Abstract
In this paper, the physical layer security of an indoor visible light communication system, that consists of two transmission light-emitting diodes to broadcast the information towards the legitimate user, is investigated. Further, a secure LED selection scheme is proposed to select an LED that can perform secure information broadcasting, in the presence of an active and/or passive eavesdropper. The probability of secure information broadcasting is obtained in terms of the positive secrecy rate which is defined under the constraints of known or unknown imperfect channel state information of both legitimate and eavesdropping links. The channel state information (CSI) knowledge of each transmitting link is estimated with the use of a minimum mean square error technique. The performance metrics of the system are defined in terms of the average secrecy capacity and secrecy outage probability parameters. Further, the performance of the system is compared with the conventional stand-alone VLC system by varying various physical parameters. Further, analytical results are corroborated with the computer simulation results.

1 INTRODUCTION

The visible light communication (VLC) is a light emitting diode (LED) based technology which, in addition to the illumination, can provide wireless access with almost zero power consumption [1]. In contrast to conventional radio frequency (RF) technology, VLC technology has several advantages such as low deployment cost [2], high-speed data transmission rate (spectrum range 370 nm-780 nm) [3] and a license-free technology [4]. However, there are few challenges in VLC technology which requires the researchers attention such as small coverage region [5], restricted user mobility [6] and vulnerability to eavesdropping attacks [7]. Mobility related issues in an indoor VLC network can be reduced by deploying multiple VLC access nodes which also helps in improving the transmission coverage distance [8]. However, due to the point-to-multipoint broadcast nature of VLC technology, the coverage region of a legitimate user can also be accessed with an eavesdropping user. Hence, secure information broadcasting by using a VLC technology is a critical issue.

1.1 Background and motivations

To provide the secure information broadcasting in wireless communication systems, the physical layer security (PLS) technique (i.e. first introduced by Shannon in the year 1949 [9]) is one of the most effective solutions which exploits the properties of the physical layer such as fading, noise, and interference. Further, the secure information broadcasting rate is measured by Wyner (who introduced wiretapper channel model in year 1975 [10]) in terms of positive secrecy rate with the assumption that the channel conditions of a legitimate link are stronger than the channel conditions of an eavesdropping link.

Later on, in order to improve the probability of a secure information broadcasting rate against the eavesdroppers, the wiretapper model is expanded for the slow-fading wireless channels in [11–14]. In these studies, the secure broadcasting is characterised for an asymptotically long coherence interval on the basis of the following two transmission strategies: i) in the beginning of each transmission interval, the source transmitter has complete channel state information (CSI) of both,
eavesdropping and legitimate links [11–13], and ii) in each coherence interval, the channel conditions of the legitimate-link are better than the channel conditions of an eavesdropping-link [14]. The PLS performance of VLC networks utilising the slow fading wireless channels has been investigated in [15–21] wherein it was verified that in contrast to the fast-fading channels, the use of slow fading channels for VLC technology is more efficient to enhance the security against eavesdropping attacks. Recently, in [22], the security performance of a dual-element VLC system adapting slow fading wireless channels was investigated using a secure link adaptation scheme.

In [11–22], the security performances were investigated with the consideration that the source transmitter has complete CSI knowledge of both eavesdropping as well as legitimate links. However, such an assumption might not be practical as the CSI availability of an eavesdropping link depends on whether an eavesdropper is an active user or a passive user. To receive the broadcasted information, an active eavesdropper (i.e. a legitimate user for another network) always shares it’s estimated CSI with the transmitter whereas a passive eavesdropper (i.e. a malicious user) does not share it’s estimated CSI [11]. Thus, CSI knowledge at transmitter is an uncertain factor and it might reduce the secure broadcasting rate as well. Recently, in [23], the PLS performance of an indoor heterogeneous VLC/RF system was investigated on basis of perfect known or unknown CSI of both eavesdropping and legitimate links. A secure link selection mechanism is proposed to select either VLC or RF technology which is efficient to provide communication security against an active/passive eavesdropper attacks. However, the VLC technology is preferred over RF technology with the consideration that VLC technology can provide the high transmission rate to an indoor user.

In a realistic scenario, the receiver (i.e. either an legitimate user or eavesdropper) cannot estimate the perfect CSI of a transmitting link due to the occurrence of Gaussian-distributed errors during channel estimation. Hence, the assumption that the perfect CSI is available at the transmitter might not be realistic as the receiver may not feedback perfect CSI to transmitter. Therefore, authors in [24] have optimised the secrecy rate of legitimate information broadcasting by considering that the transmitter has imperfect CSI of both legitimate as well as eavesdropping links. Therefore, the authors in [25–27] have investigated the physical layer security of the wireless networks with the assumption that the transmitter has imperfect CSI of both legitimate and eavesdropping links. In [25], a secure transmission scheme was designed to investigate the system performance by considering the Gaussian-distributed errors produced by the imperfect channel estimation at the legitimate user terminal. In [26], a secure on–off transmission scheme was explored to maximise the throughput under the constraints of secrecy outage probability. Further, in [27], a secure on–off secure transmission scheme was proposed on the basis of outdated CSI of the legitimate and eavesdropping links. In [28–30], author(s) have investigated the VLC systems wherein the receivers have estimated the channel with the use of minimum mean square error (MMSE) technique. To the best of our knowledge, the security performance of the VLC system by estimating imperfect CSI of both eavesdropping and legitimate links, has not been investigated. Hence, this as a consequence motivated us to analyse the security performance of a dual-LED VLC system on the basis of the unknown or known imperfect CSI of both eavesdropping and legitimate links.

