




Article

Reconfigurable Intelligent Surface-Aided Security Enhancement for Vehicle-to-Vehicle Visible Light Communications

Xiaoqiong Jing ^{1,*} , Yating Wu ^{1,*} , Fei Yu ^{2,*}, Yuru Xu ¹ and Xiaoyong Wang ³ 

¹ Key Laboratory of Specialty Fiber Optics and Optical Access Networks, Shanghai Institute for Advance Communication and Data Science, Shanghai University, Shanghai 200444, China; jingxq@shu.edu.cn (X.J.); xv_yuru@shu.edu.cn (Y.X.)

² School of Electronic and Communication Engineering, Shenzhen Polytechnic University, Shenzhen 518055, China

³ CASCO Signal Ltd., Shanghai 200072, China; wangxiaoyong@casco.com.cn

* Correspondence: ytwu@shu.edu.cn (Y.W.); yufei198275@szpu.edu.cn (F.Y.)

Abstract: Vehicle-to-vehicle (V2V) visible light communication (VLC) systems are increasingly being deployed for real-time data exchange in intelligent transportation systems (ITS). However, these systems are highly vulnerable to eavesdropping, especially in scenarios such as road intersections where signals may be exposed to unauthorized receivers. To address these security challenges, we propose a novel reconfigurable intelligent surface (RIS)-assisted security enhancement scheme for V2V VLC networks. The proposed scheme leverages RIS to improve the reception of legitimate signals at the destination vehicle while simultaneously introducing artificial noise (AN) to interfere with potential eavesdroppers. Optimization problems are formulated to maximize the SINR of the destination vehicle and simultaneously minimize the worst-case SINR of eavesdroppers. The simulation results demonstrate that the proposed scheme achieves a notable improvement in the system's secrecy rate by 1.64 bit/s/Hz and enhances the overall security performance, offering a robust solution to the security challenges in V2V VLC systems.

Keywords: visible light communication (VLC); reconfigurable intelligent surface (RIS); vehicle-to-vehicle (V2V); physical layer security (PLS)



Citation: Jing, X.; Wu, Y.; Yu, F.; Xu, Y.; Wang, X. Reconfigurable Intelligent Surface-Aided Security Enhancement for Vehicle-to-Vehicle Visible Light Communications. *Photonics* **2024**, *11*, 1151. <https://doi.org/10.3390/photonics11121151>

Received: 28 October 2024
Revised: 29 November 2024
Accepted: 4 December 2024
Published: 6 December 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

In modern transportation systems, critical issues such as traffic congestion, traffic accidents, and pollution have become increasingly severe [1]. To address these challenges, vehicle-to-vehicle (V2V) communication as an integral component of intelligent transportation systems (ITS) [2] plays a pivotal role in enhancing road safety by enabling the real-time exchange of traffic and road information between vehicles [3].

Currently, V2V data transmission primarily relies on radio frequency (RF) technologies. However, the low reliability and high latency associated with vehicular RF technology make V2V communication susceptible to disruptions, including adversarial attacks that block or interfere with vehicle communication [4]. As an alternative, visible light communication (VLC) has emerged as a cost-effective solution for establishing V2V communication. With inherent characteristics such as low power consumption, wide free spectrum, enhanced security, and resistance to electromagnetic interference, VLC is an ideal candidate for future ITS systems [5–7]. V2V VLC utilizes light-emitting diodes (LEDs) from the existing vehicle headlights as transmitters and photodetectors (PDs) or cameras as receivers [8], providing high data rate communication and illumination simultaneously. Compared to vehicular RF systems, V2V VLC systems offer enhanced security as light cannot penetrate non-transparent obstacles. This physical limitation confines data transmission to a restricted area, reducing the risk of interception by attackers [9].

Nevertheless, due to the open broadcast nature of light, potential eavesdroppers can intercept confidential signals intended for legitimate users in open environments [10]. This risk is particularly acute when vehicles are turning at road intersections where signals may unintentionally be exposed to unauthorized receivers. Moreover, V2V VLC systems rely on a direct line-of-sight (LoS) for effective communication [11]. During turns, the LoS path can be blocked as the angle between the transmitting and receiving vehicles shifts. Specifically, when vehicles turn at intersections or curves, the headlights may no longer be aimed directly at the intended recipient. The misalignment of transmitting light sources and receiving ends weakens the signal or disrupts data transmission, affecting the sharing of real-time information. Additionally, the data-carrying light source may leak in other directions, allowing nearby eavesdroppers to intercept sensitive information.

Traditional security solutions are typically implemented at the upper layers of communication systems, including access control, password protection, and end-to-end encryption. In addition to cryptographic algorithms and authentication protocols at MAC or higher layers [12,13], physical layer security (PLS) offers a secure foundation for a robust network, which is transparent across various types of data. PLS techniques complement traditional cryptographic methods by leveraging the inherent characteristics of wireless communication channels, thus strengthening the overall security framework [14].

Recently, the reconfigurable intelligent surface (RIS) has attracted considerable attention due to its ability to dynamically control the wireless propagation environment. The RIS consists of a programmable metasurface composed of smart, controllable reflecting units, where the reflection coefficients and orientation of each RIS unit can be dynamically adjusted through an intelligent controller [15]. The RIS has been widely adopted in wireless communication systems to enhance performance and security. For instance, the authors of [16] explore PLS enhancement in hybrid RIS-assisted multiple-input multiple-output (MIMO) systems. In [17], a deep learning-based end-to-end optimization framework is proposed for near-field wideband beamforming in RIS-assisted MIMO systems. While in [18], the authors develop an analytical framework for sub-array partitioning to improve modeling efficiency and maintain accuracy in RIS-enabled UAV-to-vehicle communication scenarios. Furthermore, the authors of [19] provided a stochastic geometry-based analytical framework to analyze the performance of RIS-aided hybrid vehicular VLC/RF communication networks. While previous studies on the RIS-based V2V VLC system mainly focus on the bit error rate (BER) performance, outage probability, and throughput, there has been limited investigation into the PLS of the V2V VLC system using RIS. The design and implementation of RIS-aided PLS in the V2V VLC system still require further investigation.

In recent years, there have also been several studies focusing on secure VLC using RIS. The authors of [20] investigate the PLS of an indoor VLC system assisted by a RIS, optimizing the secrecy rate by intelligently controlling the orientation of each mirror. While in [21], the PLS of a RIS-assisted VLC/RF hybrid network is analyzed. It should be noted that the RIS in [21] operates under RF channels rather than VLC channels with the primary objective of providing wide coverage rather than directly improving security.

In this article, our study addresses the under-investigated domain of PLS in RIS-aided V2V VLC systems. The novelty of our work lies in introducing a strategy that combines artificial noise (AN) with the RIS to jointly optimize the associated coefficients of the RIS and the design of the AN. Specifically, the RIS is employed to enhance the reception of legitimate signals at the destination vehicle by strategically reflecting and reinforcing the useful signal paths. Simultaneously, AN is introduced to disrupt the reception of potential eavesdroppers by creating additional interference. The joint optimization strikes a balance between signal enhancement for legitimate vehicles and interference for unauthorized interceptors, ultimately improving the overall security of the V2V VLC system.

The rest of the paper is organized as follows. Section 2 describes the system model and the proposed RIS-based AN scheme. Section 3 presents the formulation of the optimization problems and the process of solving them. Section 4 analyzes the numerical results and provides an insightful discussion. Finally, concluding remarks are summarized in Section 5.

