Optimization on Multiuser Physical Layer Security of Intelligent Reflecting Surface-Aided VLC

Shiyuan Sun, Fang Yang, *Senior Member, IEEE*, Jian Song, *Fellow, IEEE*, and Zhu Han, *Fellow, IEEE*

***Abstract*—This letter investigates physical layer security in intelligent reflecting surface (IRS)-aided VL communication (VLC). Under the point source assumption, we first elaborate the system model in the scenario with multiple legitimate users and one eavesdropper, where the secrecy rate maximization problem is transformed into an assignment problem by objective function approximation. Then, an iterative Kuhn-Munkres algorithm is proposed to optimize the transformed problem, and its computational complexity is in the second-order form of the numbers of IRS units and transmitters. Moreover, numerical simulations are carried out to verify the approximation performance and the VLC secrecy rate improvement by IRS.**

***Index Terms*—Visible light communication, intelligent reflecting surface, physical layer security, secrecy rate maximization.**

I. Introduction

As AN indispensable component of future wireless communication technologies, VL communication (VLC) has long been concerned by authoritative institutions such as the VLC Consortium (VLCC) and the hOME Gigabit Access project (OMEGA) [1], and its academic research and commercial progress are deepening. Generally, VLC shows outstanding advantages such as abundant frequency bandwidth, license-free merit, and low equipment cost [1]. Moreover, superior physical layer security in VLC, which is typically realized by effective beamforming schemes and/or jamming techniques at transmitters [2], is also a preponderance compared to radio frequency (RF) communications.

As a revolutionary technology, intelligent reflecting surface (IRS) provides a brand new perspective that physical security can be enhanced by actively re-directing the reflected signals. The physical principle of IRS lies in the manipulation of electromagnetic waves, and mainstream hardware architectures and channel models in the VL range have been investigated in [3]–[6]. As a sequel, there is a growing body of literature that studies the performance of IRS-aided VLC systems, including the outage probability reduction in mobile free-space optical communication [7], the blockage problem mitigation in single-transmitter single-user [8] and multi-transmitter multiuser scenarios [9], etc. In the area of physical layer security, a secrecy rate maximization problem is discussed for the IRS-aided VLC system [10], where the single-user single-transmitter scenario is considered and the optimization objective is the orientation of the mirror.

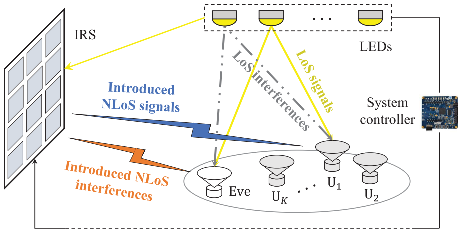


Fig. 1. The system model of the secure IRS-aided VLC.

This letter investigates the secrecy rate maximization problem of the IRS-aided VLC system, wherein multiple users are served by multiple transmitters and one of the legitimate users is monitored by an eavesdropper. Instead of optimizing the mirror orientation [10], our work adopts an additive channel model [6], through which the secrecy rate maximization process is transformed into an assignment problem. Then, the proposed iterative KM algorithm is utilized to reconfigure IRS, which is carried out by appropriately approximating the objective function and splitting the original problem into a sequence of subproblems. Moreover, numerical results are provided, showing that IRS can improve the secrecy rate of VLC systems compared to other baselines.

Notation: Symbols a (A), $\boldsymbol{a}$, and $\boldsymbol{A}$ represent the scalars, vectors, and matrices, respectively. Then, calligraphic letters $\mathcal{A}$ denote the defined index sets and $\mathbb{R}_+$ denote the real-valued and nonnegative number set. Moreover, $(\cdot)^T$, $\mathbb{I}(\cdot)$, $\lfloor\cdot\rfloor$, and $\lceil\cdot\rceil$ denote the transpose operator, the indicator function, the floor function, and the ceil function, respectively.

II. System Model

Consider a multiuser VLC system illustrated as Fig. 1, where Eve attempts to eavesdrop on a certain user and IRS is deployed to enhance system physical layer security. The light-of-sight (LoS) and non-LoS (NLoS) channel gains and received signals of both legitimate users and the eavesdropper are elaborated in the sequel of this section.

