, both ASC and SOP are no longer affected by $\tilde{\gamma}_{RD}$, which is in agreement with our asymptotic analysis.

5 | CONCLUSION

Here, we considered the PLS for a mixed dual-hop VLC/RF system. More specifically, exact SOP and ASC analyses were provided. Also, asymptotic analysis was presented to obtain some explicit insights. Results showed that both SOP and ASC converge to constants for large $\tilde{\gamma}_{RD}$. In our model, PLS for both the VLC and RF links were considered. Moreover, this paper also assumes that the direct link between S and E and D exists. Therefore, our analytical results are more general.

ORCID
Jianwu Liao  https://orcid.org/0000-0002-1436-5970

REFERENCES

1. Ghassemlooy, Z., Popoola, W., Rajbhandari, S.: Optical Wireless Communications: System and Channel Modelling with MATLAB, 2nd ed, CRC Press, Boca Raton (2019)
2. Nuwanpriya, A., Ho, S., Chen, C. S.: Indoor MIMO visible light communications: novel angle diversity receivers for mobile users. IEEE J. Sel. Areas Commun. 33(9), 1780–1792 (2015)
3. Shao, S., Khreishah, A., Khalil, I.: Joint link scheduling and brightness control for greening VLC-based indoor access networks. IEEE J. Opt. Commun. Netw. 8(3), 148–161 (2016)
4. Wyner, A. D.: The wire tap channel. Bell Syst. Tech. J. 54, 1355–1387 (1975)
5. Dong, L., et al.: Improving physical layer security via cooperating relays. IEEE Trans. Signal Process. 58, 1875–1888 (2010)
6. Yang, N., et al.: Physical layer security of TAS/MRC with antenna correlation. IEEE Trans. Inf. Foren. Sec. 8(1), 254–259 (2013)
7. Chen, J., Yang, L., Alouini, M.: Physical layer security for cooperative NOMA systems. IEEE Trans. Veh. Technol. 67(5), 4645–4649 (2018)
8. Cho, S., et al.: Impact of multipath reflections on secrecy in VLC systems with randomly located eavesdroppers. In: IEEE Wireless Commun. Net. Conf. Barcelona, 1–6 (2018)
9. Pham, T.V., Pham, A.T.: On the secrecy sum-rate of MU-VLC broadcast systems with confidential messages. In: 2016 10th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), Prague, 1–6 (2016)
10. Wang, F., et al.: Enhancing the secrecy performance of the spatial modulation aided VLC systems with optical jamming. Signal Process. 157, 288–302 (2019)
11. Chen, J., Sha, T.: Statistical modeling and analysis on the confidentiality of indoor VLC systems. IEEE Trans. Wireless Commun. 19(7), 4744–4757 (2020)
12. Yesilkaya, A.: Physical layer security in visible light communications. 2020 2nd 6G Wireless Summit (6G SUMMIT), Levi, Finland, 1–5 (2020)
13. Yang, L., Guo, W., Ansari, I.S.: Mixed dual-hop FSO-RF communication systems through reconfigurable intelligent surface. IEEE Commun. Lett. 24(7), 1558–1562 (2020)
14. Al-Eryani, Y.F., et al.: Mixed dual-hop FSO-RF communication systems through reconfigurable intelligent surface. IEEE/OSA J. Opt. Commun. Netw. 10(4), 309–321 (2018)
15. Ruan, T., Chew, Z.J., Zhu, M.: Energy-aware approaches for energy harvesting powered wireless sensor nodes. IEEE Sensors. J. 17(7), 2165–2173 (2017)
16. Siddiqui, A.M., et al.: Performance analysis of relaying systems with fixed and energy harvesting batteries. IEEE Trans. Commun. 66(4), 1386–1398 (2018)
17. Siddiqui, A.M., Musavian, L., Ni, Q: Energy efficiency optimization with energy harvesting using harvest-use approach. IEEE Int Conf on Commun Workshop. London, 1982–1987 (2015)
18. Wang, D., et al.: Relay selection in full-duplex energy-harvesting two-way relay networks. IEEE Trans. Green Commun. Commn. Netw. 1(2), 182–191 (2017)
19. Sandalidis, H.G., et al.: Illumination, data transmission, and energy harvesting: The threefold advantage of VLC. Appl. Opt. 56, 3421–3427 (2017)
20. Rakia, T., et al.: Optimal design of dual-hop VLC/RF communication system with energy harvesting. IEEE Commu. Lett. 20(10), 1979–1982 (2016)
21. Shin, W.H., et al.: Self-reverse-biased solar panel optical receiver for simultaneous visible light communication and energy harvesting. Opt. Express. 24(22), A1300–A1305 (2016)
22. Wang, J., et al.: Tradeoff Between secrecy capacity and harvested energy for secure visible light communications with SWIPT. IEEE Access. 7, 29543–29552 (2019)
23. Pan, G., et al.: Secure Cooperative Hybrid VLC-RF Systems. IEEE Trans. on Wireless Commun. 19(11), 7697–7707 (2020)
24. Liao, Z., et al.: Physical layer security for dual-hop VLC/RF communication systems. IEEE Commun. Lett. 22(12), 2603–2606 (2018)
25. Gradshteyn, I.S., Ryzhik, I.M.: Table of Integrals, Series and Products, 7th ed. Academic Press, San Diego, CA (2007)

How to cite this article: Xie, W., et al.: Secrecy performance analysis for the mixed RF/VLC cooperative relaying systems. IET Commun. 1–7 (2021). https://doi.org/10.1049/cmu2.12234