2. System Model

Consider a road intersection scenario of a V2V VLC system in vehicular networks, as shown in Figure 1. At the road intersection, when a vehicle makes a turn, the light source carrying the data may no longer be directed at the intended receiving vehicle and can instead leak in other directions. As the light strays from the receiving vehicle’s sensors, a nearby eavesdropper may intercept the leaked signals, potentially gaining access to the sensitive information transmitted between cars. This risk is particularly high during turns or navigating curves where communication signals may unintentionally become exposed to unauthorized receivers.

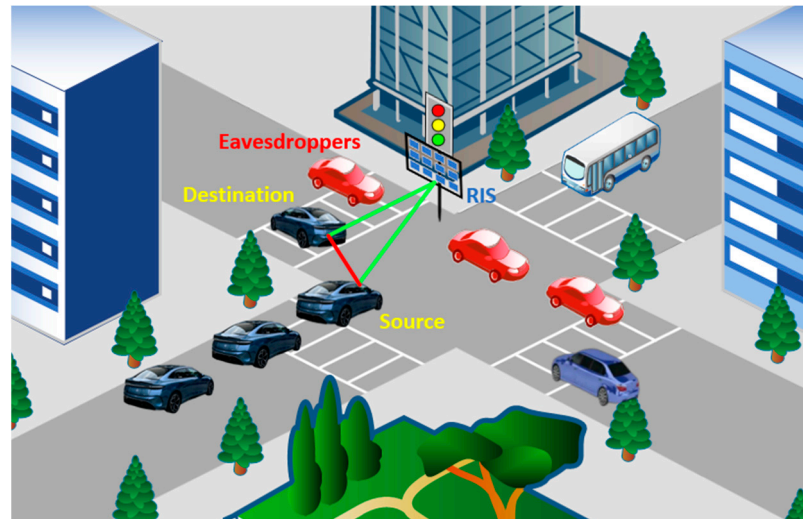


Figure 1. Illustration of RIS-based V2V VLC system at road intersection.

For practical implementation, the RIS can be integrated with the existing infrastructure, such as roadside poles or overhead gantries commonly used for mounting traffic lights or road signs. This placement ensures compatibility with typical traffic configurations while enhancing the confidential signal reception of the destination vehicle, thereby providing a more reliable and stronger communication link. It is assumed that the source vehicle communicates with the affected LoS link (red solid line) and the non-line-of-sight (NLoS) link through the RIS (green solid line). Potential eavesdroppers are positioned near the destination vehicle.

In the proposed system, the allocation of RIS resources is dynamically managed by a central controller, which coordinates communication based on the real-time positions and channel conditions of the registered vehicles. Authorized users are authenticated through the vehicular communication network, which enables secure access to the RIS-assisted VLC system. These users actively participate in the communication process and adhere to predefined protocols for channel estimation and resource allocation. Eavesdroppers, on the other hand, are unauthorized entities without access to the authentication and coordination mechanisms of the system.

Figure 2 portrays a simplified abstraction model of the proposed scenario. The source vehicle is equipped with N LEDs that work together to send the confidential signals required by the destination vehicle. The destination vehicle detects the LED transmission signals and decodes the corresponding information through K PDs or camera image sensors. The destination vehicle and M eavesdroppers are located on the vertical road, while the specific position of the eavesdropping vehicle is random. In addition, an RIS consisting of L units is deployed on traffic lights to enhance communications, and the orientation of each RIS unit can be adjusted individually. The number of RIS units can be adjusted, enabling scalable implementations that achieve a balance between performance and size to meet specific application requirements and physical constraints in real-world road environments. Furthermore, ongoing research and advancements in RIS technology are expected to drive

significant progress in miniaturization, making smaller more practical implementations feasible in the future.

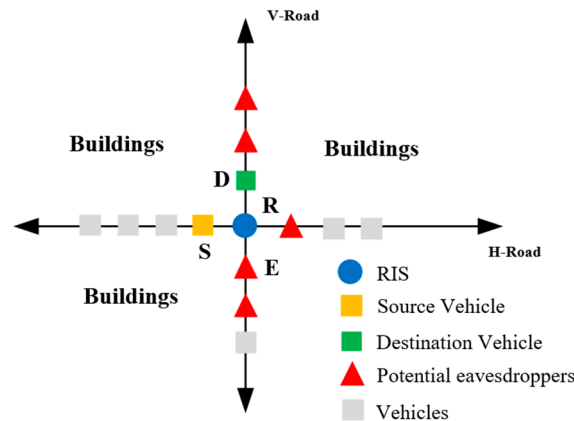


Figure 2. Abstraction system model of the intersection scenario.

2.1. Channel Model

In this paper, LEDs are used as the vehicular light sources. The radiation pattern of the vehicular light sources is simulated using the Lambertian model, which is adopted in vehicular VLC systems due to its convenient approximation for analysis [19,22–24]. Although this work employs the Lambertian model for analytical simplicity, the proposed RIS deployment strategy is flexible and remains applicable to alternative models, such as the Gaussian angular distribution model and the empirical models described in [25,26]. Future work can extend our framework to incorporate more realistic light patterns derived from experimental measurements or advanced vehicular lighting models. These refinements would enable more precise modeling of the LoS and NLoS propagation paths, ultimately enhancing the practical applicability of the proposed scheme in vehicular scenarios.

2.1.1. LoS Path

The channel gain vector of the LoS link is denoted as $\mathbf{h}_{SD,k}^{(1)} = [h_{1,k}^{(1)}, \dots, h_{N,k}^{(1)}]^T$. The LoS channel gain between the n -th LED and the k -th PD is given by [27]

$$h_{n,k}^{(1)}(\phi, \psi) = \eta \zeta \frac{(m+1)A_{PD}}{2\pi d^2} \cos^m(\phi) T(\psi) G(\psi) \cos(\psi) \quad (1)$$

where η is the LED conversion factor and ζ is the responsivity of the PD. A_{PD} is the physical area of the PD and d is the distance between the n -th LED and the k -th PD. m is the Lambertian index calculated by $m = -\ln 2 / \ln(\cos \theta_{1/2})$ and $\theta_{1/2}$ denotes the half-intensity radiation angle. ϕ and ψ are the angles of irradiance and incidence, $T(\psi)$ is the optical filter gain, and $G(\psi)$ is the optical concentrator gain, which can be expressed as

$$G(\psi) = \begin{cases} \frac{\kappa^2}{\sin^2 \psi_{FOV}}, & 0 \leq \psi \leq \psi_{FOV} \\ 0, & \psi > \psi_{FOV} \end{cases} \quad (2)$$

where κ is the refractive index and ψ_{FOV} is the half angle of the receiver PD's field of view (FOV). The channel gain of the LoS link is decreased particularly at road crossings where the opportunistic transmission of safety messages between vehicles by visible light might be obstructed by vehicles in adjacent lanes, edifices, and more such impediments.

2.1.2. NLoS Path

The NLoS path in VLC is introduced due to the reflection of the RIS. For VLC systems, optical-RIS (O-RIS) can be implemented using metasurface reflectors or intelligent mirror arrays, both of which are programmed via an O-RIS controller to focus incident optical

power. Metasurfaces operate at sub-wavelength scales and manipulate light propagation by inducing phase shifts through meta-atoms, enabling fine-grained control of the optical wavefront. In contrast, intelligent mirror arrays consist of reflective surfaces that are dynamically adjustable at the micron or millimeter scales, allowing reconfigurable beam shaping. Based on the insights provided in [28], mirror array O-RIS demonstrates superior performance compared to metasurface O-RIS in VLC systems due to its higher efficiency in focusing and redirecting optical power. Therefore, this study focuses on the use of mirror array O-RIS.