A. Channel Gain in Point Source Cases

1) LoS Path: In VLC, the LoS channel gain between the k-th photodetector (PD) and the l-th light-emitting diode (LED)

Manuscript received January 23, 2022; revised March 19, 2022; accepted April 9, 2022. Date of publication April 13, 2022; date of current version July 11, 2022. This work was supported in part by the National Natural Science Foundation of China under Grant 61871255; in part by the Beijing National Research Center for Information Science and Technology under Grant BNR2022RC01017; in part by the Fok Ying Tung Education Foundation; and in part by NSF under Grant CNS-2107216, Grant EARS-1839818, and Grant CNS-2128368. The associate editor coordinating the review of this article and approving it for publication was V. Bhatia. *(Corresponding author: Fang Yang.)*

Shiyuan Sun, Fang Yang, and Jian Song are with the Department of Electronic Engineering, Beijing National Research Center for Information Science and Technology, Tsinghua University, Beijing 100084, China, and also with the Key Laboratory of Digital TV System of Guangdong Province and Shenzhen City, Research Institute of Tsinghua University in Shenzhen, Shenzhen 518057, China (e-mail: sunsy20@mails.tsinghua.edu.cn; fangyang@tsinghua.edu.cn; jsong@tsinghua.edu.cn).

Zhu Han is with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77004 USA, and also with the Department of Computer Science and Engineering, Kyung Hee University, Seoul 446-701, South Korea (e-mail: zhan2@uh.edu).

Digital Object Identifier 10.1109/LWC.2022.3167108

generally follows the Lambertian model as [1]

$$h^{(1)}_{k,l} = \frac{A(m+1)}{2\pi d^2_{k,l}} \cos^m(\theta) g_{of} \cos(\phi) f(\phi), \tag{1}$$

where θ is the angle of irradiance, ϕ is the angle of incidence, and $f(\phi)$ is formulated by refractive index u and the semi-angle of the field-of-view (FoV) Φ [1]. Then, the parameters A, m, g_{of}, and $d_{k,l}$ represent the PD area, the Lambertian index, the optical filter gain, and the distance between the l-th transmitter and the k-th user, respectively.

2) NLoS Path: Given the negligible intensity level, the diffusely reflected path in IRS-aided VLC systems is generally ignored [4]–[7]. As for the specularly reflected path, some unique properties in the VL range are listed:

- The imaging method in geometric optics reveals that the reflected path can be regarded equivalently as emitted from the imaging transmitter [4], [5], and therefore the propagation direction of the NLoS path can be controlled by adjusting the reflector orientation.
- Considering the nanoscale wavelength of the VL, the near-field condition is guaranteed in the IRS-aided VLC systems [11]. Consequently, the upper bound of irradiance level at PD follows an "additive" model [6], instead of the "multiplicative" one in the far-field case [11].
- In point source cases, one tiny IRS unit can only serve an individual user at a time since the propagation direction of the reflected path strictly relies on the specular reflection law [9], and the location difference between transmitters will lead to misalignment at the target PD.

Based on the aforementioned discussions, an upper bound of the irradiance performance is derived under the point source assumption [6], leading to the NLoS channel gain as

$$h^{(2)}_{k,n,l} = \delta \frac{A(m+1)}{2\pi\big(d_{n,l} + d_{k,n}\big)^2} \cos^m(\theta) g_{of} \cos(\phi) f(\phi), \tag{2}$$

where δ is the reflectivity of each unit, and $d_{n,l}$ and $d_{k,n}$ are the distances between the l-th LED and the n-th IRS unit and the n-th unit and the k-th user, respectively.

B. Received Signals of Legitimate User and Eavesdropper

When an individual user k is served by the l-th transmitter, the received signal $\widehat{y}_{k,l}$ can be divided into three parts, namely the LoS component $\widehat{y}^{(1)}_{k,l}$, the NLoS component $\widehat{y}^{(2)}_{k,l}$, and the additive white Gaussian noise z_k, which is given by

$$\widehat{y}_{k,l} = \widehat{y}^{(1)}_{k,l} + \widehat{y}^{(2)}_{k,l} + z_k, \tag{3}$$

where z_k is zero mean with σ^2_k the variance of the noise.

1) Legitimate Users: Suppose the transmission symbols on LEDs are represented by the vector $\boldsymbol{x}^T = [x_1, x_2, \ldots, x_L]$, the LoS received signal is comprised of the intended information and the inter-user interferences. Given that the bandwidth of mainstream VLC systems is typically tens of MHz, the sampling interval is far larger than the delay spread, which determines that the baseband system in VLC can hardly distinguish multipath. Therefore, the received signal generally follows the single tap model as

$$\widehat{y}^{(1)}_{k,l} = \rho_k h^{(1)}_{k,l} P_l x_l + \rho_k \sum_{i=1, i\neq l}^{L} h^{(1)}_{k,i} P_i x_i, \tag{4}$$

where ρ_k and P_l denote the PD responsivity and the emission power, respectively. Without loss of generality, x_l is independent of each other and with the expectation of 1.