1.2 Contributions

Unlike previous works on indoor VLC systems, which have investigated the security performance of the system on the basis of perfect knowledge CSI, this work investigates the security performance of the VLC system on the basis of estimated known or unknown imperfect CSI. In the proposed system model, the source transmitter is equipped with two transmitting LEDs. However, according to the CSI knowledge, the transmitter broadcasts the information with use of only one LED which has an ability to withstand the eavesdropping attacks. For the selection of transmitting LED, a novel scheme is proposed having two key advantages. First, it avoids the inter-channel interference occurrence, and in second, it provides the guaranteed secure information broadcasting, in presence of an active/passive eavesdropper. In particular, our primary contributions in this work are as follows:

- A secure-LED selection scheme for the selection of an LED that can broadcast the information with the highest security, in the presence of an eavesdropper node, is proposed. The proposed scheme works well against both active and passive eavesdropping attacks.
- The secrecy rate is formulated on the basis of imperfect known/unknown CSI of eavesdropping and legitimate links. The CSI knowledge of each transmitting link is estimated with the use of minimum mean square error (MMSE) technique.
- The closed-form cumulative distribution function (CDF) and probability density function (PDF) expressions for end-to-end SNR are derived for the stand-alone VLC system.
- The security performance of system is analysed in terms of closed-form average secrecy capacity (ASC) and secrecy outage probability (SOP). Moreover, the performance of the proposed dual-LED system is compared with that of the conventional stand-alone system for both known and unknown CSI scenarios.

The rest of this paper is organised as follows. In Section 2, we discuss the system model, channel estimation technique, CSI knowledge, and the formulation of secrecy-rate. In Section 3, the proposed secure-LED selection scheme is explained. In Section 4, the CDF and PDF expressions of end-to-end SNRs are obtained and the closed-form expressions for the average secrecy capacity (ASC) and secrecy outage probability (SOP) in known and unknown CSI scenarios, are derived. The numerical results are discussed in Section 5. Finally, this paper is concluded in Section 6.
2 | SYSTEM MODEL AND SECRECY-RATE FORMULATION

In the following section, we first introduce the system model of the proposed indoor dual-LED VLC system. Then, the CSI knowledge of each transmitting link is estimated by the pilot signal process and formulate the secrecy-rate for both known and/or unknown CSI scenarios.

2.1 | System model

In this paper, we propose an indoor VLC network wherein a source transmitter (S) equipped with two LEDs (i.e. LD₁ and LD₂), transmits the information to a legitimate user (M) and assume that an active/passive eavesdropper (E) is also present in the same coverage region, as shown in Figure 1. However, each transmitter is equipped with a single photo-detector (PD). Both LD₁ and LD₂ LEDs are installed in a strategic manner so that receiver M can receive the broadcast information via each LED. Further, S is constrained to use either LD₁ or LD₂ to transmit the legitimate information. According to [11–14], each VLC link is incorporated with the slow-fading effects and the information is broadcasted into multiple coherence intervals of equal duration (T). Further, the information received at M and/or E can be given as

\[ y_{Mk}(i) = h_{Mk}(i)x(i) + n_{Mk}(i), \]  

\[ y_{Ek}(i) = h_{Ek}(i)x(i) + n_{Ek}(i), \]

where, subscript k ∈ {1, 2} is used for both legitimate (i.e. from S to M_k) and eavesdropping (i.e. from S to E_k) links, and x(i) is the transmit optical intensity signal from S in an instantaneous coherence interval i. The parameters h_{Mk} and h_{Ek} are the channel gain coefficients of the legitimate and eavesdropping links, respectively, which are also known as CSI coefficients of M_k and E_k links. Moreover, n_{Mk} ∼ N(0, σ_{Mk}) and n_{Ek} ∼ N(0, σ_{Ek}) are additive white Gaussian noise (AWGN) at M and E with zero mean and variances σ_{Mk} and σ_{Ek}, respectively. As we know that the instantaneous SNR at receiver is the function of the magnitude of CSI coefficient hence, the receiver, that is, either M and/or E must have complete CSI of their receiving links.

The channel gain h_{E_k} of the transmitting link can be expressed by [23] as

\[ h_{E_k} = \begin{cases} \Theta U(\psi_{E_k}) \cos^m \phi(\psi_{E_k}) \cos \psi_{E_k}, & 0 \leq \psi_{E_k} \leq \psi_{FOV}, \\ 0, & \psi_{E_k} > \psi_{FOV}, \end{cases} \]  

\[ g = \begin{cases} \frac{n^2}{\sin^2 \psi_{FOV}}, & 0 \leq \psi_{E_k} \leq \psi_{FOV}, \\ 0, & \psi_{E_k} > \psi_{FOV}, \end{cases} \]

where Θ = \frac{A}{2 \pi d_{E_k}^2} and \psi_{E_k} ∈ \{M_k, E_k\}. The terms A and R_p are the detector area and responsivity parameters of the photodetector and d_{E_k} is the Euclidean distance. The parameters, \psi_{E_k} and \phi(\psi_{E_k}) are denoted as the incidence and irradiance angles. The order of Lambertian radiation pattern is represented as m which can further be given by m = \frac{-1}{\log_2(\cos(\phi_{1/2}))}, where \phi_{1/2} is the semi-angle of each individual LED. The PD of the receiver is equipped with a hemisphere plastic lens to concentrate the gained optical energy, which can maintain a wide field-of-view (\psi_{FOV}) angle. U(\psi_{E_k}) denote the optical filter gain and g(\phi(\psi_{E_k})) is the optical concentrator gain, which can be given as,

\[ b_{E_k} = \frac{m+1}{(r_{E_k}^2 + L^2)^{m+1}}, \]

where n is the optical concentrator parameter denoted as reflective index. It has been considered that both legitimate and eavesdropper terminals are uniformly distributed, in a circular cell. Further, the irradiance angle \phi_{E_k}, incidence angle \psi_{E_k} and d_{E_k} is the Euclidean distance parameter of receiver node which can further be defined as \cos \psi_{E_k} = \cos \phi_{E_k} = \frac{L}{d_{E_k}} , here, L is the vertical height of the deployed transmitter S from the centre point a. d_{E_k} = (r_{E_k}^2 + L^2)^{1/2}, where, r_{E_k} is the radial distance of receiver E_k from the point a. Further, utilising (3), the DC channel gain for LOS components is given as,

Remark 1. According to [18], the directivity of the transmitting LED is related to the semi-angle \phi_{1/2}. Further, the Lambertian radiation pattern becomes unity, that is, m = 1 when \phi_{1/2} = 60°
which corresponds to an ideal LED transmitter. Thus, increasing the semi-angle value beyond 60° reduces the transmitter performance. Hence, the coverage area of the VLC technology remains limited, and the receiver is constrained to be present in the coverage region only. The scenario when we consider that multiple LEDs (i.e. \( LD_1, LD_2, ..., LD_n \)) are co-deployed in an indoor VLC environment. Then, out of \( n \) transmitting LEDs, only two/three LEDs (i.e. the LEDs which comes in the FOV range of \( M \)) are able to transmit the information to \( M \). Therefore, the proposed dual-LED indoor VLC system model is closer to the realistic deployment.