RIS-assisted VLC systems generally consider the NLoS path, which includes two main components: the LED-to-RIS path and the RIS-to-PD path. According to Snell’s law of reflection, the specular NLoS path of the n -th LED could be regarded as emitted from its imaging LED, and the energy loss that occurs on the specular reflector surface can be described by a multiplicative attenuation factor. The channel gain vector of the NLoS link is denoted as $\mathbf{h}_{SD,k}^{(2)} = [h_{1,k}^{(2)}, \dots, h_{N,k}^{(2)}]^T$. Based on geometrical optics and trigonometric analysis, the NLoS channel gain between the n -th LED and the k -th PD with the l -th RIS unit is given by [28]

$$h_{n,l,k}^{(2)}(\phi, \psi) = \eta\zeta \frac{\delta(m+1)A_{PD}}{2\pi(d_{n,l} + d_{l,k})^2} \cos^m(\phi)T(\psi)G(\psi)\cos(\psi)g_{n,l} \quad (3)$$

where δ is the reflectivity of each RIS unit, $d_{n,l}$ and $d_{l,k}$ are the distances between the n -th LED with the l -th RIS unit and the l -th RIS unit with the k -th PD, respectively. $g_{n,l}$ is defined to describe the association between RIS units and LEDs. Specifically, the discrete elements $g_{n,l} = 1$ and $g_{n,l} = 0$ indicate the cases that the l -th RIS unit is and is not assigned to the n -th LED, respectively.

2.2. RIS-Based Artificial Noise Scheme

In this paper, we mainly consider a worst-case scenario where malicious attackers are assumed to be unregistered users who appear unpredictably within the network. Hence the positions and channel state information (CSI) of these attackers are assumed to be unknown. This scenario reflects a realistic challenge in securing V2V VLC systems where attackers may dynamically enter the environment, making their CSI difficult to access or estimate. In such cases, the beamforming scheme has limited security enhancement for the system, and the AN strategy becomes a better choice, as shown in Figure 3. Artificial noise is a known and controllable interfering signal artificially added to the original signal at the transmitter side.

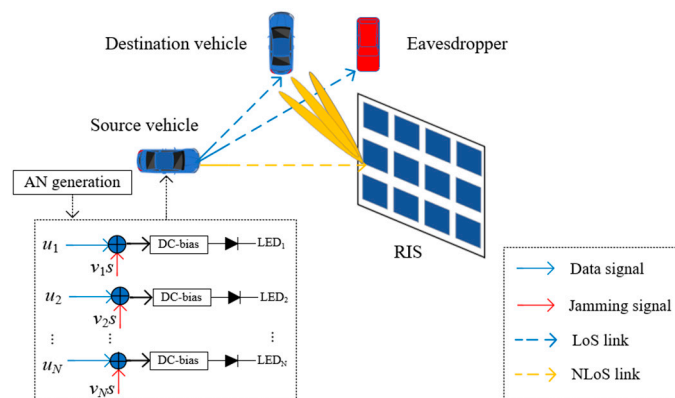


Figure 3. RIS-based artificial noise scheme.

The source vehicle emits AN along with confidential data signals. By design of the noise generator, the generated AN is located in the null space of the destination vehicle’s CSI, ensuring that the AN does not affect the signal quality at the destination.

The RIS reflects both the confidential data signals and the AN in strategically optimized directions. This optimization process aims to maximize the SINR at the destination vehicle while minimizing the worst-case SINR at potential eavesdroppers. This dual mechanism effectively enhances the system’s secrecy rate.

As shown in Figure 3, the data symbols transmitted by the LED at the transmitter are denoted as $\mathbf{u} = [u_1, u_2, \dots, u_N]^T$, and the jamming symbol is denoted as s . Without loss of generality, it is assumed that the sent data u_n and s are uniformly distributed within range $[-1, 1]$, with zero mean and variance σ_u^2 and σ_s^2 , respectively, where $\sigma_u^2 = \sigma_s^2$. The AN generator is denoted as $\mathbf{v} = [v_1, v_2, \dots, v_N]^T$, where $|v| \leq 1$. The transmitted signal from the source vehicle’s LED is given by

$$\mathbf{x} = \alpha[\rho\mathbf{u} + (1 - \rho)\mathbf{v}s] + I_D\mathbf{1}_N \tag{4}$$

where α is the amplitude factor and $\rho \in [0, 1]$ is the power coefficient. I_D is the DC-bias and $\mathbf{1}_N$ is a column vector with all ones. To ensure that the LED operates within its linear region, we introduced predistortion linearization and constrained the input current within the range $[I_{min}, I_{max}]$. This constraint ensures that the output optical power remains within the bounds $[0, P_{max}]$. The DC-bias of the LED is set as $I_D = (I_{min} + I_{max})/2$. Accordingly, the transmitted signal is limited, i.e.,

$$\alpha[\rho + (1 - \rho)\|v\|] \leq A_m \tag{5}$$

where $A_m = (I_{max} - I_{min})/2$ represents the maximum amplitude of the transmitted signal.

When the RIS serves the k -th PD, the data transmitted by the n -th LED is recognized as the confidential signal required by the vehicle. After removing the DC component from the signal directly detected by the PD at the receiving end, the received signal $y_{D,k}$ can be divided into three parts, namely the LoS component $y_{D,k}^{(1)}$, the NLoS component $y_{D,k}^{(2)}$, and the additive white Gaussian noise n_0 with variance σ_N^2 , which is given by

$$y_{D,k} = y_{D,k}^{(1)} + y_{D,k}^{(2)} + n_0 \tag{6}$$

The LoS component $y_{D,k}^{(1)}$ can be expressed as

$$y_{D,k}^{(1)} = \mathbf{h}_{SD,k}^{(1)T}\mathbf{x} + n_0 = \alpha\rho\left(h_{n,k}^{(1)}u_n + \sum_{i=1, i \neq n}^N h_{i,k}^{(1)}u_i\right) + \alpha(1 - \rho)\mathbf{h}_{SD,k}^{(1)T}\mathbf{v}s \tag{7}$$

Since the reflection direction of the mirror array is strictly dependent on the geometrical position of the RIS unit and the transceivers, the probability of light signals emitted by other LEDs reaching the destination vehicle via the RIS unit can be neglected. The NLoS component $y_{D,k}^{(2)}$ is given by

$$y_{D,k}^{(2)} = \alpha\rho h_{n,k}^{(2)}u_n + \alpha(1 - \rho)h_{n,k}^{(2)}v_n s \tag{8}$$

where $y_{D,k}^{(2)} = \sum_{l=1}^L h_{n,l,k}^{(2)}$, $n = 1, 2, \dots, N$.

The received signal of the m -th eavesdropper can be expressed as

$$y_{E,m} = \mathbf{h}_{SE,m}^T\mathbf{x} + n_0 = \alpha\rho\left(h_{n,m}^{(1)}u_n + \sum_{i=1, i \neq n}^N h_{i,m}^{(1)}u_i\right) + \alpha(1 - \rho)\mathbf{h}_{SE,m}^T\mathbf{v}s + n_0 \tag{9}$$

where $\mathbf{h}_{SE,m}$ is the channel gain vector of the LoS link between the n -th LED and the m -th eavesdropper.