Then, a binary matrix $\boldsymbol{G} = [\boldsymbol{g}_1,\ \boldsymbol{g}_2, \ldots,\ \boldsymbol{g}_L]_{N\times L}$ is defined to describe the association relationship between IRS units and LEDs, after which each unit can reconfigure itself based on a reverse lookup table [9]. More specifically, the discrete element $g_{n,l} = 1$ and $g_{n,l} = 0$ indicate the cases that the n-th unit is and is not assigned to the l-th transmitter, respectively. Therefore, the NLoS gain of the k-th legitimate user equals the aggregate gains of reflected paths that are related to IRS units of the l-th LED, and it is given by

$$\widehat{y}^{(2)}_{k,l} = \rho_k \boldsymbol{h}^{(2)\,T}_{k,l} \boldsymbol{g}_l P_l x_l, \tag{5}$$

where a defined vector $\boldsymbol{h}^{(2)}_{k,l} = [h^{(2)}_{k,1,l}, h^{(2)}_{k,2,l}, \ldots, h^{(2)}_{k,N,l}]^T \in \mathbb{R}^{N\times 1}_{+}$ is introduced to simplify the discussions.

2) Eavesdropper: Different from the traditional RF communications, the intensity modulation and direct detection (IM/DD) scheme in VLC is based on the received light intensity, and the lack of phase information makes it impossible to eliminate the eavesdropper signal by destructive interference. Nevertheless, we attempt to degrade the signal-to-interference-plus-noise ratio (SINR) of the eavesdropper by purposely introducing an unintended interference, which can be implemented since the specularly reflected light is easy to be re-directed. Compared to the legitimate users, the eavesdropper is considered as a special element with a vector $\boldsymbol{g}_0 \in \{0,1\}^{N\times 1}$ recording its IRS assignment situation. Once $g_{n,0} = 1$ ensures, the n-th unit will adjust itself so that the light of the LED, which carries an unintended signal and is closest to the eavesdropper, can be reflected and propagate to the eavesdropper. Therefore, the NLoS signal of Eve performs as the introduced interference, which can be expressed as

$$\widehat{y}^{(2)}_{E,l} = \rho_E \boldsymbol{h}^{(2)\,T}_{E,l_c} \boldsymbol{g}_0 P_{l_c} x_{l_c}, \tag{6}$$

where l_c is the index of the complementary transmitter to the l-th LED, i.e., the l_c-th LED carries the unintended signal and has the shortest distance to the eavesdropper.

III. Optimization of Overall Secrecy Rate

A. Problem Formulation

Considering the constraints of emission power limitation and real-valued and nonnegative amplitude, the capacity-achieving input distribution in VLC is discrete instead of in a typical Shannon capacity form. Nevertheless, a lower bound of dimmable channel capacity is proposed in [12], where the capacity function is given by

$$C_{k,l} = \frac{1}{2} W \log_2\Big(1 + \frac{e}{2\pi}\gamma_{k,l}\Big), \tag{7}$$

where e and W represent the value of the base of natural logarithms and the bandwidth, respectively. The individual SINR of the k-th user is denoted by

$$\gamma_{k,l} = \frac{\rho^2_k \Big(h^{(1)}_{k,l} + \boldsymbol{h}^{(2)\,T}_{k,l} \boldsymbol{g}_l\Big)^2 P^2_l}{I_{k,l}}, \tag{8}$$

where LoS interference plus noise power is expressed as

$$I_{k,l} = \sigma^2_k + \rho^2_k \sum_{i=1, i\neq l}^{L} h^{(1)2}_{k,i} P^2_i. \tag{9}$$

This letter endeavors to maximize the expectation of multiuser secrecy rate for IRS-aided VLC systems. To this end, the probability that the *k*-th user served by the *l*-th transmitter is denoted by a constant $f_{l,k}$ within the coherent time, which satisfies the equation $\sum_{k=1}^{K} f_{l,k} = 1$ according to the properties of the probability function. Consequently, the upper bound of the eavesdropper capacity is given by

$$C_E = \sum_{l=1}^{L} \frac{f_{l,k^*} W}{2} \log_2 \left(1 + \frac{\rho_E^2 h_{E,l}^{(1)2} P_l^2 e/2/\pi}{I_{E,l} + \rho_E^2 P_{l_c}^2 \left(\boldsymbol{h}_{E,l_c}^{(2)\,T} \boldsymbol{g}_0 \right)^2} \right), \tag{10}$$