### 2.2 Channel estimation

The source transmitter \( S \) utilises the pilot symbol transmission process to receive the instantaneous CSI feedbacks from both \( M \) and/or \( E \). We assume that legitimate and eavesdropping links are estimated by using a minimum mean square error (MMSE) estimation technique, which is defined in [28]. The basic advantage of this technique is that it can minimise the mean square error (MSE) during the pilot transmission process. The estimation of the channel gain is denoted as \( h_{\gamma_k} \) and the estimation error is denoted as \( \hat{h}_{\gamma_k} \) [27]. Therefore, gain of the transmitting channel can be defined as,

\[
h_{\gamma_k} = h_{\gamma_k} + \hat{h}_{\gamma_k},
\]

where \( h_{\gamma_k} \) and \( \hat{h}_{\gamma_k} \) are assumed to be zero-mean Gaussian distributed random variables. It is considered that \( y_{\gamma_k} \) is the linear function of the channel coefficient. Therefore, the estimated coefficient and estimated error are also zero-mean complex Gaussian distributed. In fact, \( y_{\gamma_k} \) is what \( M \) and/or \( E \) feedbacks to \( S \) as an instantaneous CSI. The orthogonality principle implies that \( E\{h_{\gamma_k}^2\} = E\{h_{\gamma_k}^2\} + E\{\hat{h}_{\gamma_k}^2\} \). According to [26], the variance of the channel estimation error can be written as,

\[
\sigma_{\gamma_k} = E\{\hat{h}_{\gamma_k}^2\} = \frac{1}{1 + \alpha P_s T_s},
\]

where \( P_s \) is defined as the nominal optical intensity of the transmitting signal from \( S \). Hence, the average instantaneous SNR of the VLC channel can be obtained as \( \gamma_{\gamma_k} = \frac{P_s \xi B}{\sigma_{\gamma_k}^2} \), where \( B \) can be denoted as modulation bandwidth of the broadcasted signal and \( \xi \) is an optical to electrical conversion efficiency parameter. The parameter \( \alpha \) can be given as, \( \alpha = \frac{E\{|d|^2\}}{E\{|t|^2\}} \), where \( d \) is the transmitted data symbol, \( t \) is the pilot symbol and \( E\{|\cdot|\} \) is the expectation operator. Further, when \( E\{|d|^2\} = 1 \), \( \alpha \) can be denoted as the pilot power, which is normalised by the data power \( E\{|t|^2\} \). Thus, \( \alpha \) is directly proportional to the channel training length. The parameter \( T_s \) is the length of the transmitted pilot symbol and we assume that \( T_s = 1 \). Hence, \( \sigma_{\gamma_k} \) is merely affected by the normalised pilot power \( \alpha \). We assume that each receiver is using an estimated channel gain for the information detection. Then, according to [26], the actual instantaneous SNR of the channel can be defined as,

\[
\gamma_{\gamma_k} = \frac{P_s \xi B^2}{1 + \frac{\alpha P_s}{\sigma_{\gamma_k}^2}}, \tag{8}
\]

Further, the PDF expression of \( \gamma_{\gamma_k} \) can be defined as,

\[
f_{\gamma_k}(\gamma) = \frac{K_k}{m_k + 3} \left( \frac{1}{\gamma} \right)^{m_k+2} (\gamma - \frac{\alpha P_s}{\sigma_{\gamma_k}^2})^{1/m_k+1}, \tag{9}
\]

where, \( K_k = (E\{y_{\gamma_k} \})^2 \alpha P_s \sigma_{\gamma_k}^{-2(m_k+1)} \). Moreover, the CDF expression can be obtained by using (9) as,

\[
F_{\gamma_k}(\gamma) = v_k - K_k \left( \frac{\gamma}{\gamma_{\gamma_k}} \right)^{-1/m_k+1}, \tag{10}
\]

where \( v_k = (1 + \frac{L_k^2}{\gamma_{\gamma_k}^2}) \) and \( \gamma_{\gamma_k} \in [\gamma_{\min}, \gamma_{\max}] \), where \( \gamma_{\min} \leq \gamma_{\gamma_k} \leq \gamma_{\max} \), here \( \gamma_{\min} \) and \( \gamma_{\max} \) are the instantaneous minimum and maximum SNR parameters which can further be defined as

\[
\gamma_{\min} = \frac{(E\{y_{\gamma_k} \})^2 (m_k + 1) L_k^2}{2 \alpha P_s (m_k + 3)}, \tag{11}
\]

and

\[
\gamma_{\max} = \frac{(E\{y_{\gamma_k} \})^2 (m_k + 1) L_k^2}{(\alpha P_s + L_k^2)(m_k + 3)}, \tag{12}
\]

respectively.

### 2.3 CSI knowledge

As stated before, \( S \) transmits a pilot signal to both \( M \) and \( E \) to feedback of their estimated instantaneous channel state information parameters. Since, \( M \) is a legitimate user, hence, we can assume that \( S \) gets the knowledge of legitimate link as \( \gamma_{M_k} = \gamma_{M_k} \), which is an instantaneous SNR of legitimate link. The actual SNR of legitimate link can be given by (8), when \( z_k = M_k \). However, we assume that \( E \) may be an active user (i.e. other than \( M \)) or a passive user (i.e. a malicious node). Hence, \( S \) may or may not get the feedback from \( E \). Therefore, we assume the following two scenarios on the basis of channel knowledge of an eavesdropping link.

- **Scenario 1**: Let \( E \) is an active user and hence, \( S \) can estimate the instantaneous SNR of eavesdropping link as \( \gamma_{E_k} = \gamma_{E_k} \). We assume that \( E \) can also use the MMSE estimation technique to estimate \( h_{\gamma_k} \) for the information interception purpose. Hence, the actual SNR of eavesdropping link can be obtained by (8), when \( z_k = E_k \).
Switching mechanism

SECURE LED SELECTION SCHEME

Selection strategy for Scenario-1

The secrecy-rate formulation for known/unknown CSI

Based on instantaneous CSI knowledge of the legitimate link, $S$ can estimate the received SNR at $M$ as $\gamma_{Mk}$. Hence, the channel capacity of the corresponding link can be calculated as $C_{Mk} = \log_2(1 + \gamma_{Mk})$. Further, with known CSI of the eavesdropping link, the secrecy-rate is formulated in the following.