By observing the expression for the received signal $y_{D,k}$, it can be seen that the interference terms in the received signal include interference between data signals, artificial noise, and Gaussian white noise. The interference between data signals and Gaussian white noise cannot be avoided, but the effect of artificial noise on the destination vehicle

can be eliminated by designing a noise generator at the transmitter end. For the effects of the interfering signals on the k -th PD to cancel each other out, the noise generator should satisfy as

$$\alpha(1 - \rho)(\mathbf{h}_{SD,k}^{(1)T} \mathbf{v} + h_{n,k}^{(2)} v_n) = 0 \tag{10}$$

At this point, the received signal of the k -th PD of the destination vehicle is given by

$$y_{D,k} = \alpha\rho \left(h_{n,k}^{(1)} u_n + \sum_{i=1, i \neq n}^N h_{i,k}^{(1)} u_i + h_{n,k}^{(2)} u_n \right) + n_0 \tag{11}$$

3. Problem Formulation and Solution

Motivated by the above discussions, this section formulates two optimization problems to enhance the security of the V2V VLC system. Specifically, our aim is to use the RIS to enhance the signal reception of the destination vehicle by maximizing the worst-case signal-to-interference-plus-noise ratio (SINR) of the destination vehicle. Moreover, the generated AN is designed to interfere with eavesdroppers' reception without impacting the signal received by the destination vehicle by minimizing the worst-case SINR of the eavesdropper.

3.1. Problem Formulation

Based on the above, the SINR of the k -th PD of the destination vehicle can be expressed as

$$\gamma_{D,k} = \frac{\sigma_U^2 \alpha^2 \rho^2 \left(h_{n,k}^{(1)} + h_{n,k}^{(2)} \right)^2}{\sigma_U^2 \alpha^2 \rho^2 \sum_{i=1, i \neq n}^N \left(h_{i,k}^{(1)} \right)^2 + \sigma_N^2} \tag{12}$$

When the RIS is serving the k -th PD, there is a situation where different LED light sources send the confidential signal required by the vehicle k . Since different LEDs reach PDs with different channel gains, this leads to differences in the SINR of the k -th PD of the destination vehicle. To ensure the vehicle's communication quality in any of the above cases, the objective function is to maximize the worst-case SINR of the vehicle. Therefore, the optimization problem is formulated as

$$\begin{aligned} \text{(P1): maximize } & \min_n \gamma_{D,k} \\ \text{subject to } & \begin{cases} \sum_{n=1}^N g_{n,l} = 1 \\ g_{n,l} \in \{0, 1\} \end{cases} \end{aligned} \tag{13}$$

where the constraints indicate that an individual RIS unit, each measuring $0.1 \text{ m} \times 0.1 \text{ m}$, can only serve a single user at a time due to the strict dependence of the reflection path's propagation direction on the law of specular reflection.

When the association coefficient $g_{n,l}$ is determined, in order to prevent confidential signals from being acquired by eavesdroppers, the noise generator can be optimized to minimize the SINR of the eavesdropper. For the confidential signal sent by the n -th LED, the SINR of the m -th eavesdropper is defined as

$$\gamma_{E,m,n} = \frac{\sigma_U^2 \alpha^2 \rho^2 \left(h_{n,m}^{(1)} \right)^2}{\sigma_U^2 \alpha^2 \rho^2 \sum_{i=1, i \neq n}^N \left(h_{i,m}^{(1)} \right)^2 + \alpha^2 (1 - \rho)^2 \sigma_S^2 \left| \mathbf{h}_{SE,m}^T \mathbf{v} \right|^2 + \sigma_N^2} \tag{14}$$

Since eavesdroppers appear randomly at any position on the vertical road, maximizing the interference to the eavesdropper's reception is achieved by minimizing the worst-case

SINR for the eavesdropper. This establishes the optimization problem with this as the objective function, which is formulated as

$$\begin{aligned}
 \text{(P2):} \quad & \underset{\mathbf{v}}{\text{minimize}} \quad \max_{m,n} \gamma_{E,m,n} \\
 \text{subject to} \quad & \begin{cases} \alpha(1-\rho)(\mathbf{h}_{SD,k}^{(1)T}\mathbf{v} + h_{n,k}^{(2)}v_n) = 0, \quad n = 1, 2, \dots, N \\ \alpha[\rho + (1-\rho)\|\mathbf{v}\|] \leq A_m \end{cases} \quad (15)
 \end{aligned}$$

3.2. Solution

The first optimization problem (P1) is a typical maximizing minimum problem. The minimum value of the SINR for the k -th PD when transmitting confidential signals from different LEDs is given by

$$\gamma_k = \min_n(\gamma_{D,k}) \quad (16)$$

Then, the optimization problem is transformed into

$$\begin{aligned}
 \text{(P1-a):} \quad & \underset{g_{n,l}}{\text{maximize}} \quad \gamma_k \\
 \text{subject to} \quad & \begin{cases} \gamma_k \leq \gamma_{D,k} \\ \sum_{n=1}^N g_{n,l} = 1 \\ g_{n,l} \in \{0, 1\} \end{cases} \quad (17)
 \end{aligned}$$

where the optimization variable $g_{n,l}$ takes the value of 0 or 1. This is a 0–1 integer programming problem, which can be solved directly using the mixed integer programming (MIP) algorithm.

The second optimization problem (P2) is the typical minimax problem. First, based on the solution obtained from (13), substitute the optimal solution into (15). Then, the vertical road area where the eavesdropper is located is discretized, and I_E points are taken at equal intervals on the vertical road as the possible locations of the eavesdropper. Based on the above channel model, the CSI h_{SE,i_E} of the eavesdropper located at the i_E -th position can be calculated. The SINR $\gamma_{E,i_E,n}$ of the eavesdropper located at the i_E -th position can be obtained from the definition shown in (14), where $i_E = 1, 2, \dots, I_E$. Then, the introduced slack variables can be expressed as

$$\gamma_{EX} = \max_{i_E,n}(\gamma_{E,i_E,n}) \quad (18)$$

The optimization problem (P2) to be solved is transformed into

$$\begin{aligned}
 \text{(P2-a):} \quad & \underset{\mathbf{v}}{\text{minimize}} \quad \gamma_{EX} \\
 \text{subject to} \quad & \begin{cases} \gamma_{E,i_E,n} \leq \gamma_{EX}, \quad i_E = 1, 2, \dots, I_E, n = 1, 2, \dots, N \\ \alpha(1-\rho)(\mathbf{h}_{SD,k}^{(1)T}\mathbf{v} + h_{n,k}^{(2)}v_n) = 0, \quad n = 1, 2, \dots, N \\ \alpha[\rho + (1-\rho)\|\mathbf{v}\|] \leq A_m \end{cases} \quad (19)
 \end{aligned}$$

The optimization problem (P2-a) aims to minimize the objective function, but the first constraint produces a non-convex set. In order to solve this type of problem, the Concave Convex Procedure (CCP) [29] is employed to find a local optimal solution and then obtain the global optimal solution of the problem through iteration.