where k^* is the user index concerned by the eavesdropper. To sum up, the overall secrecy rate is derived by [13]

$$C_S = \sum_{k=1}^{K} \sum_{l=1}^{L} f_{l,k} C_{k,l} - C_E, \tag{11}$$

and the secrecy rate maximization problem is formulated as

$$\mathbf{P}\colon \max_{\widetilde{\boldsymbol{G}}} \quad C_S(\widetilde{\boldsymbol{G}}) \tag{12}$$

$$\text{s.t.} \quad \widetilde{g}_{n,l} \in \{0,1\}, \qquad \forall n \in \mathcal{N}, l \in \mathcal{L} \cup \{0\}, \tag{13}$$

$$\sum_{l=0}^{L} \widetilde{g}_{n,l} = 1, \qquad \forall n \in \mathcal{N}, \tag{14}$$

$$\sum_{n=1}^{N} \widetilde{g}_{n,l} \geq \left\lfloor \frac{N}{L+1} \right\rfloor, \quad \forall l \in \mathcal{L} \cup \{0\}, \tag{15}$$

where $\widetilde{\boldsymbol{G}} = [\boldsymbol{g}_0, \boldsymbol{G}]$ denotes an aggregate matrix, and $\mathcal{L}$ and $\mathcal{N}$ indicate the index sets of the transmitters and the IRS units, respectively. Then, the constraints in (13) and (14) come from the definitions of $\boldsymbol{G}$ and $\boldsymbol{g}_0$, and the constraint in (15) aims to guarantee the fairness of the IRS configuration process.

B. Proposed Algorithm to Maximize the Secrecy Rate

Mathematically, $\mathbf{P}$ is a non-deterministic polynomial-time (NP) hard problem. To reduce the complexity, a relaxing greedy algorithm is proposed to maximize the achievable sum rate of intended users [9], wherein one of the subproblems is proved to be asymptotically convex. However, such an optimization algorithm cannot be directly used in $\mathbf{P}$ since the term of eavesdropper rate destroys the structure of the objective function. Furthermore, considering the numbers of IRS units can be large, an algorithm with controllable complexity is desirable in dealing with the time-variant environment.

Based on the characteristics of the objective function and constraints, $\mathbf{P}$ can be reanalyzed from a discrete perspective, i.e., how to assign the *n*-th IRS unit to one of the $L + 1$ targets (transmitters or eavesdropper) on the premise of fairness. The limitation is that variables are coupled together in C_S, leading to the difficulty to analyse the variation of secrecy rate. However, the capacity formulas in (7) and (10) are exactly in the logarithmic form, which hints that they can be transformed into the form of linear combination by proper approximation.

Lemma 1: The function $\eta(x^*)\log(x) + \xi(x^*)$ is a tight lower bound of $\log(1 + x)$, where η and ξ are coefficients with respect to the tangent point x^* [14].

Given Lemma 1, the capacity of the legitimate user can be approximated at $\gamma_{k,l}$ as

$$\begin{aligned} \frac{C_{k,l}}{W} &\approx \eta_k \log_2 \sqrt{\frac{\rho_k^2 \left(h_{k,l}^{(1)} + \boldsymbol{h}_{k,l}^{(2)\,T} \boldsymbol{g}_l \right)^2 P_l^2}{2\pi I_{k,l}/e}} + \frac{\xi_k}{2} \\ &= \eta_k \log_2 \left(1 + \frac{\boldsymbol{h}_{k,l}^{(2)\,T} \boldsymbol{g}_l}{h_{k,l}^{(1)}} \right) + \frac{\eta_k \log_2 \Gamma_{k,l} + \xi_k}{2}, \end{aligned} \tag{16}$$

where η_k and ξ_k are functions of $\gamma_{k,l}$ [14] and $\Gamma_{k,l} = e\rho_k^2 h_{k,l}^{(1)2} P_l^2/(2\pi I_{k,l})$ denotes the LoS component of individual SINR. Then, the logarithmic term can be further approximated by the first-order Taylor polynomial as [15]

$$\frac{C_{k,l}}{W} \approx \eta_k \frac{\boldsymbol{h}_{k,l}^{(2)\,T} \boldsymbol{g}_l - \lambda_k h_{k,l}^{(1)}}{(1+\lambda_k) h_{k,l}^{(1)} \ln 2} + \log_2 \sqrt{2^{\xi_k} \Gamma_{k,l}^{\eta_k} (1+\lambda_k)^{2\eta_k}}, \tag{17}$$

where the expansion point is determined with the average term $\lambda_k = \sum_{n=1}^{N} \sum_{l=1}^{L} h_{k,n,l}^{(2)} / \sum_{l=1}^{L} h_{k,l}^{(1)}/L$. According to Lagrange's form of the remainder, the residual of (17) follows the magnitude of $(\boldsymbol{h}_{k,l}^{(2)\,T} \boldsymbol{g}_l / h_{k,l}^{(1)} - \lambda_k)^2$, which is negligible to the first-order term since LoS channel gain far exceeds NLoS gain in VLC and therefore $\boldsymbol{h}_{k,l}^{(2)\,T} \boldsymbol{g}_l / h_{k,l}^{(1)}$ is a small quantity.