2.4.1 Scenario-1

Based on estimated CSI of the eavesdropping link, instantaneous eavesdropper SNR can be given as $\gamma_{Ek}$. Further, the channel capacity of the corresponding link can be defined as $C_{Ek} = \log_2(1 + \gamma_{Ek})$. Therefore, for perfectly known CSI scenario, secure information broadcasting rate ($C_{sk}$) [10] can be written as,

$$C_{sk} = \begin{cases} [C_{Mk}(i) - C_{Ek}(i)]^+, & \text{for } \gamma_{Mk}(i) > \gamma_{Ek}(i), \\ 0, & \text{otherwise}, \end{cases}$$  \hspace{1cm} (13)

where non-negative parameter $[x]^+ \triangleq \max\{x; 0\}$ is denoting that the positive secrecy-rate can be achieved when $\gamma_{Mk}$ is greater than $\gamma_{Ek}$ or channel conditions of legitimate link are better than the channel conditions of eavesdropping link.

2.4.2 Scenario-2

Based on channel statistics of the eavesdropping link, the transmitter $S$ estimates the average SNR at $E$ as $\overline{\gamma}_{Ek}$. Then, the average channel capacity of the eavesdropping link can be calculated as $\overline{C}_{Ek} = \log_2(1 + \overline{\gamma}_{Ek})$. In this scenario, $S$ broadcasts the information with a pre-determined broadcasting rate $R_b$ [27]. The selection of $R_b$ is related to the channel capacity of legitimate $M_k$ link. The condition when $C_{Mk}$ is greater than $R_b$, $S$ broadcasts the information towards the legitimate user $M$. Otherwise, the condition when $C_{Mk}$ is less than $R_b$ then, $S$ does not broadcast information and the connection outage occurs. Therefore, for unknown CSI scenario, the secure information broadcasting rate ($\overline{C}_{sk}$) can be written as,

$$\overline{C}_{sk} = \begin{cases} [C_{Mk}(i) - R_b(i)]^+, & \text{for } \gamma_{Mk}(i) > \overline{\gamma}_{Ek}(i), \\ 0, & \text{otherwise}, \end{cases}$$  \hspace{1cm} (14)

where $\overline{\gamma}_{Ek} = 2^{R_b} - 1$.

Remark 2. In Scenario-1, when the pilot power $\alpha$ increases, the knowledge of both legitimate as well as eavesdropping links enhances as $\alpha$ adapts the pilot signalling technique to estimate the feedbacks from both $M$ and $E$. Hence, $\alpha$ does not affect the secrecy-rate given by (13). This incurs a negative impact on the secure information transmission. However, in Scenario-2, when $\alpha$ increases, the knowledge of legitimate link enhances and $R_b$ does not depend on $\alpha$. Hence, $\alpha$ affects the secrecy-rate given by (14).

3 SECURE LED SELECTION SCHEME

In this section, we first define the switching mechanism of the source transmitter and then, the desire LED selection strategies of the proposed scheme are described in detail.

3.1 Switching mechanism

In a transmission time interval $t$, $S$ transmits a pilot signal over each transmitting link to estimate their CSI knowledge. Further, on the basis of the feedbacks received from $M$ and/or $E$, $S$ calculates the secrecy-rate of the legitimate information broadcasting, and selects either $LD_1$ or $LD_2$. If both of the LEDs satisfy the positive secrecy-rate, $S$ selects the LED which provides the higher secrecy-rate. Otherwise, the system outage occurs and then, $S$ remains silent.

3.2 Selection strategy for Scenario-1

Let us consider the decision indicator $I_i$ for the selection of secure-link in time interval $i$ such that $I_i = 0$ indicates that $LD_1$ is selected, and $I_i = 1$ indicates that $LD_2$ is selected, and $I_i = -1$ indicates that none of the LED is selected and hence, $S$ remains silent.

In Scenario-1, $S$ has instantaneous CSIs of both $M_k$ and $E_k$ links. Then, the condition when $C_{M1} \geq C_{E1}$ (or $C_{M2} \geq C_{E2}$) satisfies, the LED $LD_1$ (or $LD_2$) is selected for broadcasting. However, if $C_{M1} < C_{E1}$ and $C_{M2} < C_{E2}$, none of the LED is selected. Then, the system outage condition occurs, and $S$ remains silent. The summary of this selection strategy is given in Algorithm 1.

3.3 Selection strategy for Scenario-2

If transmitter $S$ has instantaneous CSI of $M_k$ link only and if $C_{M1} \geq R_b$ (or $\overline{C}_{M1} \geq R_b$) then $LD_1$ (or $LD_2$) is selected for broadcasting. However, if $C_{M1} < R_b$ and $\overline{C}_{M2} < R_b$, none of the LED is selected. Then, the system outage condition occurs, and $S$ remains silent. The summary of this selection strategy is given in Algorithm 2.
ALGORITHM 1 Selection algorithm for Scenario-1

1: initialisations : Instantaneous CSIs of both $M_k$ and $E_k$ links;
2: Decision : Link decision indicator $L_i$ here $i \in \{1, 2, 3, \ldots, T\}$;
3: for $i = 1; i \leq T : i + +$ do
4: Calculate $C_{M_k}(i)$ and $C_{E_k}(i)$ based on obtained CSIs;
5: if $C_{M_k}(i) \geq C_{E_k}(i) \wedge C_{a_k}(i) > 0$ then 
6: $L_i = 0$;
7: else if $C_{M_k}(i) \geq C_{E_k}(i) \wedge C_{a_k}(i) > 0$ then 
8: $L_i = 1$;
9: else 
10: $L_i = -1$;
11: end if
12: end for

ALGORITHM 2 Selection algorithm for Scenario-2

1: Initialisations : Instantaneous CSIs of $M_k$ link, non-negative threshold parameter $R_o$;
2: Decision : Indicator $L_i$ here $i \in \{1, 2, 3, \ldots, T\}$;
3: for $i = 1; i \leq T : i + +$ do
4: Calculate $C_{M_k}(i)$ based on obtained CSI;
5: if $C_{M_k}(i) \geq R_o \wedge C_{a_k}(i) > 0$ then 
6: $L_i = 0$;
7: else if $C_{M_k}(i) \geq R_o \wedge C_{a_k}(i) > 0$ then 
8: $L_i = 1$;
9: else 
10: $L_i = -1$;
11: end if
12: end for

4 PERFORMANCE ANALYSIS

In this section, the closed-form secrecy outage probability (SOP) and average secrecy capacity (ASC) expressions for the end-to-end SNR are derived for both known and unknown CSI scenarios.