The first constraint of (19) can be expanded as

$$\alpha^2 \rho^2 (h_{n,i_E}^{(1)})^2 - \gamma_{EX} \left(\alpha^2 \rho^2 \sum_{i=1, i \neq n}^N (h_{i,i_E}^{(1)})^2 + \sigma_N^2 / \sigma_U^2 \right) \leq \gamma_{EX} \left(\alpha^2 (1-\rho)^2 \right) \left| \mathbf{h}_{SE,i_E}^T \mathbf{v} \right|^2 \quad (20)$$

Expanding $\left| \mathbf{h}_{SE,i_E}^T \mathbf{v} \right|^2$ in (20) through the Taylor series, we have

$$\left| \mathbf{h}_{SE,i_E}^T \mathbf{v} \right|^2 \geq \mathbf{v}_0^T \mathbf{h}_{SE,i_E} \mathbf{h}_{SE,i_E}^T \mathbf{v}_0 + 2 \left(\mathbf{h}_{SE,i_E} \mathbf{h}_{SE,i_E}^T \mathbf{v}_0 \right)^T (\mathbf{v} - \mathbf{v}_0) \quad (21)$$

where \mathbf{v}_0 is a given initial feasible solution.

Substitute (21) into (20) and use the sequential quadratic programming [30] standard optimization algorithm to find the optimal solution based on this lower bound. Next, the obtained optimal solution \mathbf{v} is passed to \mathbf{v}_1 and the same steps are repeated until the improvement of the objective value is less than a predefined threshold ε . The detailed process of solving (19) is summarized in Algorithm 1.

Algorithm 1 The Concave Convex Procedure Algorithm

- Input:** Initial feasible points \mathbf{v}_0 ; index $i = 0$; convergence accuracy ε .
 1: **Set:** Constraints on SINR and AN generator γ_E, \mathbf{v} ; objective function in (19).
 2: Generate confidential signal u and artificial noise s .
 3: Identify the RIS central unit.
 4: **Calculation:** The channel gain in the LoS and NLoS path.
 5: **Repeat:**
 6: **Convexify.** Form $f_i(\mathbf{v}, \mathbf{v}_i) = \mathbf{v}_0^T \mathbf{h}_{SE,i_E} \mathbf{h}_{SE,i_E}^T \mathbf{v}_0 + 2 \left(\mathbf{h}_{SE,i_E} \mathbf{h}_{SE,i_E}^T \mathbf{v}_0 \right)^T (\mathbf{v} - \mathbf{v}_0)$,
 7: **Solve the convex problem.** Set the value of \mathbf{v}_{i+1} to a solution of (19).
 8: **Update** \mathbf{v}_{i+1} as the solution of Equation (19).
 9: **Until** convergence.
 10: **Output** optimized \mathbf{v} and the optimum value of the objection function γ_{EX} .
-

3.3. Secrecy Rate

To measure the security performance of the system, the secrecy rate quantifies the maximum rate at which information can be transmitted securely over a communication channel. It represents the difference between the capacity of the legitimate channel and the capacity of the eavesdropper’s channel. The secrecy rate serves as a crucial metric in evaluating and designing secure communication systems, ensuring that information can be transmitted safely while minimizing the risk of interception by unauthorized parties. We assume that the perfect CSI can be estimated by the legitimate receiver and is perfectly known at the RIS for the joint design of transmit beamforming. Additionally, the specific position of the eavesdropping vehicle is random.

The secrecy rate is mathematically defined as

$$R_S = [(R_{D,k} - R_{E,k})]^+ \quad (22)$$

where $|x|^+ = \max(x, 0)$. $R_{E,k}$ is the achievable rate for the eavesdropper of the confidential signal sent to the k -th PD of the destination vehicle, while $R_{D,k}$ is the achievable rate for the k -th PD of the destination vehicle. Assuming that the transmitted confidential signal is uniformly distributed over the interval $[-1, 1]$, the achievable rates can be expressed as [31–33]

$$R_{D,k} = \frac{1}{2} \log_2 \left(4\alpha^2 \rho^2 \left[\sum_{i=1}^N (h_{i,k}^{(1)})^2 + (h_{n,k}^{(2)})^2 \right] + 2\pi e \sigma_N^2 \right) - \frac{1}{2} \log_2 \left(\frac{2}{3} \pi e \alpha^2 \rho^2 \sum_{i=1, i \neq n}^N (h_{i,k}^{(1)})^2 + 2\pi e \sigma_N^2 \right) \quad (23)$$

$$R_{E,k} = \frac{1}{2} \log_2 (1 + \gamma_{E,i_E,k}) \quad (24)$$

where $\gamma_{E,i_E,k}$ is the SINR of the eavesdropper located at the i_E -th position.

4. Simulation Results and Analysis

The security enhancement of the proposed RIS-aided AN scheme is evaluated and analyzed. Meanwhile, the individual contributions of the RIS and AN to the improvement in the secrecy rate performance for the V2V VLC system are illustrated, respectively.

4.1. Simulation Parameters

In our simulation setup, the parameters are selected to approximate a realistic vehicular environment and ensure practical relevance. Specifically, a car width of 2 m is chosen to represent an average vehicle size. The LED headlamps of the source vehicle are fixed at 0.8 m above the ground, with an inter-distance of 1.6 m, reflecting standard automotive lighting configurations [34]. On the receiving vehicle, PDs are installed on the front bumper of the receiving vehicle, 0.8 m above the ground, with an FOV of 60°, which is a typical specification for optical receivers in vehicular applications. The two PDs of the destination vehicle are located on the vertical road at the coordinates of (5 m, 25 m, 0.8 m) and (4 m, 25 m, 0.8 m), while the source vehicle is positioned on a horizontal road with LEDs deployed at the coordinates of (0 m, 20.8 m, 0.8 m) and (0 m, 19.2 m, 0.8 m). This layout models a practical road scenario with typical inter-vehicle distances. The RIS comprises L units uniformly distributed across a rectangular area, with each unit covering $0.1 \text{ m} \times 0.1 \text{ m}$, representing feasible hardware specifications. It is mounted on the traffic lights or road signs at the intersection, ensuring that it does not interfere with the existing infrastructure. Eavesdroppers are randomly placed along the vertical road at 2-m intervals, maintaining a fixed horizontal coordinate of 7 m from the source vehicle, while varying in vertical positions. This configuration models the potential threat posed by eavesdroppers at different locations, allowing for an analysis of the security performance across various eavesdropper positions. Additional simulation parameters are summarized in Table 1.

Table 1. Simulation parameters.

Parameter	Symbol	Value
Number of LEDs	N	2
Number of PDs	K	2
LED semi-angle	$\theta_{1/2}$	60°
Maximum amplitude of the transmitted signal	A_m	2 W
LED conversion factor	η	0.4 W/A
RIS reflectivity	δ	1
PD area	A_{PD}	1 cm ²
PD responsivity	ζ	0.54 A/W
Half angle of PD's FOV	ψ_{FOV}	60°
Optical filter gain	$T(\psi)$	1
Refractive index	κ	1.5
Gaussian noise variance	σ_n^2	−95 dBm
Transmission power	σ_U^2	1/3
Power coefficient	ρ	0.5

4.2. Simulation Results

Figure 4 illustrates the influence of reflectivity and the number of RIS units when the destination vehicle's PD is served by the RIS. In the absence of the RIS, the SINR at the PD drops to a minimum of −5.54 dB due to interference from signals transmitted by the LEDs, making it challenging for the vehicle to decode the desired data. However, when the RIS is employed, the SINR improves as the reflection coefficient increases, which aligns with the theoretical analysis. Additionally, the SINR increases linearly with the number of RIS units. This is because RIS units create additional NLoS links from the LED to the destination vehicle, thus enhancing the SINR. With the optimal configuration, the SINR reaches a maximum of 16.82 dB, representing a 22.36 dB improvement compared to the scenario without the RIS. This substantial improvement significantly enhances the quality of the communication link for the destination vehicle.