Similarly, the capacity of the eavesdropper is rewritten as

$$\begin{aligned} \frac{-C_E}{W} &\approx -\sum_{l=1}^{L} \eta_E f_{l,k^*} \log_2 \sqrt{\frac{e\rho_E^2 h_{E,l}^{(1)2} P_l^2/(2\pi)}{I_{E,l} + \rho_E^2 P_{l_c}^2 \left(\boldsymbol{h}_{E,l_c}^{(2)\,T} \boldsymbol{g}_0 \right)^2}} + \frac{\xi_E f_{l,k^*}}{2} \\ &= \sum_{l=1}^{L} \eta_E f_{l,k^*} \log_2 \sqrt{1 + \frac{\left(\boldsymbol{h}_{E,l_c}^{(2)\,T} \boldsymbol{g}_0 \right)^2}{I_{E,l}/\rho_E^2/P_{l_c}^2}} - f_{l,k^*} \log_2 \sqrt{2^{\xi_E} \Gamma_{E,l}^{\eta_E}} \\ &\overset{(a)}{\approx} \sum_{l=1}^{L} f_{l,k^*} \frac{\eta_E \rho_E^2 P_{l_c}^2 \Delta}{2 I_{E,l} \ln 2} \boldsymbol{h}_{E,l_c}^{(2)\,T} \boldsymbol{g}_0 - f_{l,k^*} \log_2 \sqrt{2^{\xi_E} \Gamma_{E,l}^{\eta_E}}, \end{aligned} \tag{18}$$

where (*a*) satisfies due to the first-order Taylor expansion at the point 0 and Δ is a constant quantity of the same order of magnitude as $\boldsymbol{h}_{E,l_c}^{(2)\,T} \boldsymbol{g}_0$. With proper approximations, the overall secrecy rate can be linearly divided into the NLoS components and LoS direct bias as

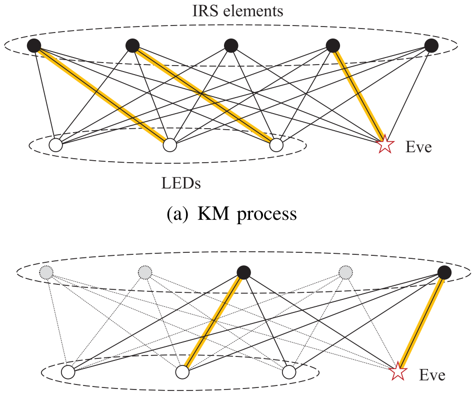
$$\widehat{C}_S(\widetilde{\boldsymbol{G}}) = \sum_{n=1}^{N} \sum_{l=0}^{L} w_{n,l} \widetilde{g}_{n,l} + Q, \tag{19}$$

where the bias term Q results from the constant parts in (16) and (18), and the coefficients $w_{n,l}$ can be formulated as

$$\begin{aligned} w_{n,l} &= \mathbb{I}(l > 0) \sum_{k=1}^{K} \frac{\eta_k W f_{l,k} h_{k,n,l}^{(2)}}{h_{k,l}^{(1)} \ln 2} \\ &\quad + \mathbb{I}(l = 0) \sum_{i=1}^{L} \frac{\eta_E f_{i,k^*} W \rho_E^2 P_{i_c}^2 h_{E,n,i_c}^{(2)}}{2 I_{E,i} \ln 2} \Delta. \end{aligned} \tag{20}$$

where the index of the complementary transmitter to the *i*-th LED is denoted by i_c, and $\Delta = \sum_{n=1}^{N} \sum_{l=1}^{L} h_{E,n,l}^{(2)}/L^2$.

Consequently, the secrecy rate maximization process is transformed into an optimal matching search in a bipartite graph, wherein two index sets are $\mathcal{N}$ and $\mathcal{L} \cup \{0\}$. The KM



(a) KM process

(b) Delete the selected vertices

Fig. 2. The sketch map of the proposed iterative KM algorithm.