4.1 SOP for Scenario-1

A pre-defined secrecy rate $R_s$ (here $R_s > 0$) is considered. Further, $S$ can broadcast the information when $C_{a_k}$ is greater than $R_s$. However, $S$ does not broadcast the information when $C_{a_k}$ is less than $R_s$, then, it is considered that the system outage occurs [9]. Therefore, the SOP expression of the stand-alone VLC system can be written as,

$$ P_{o_k}(R_s) = P[C_{a_k} < R_s] $$

where the parameter $\lambda_k = \tau (1 + \gamma_{E_k}) - 1$, which is directly mapped through secrecy rate $R_s$. Further, utilising (9) and (15), the closed-form SOP expression can be obtained as

$$ P_{o_k}(R_s) = \sum_{k=0}^{\infty} \left( -\frac{1}{\alpha_k+1} \right) S_{k,1} \left( \gamma_{\min} - \frac{1}{\alpha_k+1} \lambda_k \right) \left( \gamma_{\max} \right) $$

where term $S_{k,1}$ can be given as,

$$ S_{k,1} = \frac{K_k^2 T_k \gamma_{E_k}^{\alpha_k+3}}{(\alpha_k + 1)!} \left( \gamma_{\max} \right) $$

The parameters $\gamma_{\min}$ and $\gamma_{\max}$ are given in (11) and (12), respectively. After substituting the value of $k = 1$ and/or $k = 2$, in (16), the closed-form SOP expression of end-to-end SNR can be obtained for the case when $S$ can utilise either LD$D_1$ and/or LD$D_2$ LED to broadcast the information. The outage condition of secure broadcasting of the proposed system occurs when broadcasting rate of both $M_k$ and $M_2$ links falls below $R_s$. Therefore, the closed-form SOP expression of the proposed VLC system can be written as,

$$ P_{o_{\text{Dual-LED}}}(R_s) = P(C_{a_1} < R_s, C_{a_2} < R_s) $$

Further, after substituting (16) and (30) into (30), one can obtain the closed-form SOP expression of proposed VLC system.

4.2 ASC for Scenario-1

The broadcasting rate $C_{s_k}$ with known CSI scenario, can be written by using (13) as,

$$ C_{s_k}(\gamma_{M_k}, \gamma_{E_k}) = \left[ \log_2 \left( 1 + \frac{\gamma_{M_k}}{1 + \gamma_{E_k}} \right) \right]^{+} $$

(19)
Further, the average secrecy capacity ($\overline{C}$) is defined as,

$$\overline{C}_{\text{sk}}(\gamma_{M_1}, \gamma_{E_2}) = E[C_{\text{sk}}(\gamma_{M_1}, \gamma_{E_2})]$$

$$= \int_{Y_{\text{min}}}^{Y_{\text{max}}} \int_{Y_{\text{min}}}^{Y_{\text{max}}} C_{\text{sk}}(\gamma_{M_1}, \gamma_{E_2}) f_{\gamma_{M_1}}(\gamma_{M_1}) f_{\gamma_{E_2}}(\gamma_{E_2}) d\gamma_{M_1} d\gamma_{E_2},$$

(20)

Utilising $f_{\gamma_{M_1}}(\gamma_{M_1})$ and $f_{\gamma_{E_2}}(\gamma_{E_2})$ expressions from (9) to (20), the closed-form ASC expression is given in (21).

$$\overline{C}_{\text{sk}}(\gamma_{M_1}, \gamma_{E_2})$$

$$= \frac{1}{\ln2} v_k(1 - v_k) C_{k,1} + \frac{2r_k}{\gamma_{M_1} - \gamma_{E_2}} - \frac{1}{\gamma_{M_1} - \gamma_{E_2}} C_{k,2}$$

$$- \frac{K_k^2}{\gamma_{M_1} - \gamma_{E_2}} \left[ \overline{C}_{k,3} \right],$$

(21)

Further, the parameters $\overline{C}_{k,1}$, $\overline{C}_{k,2}$ and $\overline{C}_{k,3}$ given in (21), can be defined by using eq.(1.112.1) of [31] as,

$$\overline{C}_{k,1} = \sum_{i_k=1}^{\infty} (-1)^{i_k - 1} \left[ \gamma_{\text{max}}^i - \gamma_{\text{min}}^i \right],$$

(22)

$$\overline{C}_{k,2} = \sum_{i_k=1}^{\infty} (-1)^{i_k - 1} \left[ \frac{1}{\gamma_{\text{max}}^{i_k} - \gamma_{\text{min}}^{i_k}} - \frac{1}{\gamma_{\text{max}}^{i_k} - \gamma_{\text{min}}^{i_k}} \right],$$

(23)

and

$$\overline{C}_{k,3} = \sum_{i_k=1}^{\infty} (-1)^{i_k - 1} \left[ \frac{1}{\gamma_{\text{max}}^{i_k} - \gamma_{\text{min}}^{i_k}} - \frac{1}{\gamma_{\text{max}}^{i_k} - \gamma_{\text{min}}^{i_k}} \right].$$

(24)

After substituting the value of $k = 1$ and/or $k = 2$ in (21), once can obtain the ASC expressions of the legitimate link when transmitter adapts either $LD_{1}$ or $LD_{2}$ to broadcast information.