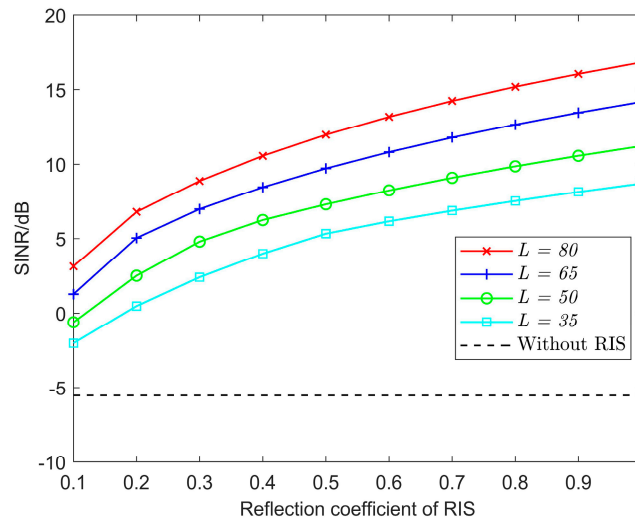


Figure 4. The SINR of PD of the destination vehicle versus reflection coefficient under different numbers of RIS units.

Additionally, after optimizing the noise generator, the worst SINR for the eavesdropper is reduced to -13.22 dB, a decrease of 5.87 dB compared to the scenario without AN. This indicates that the interference signal generated by the noise generator effectively disrupts the eavesdropper’s reception. Notably, due to the symmetrical positioning of the two LEDs about the center axis of the horizontal road, the SINR curves for the eavesdroppers exhibit symmetry when the two LEDs transmit confidential signals separately.

Figure 5 illustrates the impact of the source-to-RIS distance and the transmit power on the SINR at the destination vehicle. The results indicate that as the source-to-RIS distance increases, the SINR decreases, primarily due to path loss occurring before the RIS. While increasing the transmit power improves the signal reception quality, this benefit diminishes as the distance grows due to the combined effects of path loss and light interference in VLC systems. Additionally, a higher transmit power may lead to signal interference among vehicles operating within the same frequency band, potentially leading to significant interference issues.

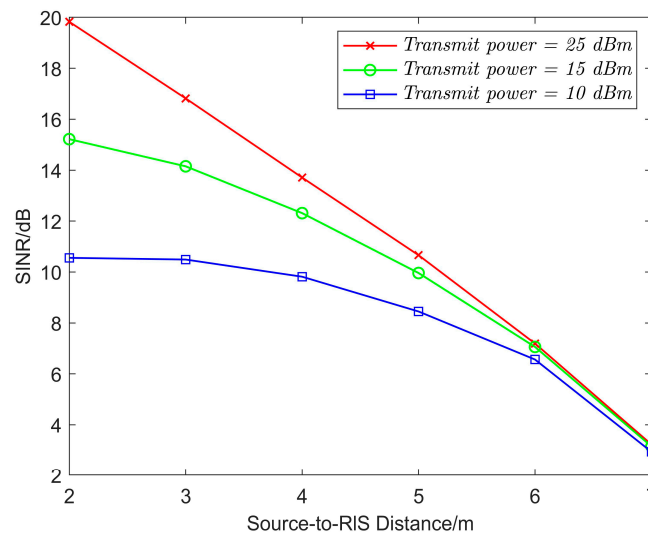


Figure 5. The SINR at the destination vehicle versus source-to-RIS distance under different transmit power.

Figure 6 illustrates the variation in the secrecy rate with the eavesdropper’s position and the number of RIS units. The results show that the secrecy rate decreases slightly

when the eavesdropper is positioned within a small area near the LED transmitting the confidential signal. In contrast, the secrecy rate increases significantly as the eavesdropper moves farther away from this region. When there are 80 RIS units and the reflection coefficient is set to 1, the secrecy rate ranges between a maximum of 1.73 bit/s/Hz and a minimum of 1.16 bit/s/Hz. This variation demonstrates the sensitivity of the secrecy rate to the position of the eavesdropper. Moreover, the results clearly indicate that increasing the number of RIS units leads to an improvement in the secrecy rate. This highlights the critical role of the RIS in optimizing the signal reflection to enhance secure communication.

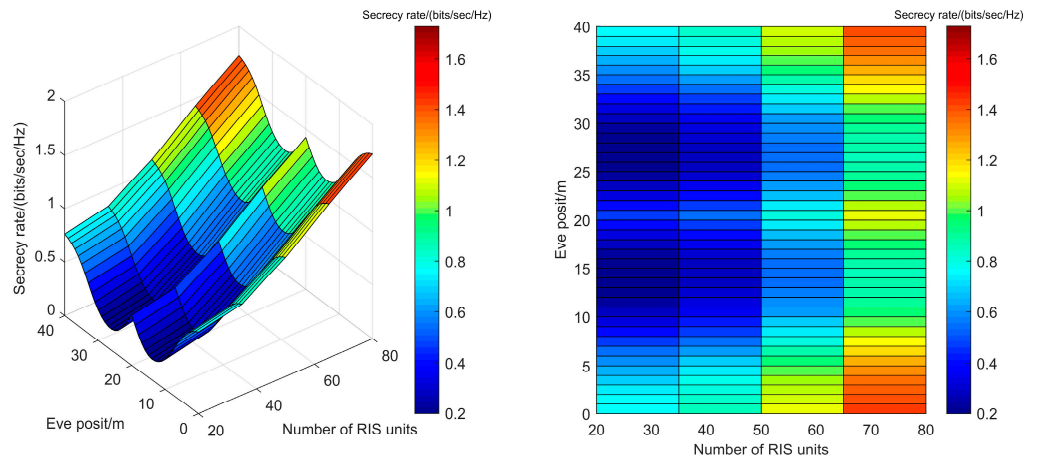


Figure 6. The secrecy rate of the proposed scheme versus the position of eavesdroppers under different numbers of RIS units.

As shown in Figure 7, the secrecy rate is significantly improved when the RIS is employed compared to the case without the RIS, confirming that the RIS enhances the system’s secrecy performance, as discussed earlier. In the absence of the RIS, the secrecy rate drops to a minimum value of -0.48 bit/s/Hz. It is worth noting that a negative secrecy rate indicates that the eavesdropper’s channel is stronger than the legitimate channel, rendering secure communication unachievable. Introducing the RIS improves the secrecy rate by approximately 1.64 bit/s/Hz, achieving a maximum rate of 1.16 bit/s/Hz in this scenario. This substantial improvement validates the effectiveness of the RIS in improving the SINR at the destination vehicle, ensuring that the legitimate user’s signal remains stronger than any eavesdropper’s, thereby enhancing communication security.

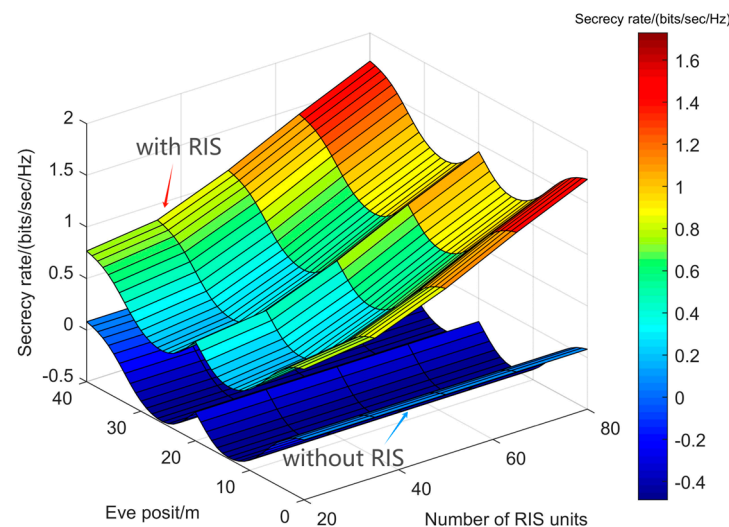


Figure 7. The secrecy rate versus the position of eavesdroppers with and without RIS.