Algorithm 1 Proposed Iterative KM Algorithm

```
Input: $h^{(1)}_{k,l}$, $h^{(2)}_{k,n,l}$, $t \leftarrow 0$.
Output: $\widetilde{G}$.
repeat
    Calculate ($\eta_k$, $\xi_k$, $\eta_E$, $\xi_E$) as Lemma 1 and $t \leftarrow 0$;
    Calculate the rate bias $Q$ according to (16) and (18);
    Generate the weight matrix $W$ according to (20);
    repeat
        Run the KM algorithm;
        $g_{n,l} \leftarrow 1$ for the selected edges;
        Delete these vertices and their related edges;
        $t \leftarrow t + 1$
    until $N \leq t(L + 1)$
until Convergence
```

algorithm can generally achieve the global optimal solution of such bipartite problems, but the maximum number of matching edges in the KM algorithm is min(N, L + 1). To ensure the fairness constraint in (15), we propose an iterative KM algorithm to solve the modified **P**. As shown in Algorithm 1, the weight matrix W and rate bias term Q are calculated before the assignment. Then, the KM algorithm is carried out in each loop t, after which the indices of selected IRS units and their corresponding edges are deleted as illustrated in Fig. 2. This process will go on till the number of remaining IRS units is a negative number, and the above steps correspond to one time of assignment. Considering the IRS configuration result affects the individual SINR conversely, the unit assignment and approximate parameters need to be conducted alternatively until convergence, i.e., the matrix $\widetilde{\boldsymbol{G}}$ remains unchanged. Moreover, the proposed algorithm will inevitably end since there are at most $\lceil N/(L+1) \rceil$ KM algorithm calls in each assignment.

C. Analyses on Optimality and Complexity

1) Global Optimality Analysis: The result of Algorithm 1 will naturally satisfy the fairness constraint (15) due to the iterative process. Then, the analysis on the optimality of the proposed algorithm is given as follows.

Lemma 2: The KM algorithm obtains the optimal matching result of the weighted bipartite graph [16].

Proposition 1: The proposed iterative KM algorithm will achieve the optimal result of the approximate rate function.

Proof: If each element in $\mathcal{L} \cup \{0\}$ has up to one matching edge, the proposed algorithm will achieve the optimal result according to Lemma 2. Suppose the optimality ensures when the number of matching edges for an element is J, i.e., the total matched edges is $J(L + 1)$. Then, when the number goes to J + 1, the optimality of the proposed algorithm still holds because the KM algorithm can obtain the optimal matching result in each assignment. ■

TABLE I
SIMULATION PARAMETERS

$K = 4$	$L = 4$	$W = 20$ MHz	$\delta = 0.5$
$g_{of} = 1$	$m = 1$	$A = 4$ cm^2	$\rho_k = 0.5\ A/W$
$\Phi = 80°$	$u = 1.5$	$D = 100$ cm^2	$\sigma^2 = 10^{-10}\ W$

2) Complexity Analysis: According to (20), the calculations of the weighted matrix and direct bias lead to a complexity of $\mathcal{O}(NLK)$. In the t-th loop, the KM algorithm is processed on a bipartite graph composed of two sets of L + 1 points and N − t(L + 1) points. Each loop has a complexity of $\mathcal{O}(N(L+1)^2 - t(L+1)^3)$ [16] and the proposed algorithm conducts till $t = \lceil N/(L+1) \rceil$. Therefore, the computational complexity of Algorithm 1 is given by

$$\begin{aligned}&\sum_{t=0}^{\lceil N/(L+1)\rceil-1} T\Big\{N(L+1)^2 - t(L+1)^3\Big\}\\&= T(L+1)^2\left\lceil\frac{N}{L+1}\right\rceil\left\{N-\frac{L+1}{2}\left(\left\lceil\frac{N}{L+1}\right\rceil-1\right)\right\}\\&\approx \frac{TNL(N+L)}{2},\end{aligned} \qquad (21)$$

where T denotes the time of assignments. Notably, the time consumption is proportional to the quadratic power of N and L, which is far lower than the exhaustive search method with the complexity of $\mathcal{O}((L+1)^N)$.