According to [22], it has been considered that the ASC of the proposed system affects mainly due to the following two factors: i) the information broadcasting rate of the transmitting $M_1$ and $M_2$ links; and ii) the secrecy outage period of simultaneous LEDs, that is, either $LD_{1}$ or $LD_{2}$ remain active. Hence, the ASC expression of proposed system can be written as,

$$\overline{C}_{\text{sk}} = \left( 1 - P_{\text{th}}(R) \right) \overline{C}_{\text{th}} + \left( 1 - P_{\text{sk}}(R) \right) \overline{C}_{\text{sk}}.$$  

(25)

Utilising (21), (16), and (25), the closed-form expression for ASC can be obtained.

**Remark 3.** The infinite series given (16) and (21) are convergent series and hence, the obtained closed-form expressions does not require infinite sum terms. For determining the convergence of series, the ratio test is performed. From (16), the ratio test parameter $I_{\text{sg}} = \lim_{i_k \to \infty} \left( \frac{1}{\gamma_{\text{max}}^{i_k + 1}} - \frac{1}{\gamma_{\text{max}}^{i_k}} \right)$ can be expressed as

$$I_{\text{sg}} = \lim_{i_k \to \infty} \frac{1}{\gamma_{\text{max}}^{i_k + 1}} - \frac{1}{\gamma_{\text{max}}^{i_k}} = \frac{1}{\gamma_{\text{max}}^{i_k + 1}} - \frac{1}{\gamma_{\text{max}}^{i_k}},$$

(26)

after doing some algebra. (26) can be obtained as

$$I_{\text{sg}} = \lim_{i_k \to \infty} \frac{1}{\gamma_{\text{max}}^{i_k + 1}} - \frac{1}{\gamma_{\text{max}}^{i_k}} = \frac{1}{\gamma_{\text{max}}^{i_k + 1}} - \frac{1}{\gamma_{\text{max}}^{i_k}}.$$  

(27)

After substituting $i_k = \infty$ in (27), the obtained value of $I_{\text{sg}}$ is zero. Thus, by ratio test it has been verified that $I_{\text{sg}} < 1$ and hence, the given series converges. Moreover, after substituting (22)–(24) in (21) and by ratio test, it has been verified that the series given in (21) converges as both $\gamma_{\text{min}}$ and $\gamma_{\text{max}}$ tends to zero at $i_k = \infty$. Therefore, obtained expressions in (16) and (21) are closed-form expressions.

4.3 | SOP for Scenario-2

Substituting (14), the SOP expression for the stand-alone system, can be defined as,

$$P_{\text{sg}}(R) = P [\overline{C}_{\text{th}} < R]$$

$$= P [\overline{C}_{\text{th}} < R (1 + \gamma_{\text{th}}) - 1]$$

$$= \int_{\overline{C}_{\text{th}}}^{\overline{C}_{\text{th}} + 2R} f_{\gamma_{M_1}}(\gamma_{M_1}) d\gamma_{M_1},$$

(28)
where $\hat{\lambda}_k = \tau \left( 1 + \gamma_{th_k} \right) - 1$. From (9) and (28), the closed-form SOP expression can be obtained as,

$$P_{k}(R_{s}) = K_{3} \gamma_{th_k}^{\frac{1}{\alpha_k+1}} \left( \gamma - \frac{1}{\alpha_k+1} - \frac{1}{\alpha_k+1} \right). \tag{29}$$

After substituting the valued of $k = 1$ and/or $k = 2$, in (29), the SOP expressions for each individual transmitting LED can be obtained.

According to [22], it has been considered that the outage for information broadcasting occurs when broadcasting rates of both individual $M_1$ and $M_2$ links falls below $R_s$. Therefore, the closed-form SOP expression of the proposed VLC system can be written as,

$$P_{\text{Dual-LED}}(R_{s}) = P(C_{\text{th}_1} < R_s, C_{\text{th}_2} < R_s)$$

$$= P(C_{\text{th}_1} < R_s) \times P(C_{\text{th}_2} < R_s)$$

$$= P_{\text{th}_1}(R_s) \times P_{\text{th}_2}(R_s). \tag{30}$$

After substituting (16) and (30) into (30), the closed-form SOP expression can be obtained.

### 5 | NUMERICAL RESULTS

In the following section, we first quantify three optimal values of normalised pilot power ($\alpha$) according to achieved secrecy-rate under the constraint of interference power of primary user. Then, the performance of proposed system is evaluated according to optimal values of $\alpha$ by varying various physical parameters. The performance of the proposed system is analysed on the basis of the parameters which are given in Table 1.

Figure 2 demonstrates the achievable broadcasting rate in terms of secrecy-rate against the normalised pilot signal power $\alpha$, when $\gamma_{th} = 0$ dB and $R_0 = 0.6781$ bits/s/Hz. For Scenario-1, it can be observed from the curves of $\gamma_{th} = 5$ dB, $\gamma_{th} = 10$ dB and $\gamma_{th} = 15$ dB that the secrecy-rate increases fast to a peak value when $\alpha$ increases to its optimal value at $\alpha = 19$ for $\gamma_{th} = 5$ dB, at $\alpha = 9$ for $\gamma_{th} = 10$ dB, and at $\alpha = 6$ for $\gamma_{th} = 15$ dB. Similarly, for Scenario-2, the secrecy-rate increases to its peak value when $\alpha$ increases to its optimum value at $\alpha = 18$ for $\gamma_{th} = 5$ dB, at $\alpha = 8$ for $\gamma_{th} = 10$ dB, and at $\alpha = 5$ for $\gamma_{th} = 15$ dB. Thus, it is not always good to have more pilot power to get more accurate channel estimations as increasing $\alpha$ value increases to a problem against the secure information broadcasting (as discussed in Remark-1). As an alternative solution, we have calculated three optimum values of $\alpha$ under which $S$ can transmit information securely. Then, the performance of the proposed dual-LED system is evaluated on the basis of these three $\alpha$ values. It can also be observed from the plot that the achieved secrecy-rate under known CSI is higher than the achieved secrecy-rate under unknown CSI scenario. One can notice that the optimised values of $\alpha$ under which $S$ can transmit information securely. Then, the performance of the proposed dual-LED system is evaluated on the basis of these three $\alpha$ values. It can also be observed from the plot that the achieved secrecy-rate under knownCSI is higher than the achieved secrecy-rate under unknownCSI scenario. One can notice that the optimised values of $\alpha$ under which $S$ can transmit information securely. Then, the performance of the proposed dual-LED system is evaluated on the basis of these three $\alpha$ values. It can also be observed from the plot that the achieved secrecy-rate under knownCSI is higher than the achieved secrecy-rate under unknownCSI scenario. One can notice that the optimised values of $\alpha$ under which $S$ can transmit information securely. Then, the performance of the proposed dual-LED system is evaluated on the basis of these three $\alpha$ values. It can also be observed from the plot that the achieved secrecy-rate under knownCSI is higher than the achieved secrecy-rate under unknownCSI scenario. One can notice that the optimised values of $\alpha$ under which $S$ can transmit information securely. Then, the performance of the proposed dual-LED system is evaluated on the basis of these three $\alpha$ values. It can also be observed from the plot that the achieved secrecy-rate under knownCSI is higher than the achieved secrecy-rate under unknownCSI scenario. One can notice that the optimised values of $\alpha$ under which $S$ can transmit information securely. Then, the performance of the proposed dual-LED system is evaluated on the basis of these three $\alpha$ values. It can also be observed from the plot that the achieved secrecy-rate under knownCSI is higher than the achieved secrecy-rate under unknownCSI scenario. One can notice that the optimised values of $\alpha$ under which $S$ can transmit information securely. Then, the performance of the proposed dual-LED system is evaluated on the basis of these three $\alpha$ values. It can also be observed from the plot that the achieved secrecy-rate under knownCSI is higher than the achieved secrecy-rate under unknownCSI scenario.