Figure 8 illustrates the secrecy rate as a function of the eavesdroppers' position, comparing scenarios with and without AN. The underlying principle of AN is to deliberately introduce noise that degrades the performance of eavesdroppers while preserving the signal quality for the legitimate receiver, making it a powerful approach for securing communication against potential eavesdropping threats. The simulation results demonstrate that introducing AN significantly enhances the secrecy rate, underscoring its positive impact on system security. By effectively reducing the SINR of the eavesdroppers, AN makes it more challenging for them to decode the transmitted messages. Without AN, the secrecy rate drops to a minimum of 0.63 bit/s/Hz. In contrast, with AN, the secrecy rate improves by approximately 0.34 bit/s/Hz, highlighting its effectiveness in enhancing communication security.

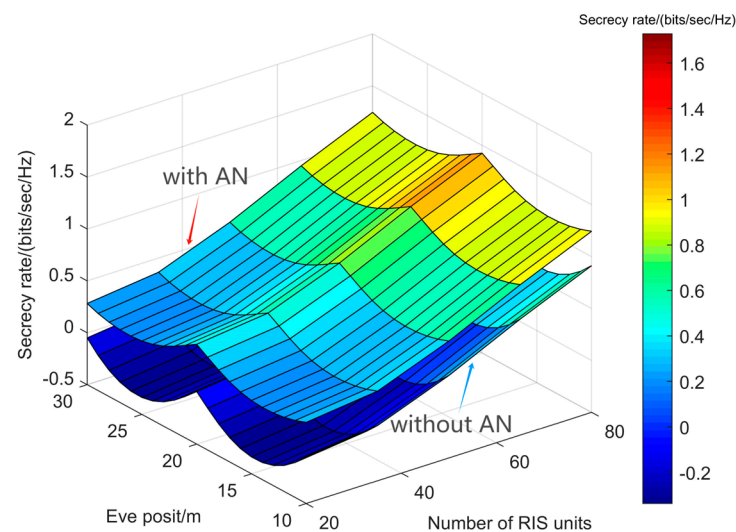


Figure 8. The secrecy rate versus the position of eavesdroppers with and without AN.

The simulation results and discussions reveal that the proposed scheme significantly enhances the system's secrecy rate and overall security performance. This improvement is achieved by employing an RIS to amplify the reception of confidential signals at the destination vehicle while simultaneously using AN to disrupt potential eavesdroppers.

5. Discussion and Conclusions

In this paper, we have investigated the enhancement of the RIS-assisted PLS for the V2V VLC system at road intersections. We propose a novel RIS-assisted security enhancement scheme for V2V VLC networks that leverages the RIS to boost the reception of useful signals at the destination vehicle while simultaneously introducing AN to interfere with potential eavesdroppers. Specifically, we maximize the SINR of the destination vehicle by optimizing the configuration of RIS units. Meanwhile, we optimize the noise generator to minimize the worst-case eavesdropper's SINR without affecting the reception quality for the destination vehicle. The simulation results demonstrate that the proposed scheme significantly enhances the SINR of the destination vehicle while concurrently reducing the SINR of the potential eavesdroppers to weaken the eavesdropper's ability to intercept confidential signals. This dual improvement significantly increases the system's secrecy rate and enhances the overall security performance. When the proposed scheme is adopted, the system's secrecy rate is improved by 1.64 bits/s/Hz compared to the conventional VLC systems.

Our study addresses the under-investigated domain of PLS in RIS-aided V2V VLC systems. The novelty of our work lies in introducing a strategy that combines AN with an RIS to jointly optimize the associated coefficients of the RIS and the design of the AN. Compared to other studies, the proposed scheme offers a robust solution to V2V VLC security challenges in high-risk scenarios. For future work, adapting and scaling the

proposed approach to deal with more complex scenarios, such as urban environments with heavy traffic, is an interesting topic for research and deserves further investigation. Moreover, the impact of environmental factors, such as rain, fog, or low visibility on 2V VLC systems needs to be further studied, which will be helpful in establishing a practical and reliable V2V VLC system in real-world conditions.

Author Contributions: Conceptualization, F.Y. and Y.W.; methodology, X.J. and Y.W.; software, X.J. and X.W.; validation, X.J.; formal analysis, Y.W. and F.Y.; investigation, X.J. and Y.W.; resources, X.J.; data curation, X.J.; writing—original draft preparation, X.J. and Y.W.; writing—review and editing, Y.W. and F.Y.; visualization, X.J. and Y.X.; supervision, F.Y. and Y.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Natural Science Foundation of Shanghai, Grant Number 22ZR1422200; the National Key Research and Development Program of China, Grant Number 2021YFB2900800; the Science and Technology Commission of Shanghai Municipality, Grant Numbers 22511100902, 22511100502, and 111 Project (D20031).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: Author Xiaoyong Wang was employed by CASCO Signal Ltd. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. Jia, D.; Lu, K.; Wang, J.; Zhang, X.; Shen, X. A Survey on Platoon-Based Vehicular Cyber-Physical Systems. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 263–284. [[CrossRef](#)]
2. Papadimitratos, P.; La Fortelle, A.; Evenssen, K.; Brignolo, R.; Cosenza, S. Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation. *IEEE Commun. Mag.* **2009**, *47*, 84–95. [[CrossRef](#)]
3. Noor-A-Rahim, M.; Liu, Z.; Lee, H.; Khyam, M.O.; He, J.; Pesch, D.; Moessner, K.; Saad, W.; Poor, H.V. 6G for Vehicle-to-Everything (V2X) Communications: Enabling Technologies, Challenges, and Opportunities. *arXiv* **2020**, arXiv:2012.07753. [[CrossRef](#)]
4. Amoozadeh, M.; Raghuramu, A.; Chuah, C.-N.; Ghosal, D.; Zhang, H.M.; Rowe, J.; Levitt, K. Security Vulnerabilities of Connected Vehicle Streams and Their Impact on Cooperative Driving. *IEEE Commun. Mag.* **2015**, *53*, 126–132. [[CrossRef](#)]
5. *IEEE P802. 15.7/D3a*; IEEE Approved Draft Standard for Local and Metropolitan Area Networks—Part 15.7: Short-Range Optical Wireless Communications. IEEE: New York, NY, USA, 2018; pp. 1–428.
6. Abumarshoud, H.; Mohjazi, L.; Dobre, O.A.; Renzo, M.D.; Imran, M.A.; Haas, H. LiFi through Reconfigurable Intelligent Surfaces: A New Frontier for 6G? *IEEE Veh. Technol. Mag.* **2022**, *17*, 37–46. [[CrossRef](#)]
7. Kashaf, M.; Ismail, M.; Abdallah, M.; Qaraqa, K.A.; Serpedin, E. Energy Efficient Resource Allocation for Mixed RF/VLC Wireless Networks. *IEEE J. Sel. Areas Commun.* **2016**, *34*, 883–893. [[CrossRef](#)]
8. Meucci, M.; Seminara, M.; Nawaz, T.; Caputo, S.; Mucchi, L.; Catani, J. Bidirectional Vehicle-to-Vehicle Communication System Based on VLC: Outdoor Tests and Performance Analysis. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 11465–11475. [[CrossRef](#)]
9. Cho, S.; Chen, G.; Coon, J.P. Secrecy Analysis in Visible Light Communication Systems with Randomly Located Eavesdroppers. In Proceedings of the 2017 IEEE International Conference on Communications Workshops (ICC Workshops), Paris, France, 21–25 May 2017; pp. 475–480.
10. Liang, Y.; Poor, H.V.; Shamai, S. Physical Layer Security in Broadcast Networks. *Secur. Commun. Netw.* **2009**, *2*, 227–238. [[CrossRef](#)]
11. Ji, P.; Tsai, H.-M.; Wang, C.; Liu, F. Vehicular visible light communications with LED taillight and rolling shutter camera. In Proceedings of the 2014 IEEE 79th Vehicular Technology Conference (VTC Spring), Seoul, Republic of Korea, 18–21 May 2014; pp. 1–6.
12. Ucar, S.; Coleri Ergen, S.; Ozkasap, O.; Tsonev, D.; Burchardt, H. SecVLC: Secure visible light communication for military vehicular networks. In Proceedings of the 14th ACM International Symposium on Mobility Management and Wireless Access, Malta, Malta, 13–17 November 2016; pp. 123–129.
13. Zaman, I.U.; Lopez, A.B.; Al Faruque, M.A.; Boyraz, O. A physical layer security key generation technique for inter-vehicular visible light communication. In *Signal Processing in Photonic Communications*; Paper SpTu1F-3; Optical Society of America: New Orleans, LA, USA, 2017.
14. Yang, N.; Wang, L.; Geraci, G.; ElKashlan, M.; Yuan, J.; Di Renzo, M. Safeguarding 5G wireless communication networks using physical layer security. *IEEE Commun. Mag.* **2015**, *53*, 20–27. [[CrossRef](#)]
15. Basar, E.; Di Renzo, M.; De Rosny, J.; Debbah, M.; Alouini, M.-S.; Zhang, R. Wireless communications through reconfigurable intelligent surfaces. *IEEE Access* **2019**, *7*, 116753–116773. [[CrossRef](#)]