IV. NUMERICAL RESULTS

In this section, we provide simulation results to testify the previous theoretical analyses. Specifically, four LEDs located at (1m, 1m, 3m), (1m, 7m, 3m), (7m, 1m, 3m), and (7m, 7m, 3m) are transmitters in an 8m × 8m × 3m room, and users are distributed randomly in the plane 0.5m above the ground. Considering that indoor mobile velocity is far slower than the channel acquisition rate, the user-mobility can be regarded as a series of quasi-static moments, where the channel gain is deterministic by the user location. For each transmitter, its service probability for a certain user is inversely proportional to the square of transceiver distances. Then, a planar IRS with unit area D is deployed on the wall, and its horizontal and vertical margins are 1m and 0.3m, respectively. Moreover, the spacing between two IRS units is set as 20cm, and more detailed parameters are given in Table I.

To start with, the numerical simulation is executed to evaluate the performance of the proposed algorithm as well as the correctness of functions approximation in (16) and (18). Without loss of generality, four users are located at (3.6m, 2.7m, 0m), (1.0m, 3.3m, 0m), (3.0m, 4.5m, 0m), and (6.4m, 2.2m, 0m), where the first one is eavesdropped by Eve located at (2.1m, 1.5m, 0m). The emission power on LEDs varies from 0 dBW to 10 dBW, and benchmarks are given by:

1) Approximation Secrecy Rate: Assign IRS units according to Algorithm 1 and obtain the approximate result $\widehat{C}_S(\widetilde{\boldsymbol{G}})$.

2) Proposed Algorithm With & Without Eve's SINR: For these two schemes, the secrecy rate functions in (18) are approximated at real SINR and a random point, respectively.

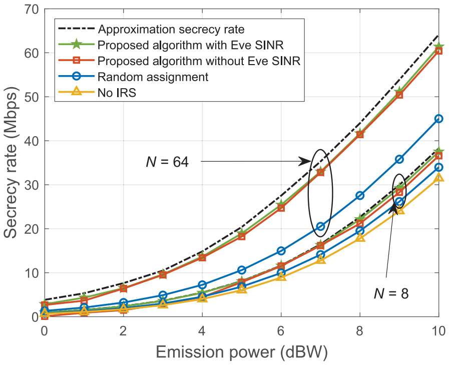


Fig. 3. The performance of proposed algorithm compared with other baselines.

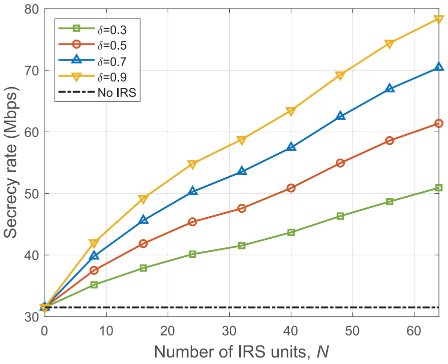


Fig. 4. The secrecy rate versus the number of IRS units under different reflectivity.

Then, IRS units are assigned according to Algorithm 1 and the secrecy rate herein is calculated by (11).

3) Random Assignment: Assign all IRS units equally among different columns so that each of them has nearly $N/(L+1)$ ones. Then, the variable $\widetilde{\boldsymbol{G}}$ is scrambled and randomly rearranged according to rows. For accuracy, the secrecy rate is calculated by averaging 200 independent trials.

4) No IRS: Obtain the secrecy rate with $\widetilde{\boldsymbol{G}} = \mathbf{0}$.

As shown in Fig. 3, the proposed approximation method is considerably tight to the capacity formula in (11), and the rate gap becomes large when N increases from 8 to 64. This is because steps in (17) and (18) generate non-negligible errors with the increase of N. Notably, the VLC system security benefits a lot from the deployed IRS. When the emission power is 10 dBW, the surface with $N = 64$ units can achieve nearly 30 Mbps gain compared to the case without IRS, and even the random assignment scheme improves the secrecy rate by 15 Mbps. Nevertheless, the rate gain obtained by IRS is much smaller when $N = 8$, i.e., less than 8 Mbps at 10 dBW power, which reveals that the secrecy improvement performance is sensitive to the number of IRS units. Moreover, the results also show that the proposed algorithm has less SINR requirement for the eavesdropper, namely the tangent point of η_E and ξ_E will not significantly affect the secrecy rate. This can be explained by the closeness between the approximate function and the original rate function in Lemma 1.

Numerical simulations are carried out in Fig. 4 to investigate the influence of reflectivity as well as the number of IRS units. The emission power herein is 10 dBW, and N increases from 0 to 64 under certain reflectivity values. It can be seen from the result that there is a positive correlation between the overall secrecy rate and N, e.g., the rate when $\delta = 0.5$ and $N = 64$ is doubled compared to no IRS case. Besides, the numerical results show that a higher secrecy rate can also be achieved with large δ, i.e., the case with $\delta = 0.7$ and $N = 8$ and the one with $\delta = 0.3$ and $N = 24$ both correspond to the overall secrecy rate of 40 Mbps. This phenomenon suggests that the secrecy rate can be increased by cooperatively determining the values of reflectivity and the number of IRS units.