The plot represented in Figure 4 represents the effect of $\gamma_{th}$ in dB on the ASC is shown for different FOV values. It can be observed from the figure that the lower values of FOV provide better results for ASC. This is due to the fact that the incident power at the receiver is related to the FOV angle, and as FOV angle decreases, the optical concentrator gain of the receiver improves [18]. It is quite intuitive from the plot that FOV at 50° provides higher broadcasting rate against eavesdropping attacks than the FOV at 60°. However, the FOV value cannot be decreased below a certain limit as this might affect the receiver mobility [7], [22]. Therefore, for further enhancement in the security performance, the vertical height $L$ is reduced as it can enhance the receiver SNR. It can be observed that as height $L$ reduces form 3.5 m to 2.5 m, the ASC value increases.

The plot represented in Figure 4 represents the effect of $\gamma_{th}$ on SOP performance for both known and unknown CSI scenarios, when $\gamma_{th} = 5$ dB and $R_0 = 4$ bits/s/Hz. It can be seen from the plot that when FOV value increases from 50° to 60°, the

| Parameters      | Values       |
|-----------------|--------------|
| Room size $l \times b \times h$ | $5m \times 5m \times 5m$ |
| Refractive index ($\alpha$) | 1.5 |
| Optical filter gain ($U/\psi_{\lambda})$ | 1 |
| Effective aperture of PD ($A$) | $10^{-4}m$ |
| Field-of-view ($\psi_{1/2}$) | 70° |
| Semiangle at half power ($\psi_{1/2}$) | 70° |
| Optical-to-electrical conversion efficiency ($\varepsilon$) | 0.64 A/W |
| Noise power spectral density ($N_0$) | $10^{-21} \text{A}^2/\text{Hz}$ |

![Figure 2: Secrecy-rate versus $\alpha$ for varying $\gamma_{th}$ with known and unknown imperfect CSI scenarios](image-url)
SOP value increases. Hence, the probability of secure information broadcasting rate enhances when the FOV value decreases [6], [22]. It can also be observed from the plot that the SOP value for known CSI is lower than the SOP value with unknownCSI. Therefore, the probability of the secrecy outage occurrence for the proposed dual-LED system under known CSI scenario is less than the outage occurrence under unknown CSI scenario.

The Figure 5 shows the effect of $\gamma_M$ on the ASC wherein one can observe the effect of $\gamma_E$ on secure information rate. It can be seen form the plot that as $\gamma_E$ increases form 5 dB to 15 dB, the value of ASC decreases. Hence, this realises the fact that the secure information broadcasting rate reduces when eavesdropper channel conditions becomes better than the channel conditions of legitimate link [19]. For further enhancement in security performance, one can adjust the pre-defined secrecy-rate parameter, $R_s$. Therefore, $R_s$ at 1 bit/s/Hz provides the higher security against eavesdropping attacks than $R_s$ at 2 bits/s/Hz.

In Figure 6, the effect of $\gamma_M$ is shown on the SOP with known and unknown CSI scenarios, when $\text{FOV}=50^\circ$, $L=2.5$ m. For known CSI scenario, it can be seen form the plot that as $\gamma_E$ increases form 5 dB to 15 dB, the SOP increases. Moreover, $R_s$ at 1 bit/s/Hz provides better results in comparison to $R_s$ at 2 bits/s/Hz. For unknown CSI scenario, the SOP is higher, when $\gamma_{th}$ increases from 45dB to 55dB. To prevent the eavesdropping attacks, the higher value of pre-defined transmission rate $R_b$ (here, $R_b = 5.5236, 5.8074$ bits/s/Hz) is considered [27]. However, from (14), it is clear that high value of $R_b$ reduces the secrecy-rate.
The effect of $\gamma_M$ on SOP analysis with known and unknown CSI scenarios is shown in Figure 7 where $\gamma_E = 5$ dB, FOV = 50° and $R_k = 4$ bits/s/Hz. We have taken three pre-optimised values of $\alpha$ (i.e. $\alpha = 19$, 9, 6) into consideration. Hence, it can be seen from the Figure 7 that when $\alpha$ increases, the SOP performance deteriorates. This is because of the fact that as $\alpha$ increases, the secrecy-rate reaches to its peak value, as discussed earlier. The security performance of the system with known CSI scenario is better than the performance with unknown CSI. It can be observed from all plots that the proposed dual-LED VLC system is providing better results in comparison to the conventional stand-alone VLC system. In each plotted result, we can observe that the numerical results are in excellent agreement with the simulation results.

6 | CONCLUSION

The secure information broadcasting in the proposed dual-LED VLC system is analysed and the novel closed-form ASC and SOP expressions are derived. In particular, the secrecy rate expressions are formulated for both known and/or unknown imperfect CSI scenarios utilising the MMSE estimation technique. The numerical analysis concludes that our proposed dual-LED VLC system performs better in contrast to the conventional stand-alone VLC system, from security prospective. Thus, it can be concluded that the proposed secure-LED selection scheme is guarantee to provide secure broadcasting against both active as well as passive eavesdropping attacks.