V. Conclusion

An IRS-aided secure VLC system is modeled in this letter, wherein one legitimate user is monitored by an eavesdropper. By appropriately approximating the objective function and splitting the problem, the process of secrecy rate maximization is transformed into a sequence of assignment subproblems, and then the IRS configuration matrix is optimized by the proposed iterative KM algorithm. Numerical results show that the secrecy rate has been prominently improved by IRS, and the rate gain is nearly proportional to the number of units and reflectivity. Furthermore, the utilization of IRS enhances the physical layer security of VLC, showing enormous potentials of IRS for future academic research.

References

[1] P. H. Pathak, X. Feng, P. Hu, and P. Mohapatra, "Visible light communication, networking, and sensing: A survey, potential and challenges," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2047–2077, 4th Quart., 2015.

[2] N. Su, E. Panayirci, M. Koca, A. Yesilkaya, H. V. Poor, and H. Haas, "Physical layer security for multi-user MIMO visible light communication systems with generalized space shift keying," *IEEE Trans. Commun.*, vol. 69, no. 4, pp. 2585–2598, Apr. 2021.

[3] G. K. Shirmanesh, R. Sokhoyan, P. C. Wu, and H. A. Atwater, "Electro-optically tunable multifunctional metasurfaces," *ACS Nano*, vol. 14, no. 6, pp. 6912–6920, Jun. 2020.

[4] M. Najafi and R. Schober, "Intelligent reflecting surfaces for free space optical communications," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Waikoloa, HI, USA, Dec. 2019, pp. 1–7.

[5] M. Najafi, B. Schmauss, and R. Schober, "Intelligent reflecting surfaces for free space optical communication systems," *IEEE Trans. Commun.*, vol. 69, no. 9, pp. 6134–6151, Sep. 2021.

[6] A. M. Abdelhady, A. K. S. Salem, O. Amin, B. Shihada, and M.-S. Alouini, "Visible light communications via intelligent reflecting surfaces: Metasurfaces vs mirror arrays," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1–20, 2021.

[7] H. Wang *et al.*, "Performance analysis of multi-branch reconfigurable intelligent surfaces-assisted optical wireless communication system in environment with obstacles," *IEEE Trans. Veh. Technol.*, vol. 70, no. 10, pp. 9986–10001, Oct. 2021.

[8] S. Aboagye, T. M. N. Ngatched, O. A. Dobre, and A. R. Ndjiongue, "Intelligent reflecting surface-aided indoor visible light communication systems," *IEEE Commun. Lett.*, vol. 25, no. 12, pp. 3913–3917, Dec. 2021.

[9] S. Sun, F. Yang, and J. Song, "Sum rate maximization for intelligent reflecting surface-aided visible light communications," *IEEE Commun. Lett.*, vol. 25, no. 11, pp. 3619–3623, Nov. 2021.

[10] L. Qian, X. Chi, L. Zhao, and A. Chaaban, "Secure visible light communications via intelligent reflecting surfaces," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Montreal, QC, Canada, Jun. 2021, pp. 1–6.

[11] W. Tang *et al.*, "Wireless communications with reconfigurable intelligent surface: Path loss modeling and experimental measurement," *IEEE Trans. Wireless Commun.*, vol. 20, no. 1, pp. 421–439, Jan. 2021.

[12] J.-B. Wang, Q.-S. Hu, J. Wang, M. Chen, and J.-Y. Wang, "Tight bounds on channel capacity for dimmable visible light communications," *J. Lightw. Technol.*, vol. 31, no. 23, pp. 3771–3779, Dec. 1, 2013.

[13] A. Mostafa and L. Lampe, "Physical-layer security for MISO visible light communication channels," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 9, pp. 1806–1818, Sep. 2015.

[14] J. Papandriopoulos, S. Dey, and J. Evans, "Optimal and distributed protocols for cross-layer design of physical and transport layers in MANETs," *IEEE/ACM Trans. Netw.*, vol. 16, no. 6, pp. 1392–1405, Dec. 2008.

[15] A. Wiesel, "Unified framework to regularized covariance estimation in scaled Gaussian models," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 29–38, Jan. 2012.

[16] L. Wang and H. Wu, "Fast pairing of device-to-device link underlay for spectrum sharing with cellular users," *IEEE Commun. Lett.*, vol. 18, no. 10, pp. 1803–1806, Oct. 2014.