ACKNOWLEDGEMENT

This paper is supported by Science and Engineering Research Board (SERB) sponsored CRG project titled as “Energy Efficient RF/VLC networks for IoT Applications” File No: CRG/2018/002651.

REFERENCES

1. Pathak, P.H., et al.: Visible light communication, networking, and sensing: A survey, potential and challenges. IEEE Commun. Sur. Tutor. 17(4), 2047–2077 (2015)
2. Cálcia, A., Diniz, M.: Current challenges for visible light communications usage in vehicle applications: A survey. IEEE Commun. Sur. Tutor. 19(4), 2681–2703 (2017)
3. Komine, T., et al.: Adaptive equalization system for visible light wireless communication utilizing multiple white LED lighting equipment. IEEE Trans. Wirel. Commun. 8(6), 2892–2900 (2009)
4. Bykhovsky, D., Arnon, S.: Multiple access resource allocation in visible light communication systems. J. Lightwave Technol. 32(8), 1594–1600 (2014)
5. Chen, C., et al.: On the coverage of multiple-input multiple-output visible light communications. IEEE/OSA J. Opt. Commun. Netw. 9(9), D31–D41 (2017)
6. Basnayaka, D.A., Haas, H.: Design and analysis of a hybrid radio frequency and visible light communication system. IEEE Trans. Commun. 65(10), 4334–4347 (2017)
7. Wang, J., et al.: Physical-layer security for indoor visible light communications: Secrecy capacity analysis. IEEE Trans. Commun. 66(12), 6423–6436 (2018)
8. Wang, J., et al.: On the secrecy rate of spatial modulation-based indoor visible light communications. IEEE J. Sel. Areas Commun. 37(9), 2087–2101 (2019). https://doi.org/10.1109/JSAC.2019.2929403
9. Shannon, C.E.: Communication theory of secrecy systems. Bell Labs Tech. J. 28(4), 656–715 (1949)
10. Wyner, A.D.: The wire-tap channel. Bell Syst. Tech. J. 54(8), 1355–1387 (1975)
11. Parada, P., Blahut, R.: Secrecy capacity of SIMO and slow fading channels. In: Proceedings of International Symposium on Information Theory, pp. 2152–2155. IEEE, Piscataway (2005)
12. Barros, J., Rodrigues, M.R.D.: Secrecy capacity of wireless channels. In: 2006 IEEE International Symposium on Information Theory, pp. 358–360. IEEE, Piscataway (2006)
13. Gopala, P.K., et al.: On the secrecy capacity of fading channels. In: IEEE Trans. Inf. Theory 54(10), 4687–4698 (2008)
14. Bloch, M., et al.: Wireless information-theoretic security. IEEE Trans. Inf. Theory 54(6), 2515–2534 (2008)
15. Al-Moliki, Y.M., et al.: Secret key generation protocol for optical OFDM systems in indoor VLC networks. IEEE Photon. J. 9(2), 1–15 (2017)
16. Liao, Z., et al.: Physical layer security for dual-hop VLC/RF communication systems. IEEE Commun. Lett. 22(12), 2603–2606 (2018)
17. Mostafa, A., Lampe, L.: Physical-layer security for MISO visible light communication channels. IEEE J. Sel. Areas Commun. 33(9), 1806–1818 (2015)
18. Yin, L., Haas, H.: Physical-layer security in multiuser visible light communication networks. IEEE J. Sel. Areas Commun. 36(1), 162–174 (2018)
19. Bloch, M.R., Laneman, J.N.: Strong secrecy from channel resolvability. IEEE Trans. Inf. Theory 59(12), 8077–8098 (2013)
20. Al-Moliki, Y.M., et al.: Randomness evaluation of key generation based on optical OFDM system in visible light communication networks. Electron. Lett. 53(24), 1594–1596 (2017)
21. Al-Moliki, Y.M., et al.: Physical-layer security against known/unknown plaintext attacks for OFDM-based VLC system. IEEE Commun. Lett. 21(12), 2606–2609 (2017)
22. Ambrish, G.P.: Dual-element indoor VLC network with two-stage secure link adaptation scheme. In: 2019 5th International Conference on Signal Processing, Computing and Control (ISPCC), pp. 366–371 (2019). IEEE, Piscataway (2019)
23. Kumar, A., et al.: PLS analysis in an indoor heterogeneous VLC/RF network based on known and unknown CSI. IEEE Syst. J. (2020). https://doi.org/10.1109/JSYST.2020.2964033
24. Mostafa, A., Lampe, L.: Optimal and robust beamforming for secure transmission in MISO visible-light communication links. IEEE Trans. Signal
25. Yang, N., et al.: Physical layer security of TAS/MRC with antenna correlation. IEEE Trans. Inf. Forensics Security 8(1), 254–259 (2013)
26. He, B., Zhou, X.: Secure on-off transmission design with channel estimation errors. IEEE Trans. Inf. Foren. Security 8(12), 1923–1936 (2013)
27. Hu, J., et al.: On-off-based secure transmission design with outdated channel state information. IEEE Trans. Veh. Technol. 65(8), 6075–6088 (2016)
28. Estrada-Jiménez, J.C., et al.: Superimposed training-based channel estimation for MISO optical-OFDM VLC. IEEE Trans. Veh. Technol. 68(6), 6161–6166 (2019)
29. Ho, S., et al.: Coding and bounds for channel estimation in visible light communications and positioning. IEEE J. Sel. Areas Commun. 36(1), 34–44 (2018)
30. Sayli, O., et al.: On channel estimation in DC biased optical OFDM systems over VLC channels. In: 2016 International Conference on Advanced Technologies for Communications (ATC), pp. 147–151. IEEE, Piscataway (2016)
31. Gradshteyn, I.S., Ryzhik, I.M.: Table of Integrals, Series and Products, 6th edn. Academic Press, San Diego (2000)

How to cite this article: Ambrish, Garg P, Sharma PK, Gupta A. Secure information broadcasting analysis in an indoor VLC system with imperfect CSI. IET Commun. 2021;15:526–536. https://doi.org/10.1049/cmu2.12084