16. Chen, Z.; Guo, Y.; Zhang, P.; Jiang, H.; Xiao, Y.; Huang, L. Physical layer security improvement for hybrid RIS-assisted MIMO communications. *IEEE Commun. Lett.* **2024**, *28*, 2493–2497. [[CrossRef](#)]
17. Wang, J.; Xiao, J.; Zou, Y.; Xie, W.; Liu, Y. Wideband Beamforming for RIS Assisted Near-Field Communications. *IEEE Trans. Wirel. Commun.* **2024**, *23*, 16836–16851. [[CrossRef](#)]
18. Jiang, H.; Shi, W.; Zhang, Z.; Pan, C.; Wu, Q.; Shu, F.; Wang, J. Large-Scale RIS Enabled Air-Ground Channels: Near-Field Modeling and Analysis. *arXiv* **2024**, arXiv:2403.12781. [[CrossRef](#)]
19. Singh, G.; Srivastava, A.; Bohara, V.A. Visible light and reconfigurable intelligent surfaces for beyond 5G V2X communication networks at road intersections. *IEEE Trans. Veh. Technol.* **2022**, *71*, 8137–8151. [[CrossRef](#)]
20. Qian, L.; Chi, X.; Zhao, L.; Chaaban, A. Secure Visible Light Communications via Intelligent Reflecting Surfaces. In Proceedings of the ICC 2021—IEEE International Conference on Communications, Montreal, QC, Canada, 14–23 June 2021; pp. 1–6.
21. Zhang, W.; Zhao, X.; Jiang, G. Physical Layer Security for Intelligent Reflecting Surface-Assisted VLC/RF Hybrid Network. In Proceedings of the 2022 14th International Conference on Communication Software and Networks (ICCSN), Chongqing, China, 10–12 June 2022; pp. 23–27.
22. Zhan, L.; Zhao, H.; Zhang, W.; Lin, J.; Zhao, X. Performance Analysis and Node Selection of Intelligent Reflecting Surface-Aided Visible Light Communication for Parallel Vehicles. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 1462960. [[CrossRef](#)]
23. Singh, S.; Singh, P.; Singh, A.; Srivastava, A. Hybrid RF-VLC technology for V2X in platooning applications under different weather conditions. In Proceedings of the 2024 IEEE Wireless Communications and Networking Conference (WCNC), Dubai, United Arab Emirates, 21–24 April 2024; pp. 1–6.
24. Xie, Y.; Xu, D.; Zhang, T.; Yu, K.; Hussain, A.; Guizani, M. VLC-assisted safety message dissemination in roadside infrastructure-less IoV systems: Modeling and analysis. *IEEE Internet Things J.* **2024**, *11*, 8185–8198. [[CrossRef](#)]
25. Eldeeb, H.B.; Eso, E.; Jarchlo, E.A.; Zvanovec, S.; Uysal, M.; Ghassemlooy, Z.; Sathian, J. Vehicular VLC: A ray tracing study based on measured radiation patterns of commercial taillights. *IEEE Photonics Technol. Lett.* **2021**, *33*, 904–907. [[CrossRef](#)]
26. Alsalami, F.M.; Aigoro, N.; Mahmoud, A.A.; Ahmad, Z.; Haigh, P.A.; Haas, O.C.; Rajbhandari, S. Impact of vehicle headlights radiation pattern on dynamic vehicular VLC channel. *J. Light. Technol.* **2021**, *39*, 3162–3168. [[CrossRef](#)]
27. Aboagye, S.; Ngatched, T.M.; Dobre, O.A.; Ndjiongue, A.R. Intelligent Reflecting Surface-Aided Indoor Visible Light Communication Systems. *IEEE Commun. Lett.* **2021**, *25*, 3913–3917. [[CrossRef](#)]
28. Abdelhady, A.M.; Salem, A.K.S.; Amin, O.; Shihada, B.; Alouini, M.-S. Visible light communications via intelligent reflecting surfaces: Metasurfaces vs mirror arrays. *IEEE Open J. Commun. Soc.* **2021**, *2*, 1–20. [[CrossRef](#)]
29. Lipp, T.; Boyd, S. Variations and extension of the convex–concave procedure. *Optim. Eng.* **2016**, *17*, 263–287. [[CrossRef](#)]
30. Boggs, P.T.; Tolle, J.W. Sequential quadratic programming. *Acta Numer.* **1995**, *4*, 1–51. [[CrossRef](#)]
31. Ben, Y.; Chen, M.; Cao, B.; Yang, Z.; Li, Z.; Cang, Y.; Xu, Z. On secrecy sum-rate of artificial-noise-aided multi-user visible light communication systems. In Proceedings of the 2021 IEEE International Conference on Communications Workshops (ICC Workshops), Montreal, QC, Canada, 14–23 June 2021; pp. 1–6.
32. Yin, L.; Haas, H. Physical-Layer Security in Multiuser Visible Light Communication Networks. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 162–174. [[CrossRef](#)]
33. Cui, M.; Zhang, G.; Zhang, R. Secure Wireless Communication via Intelligent Reflecting Surface. *IEEE Wirel. Commun. Lett.* **2019**, *8*, 1410–1414. [[CrossRef](#)]
34. Shaaban, R.; Faruque, S. Cyber Security Vulnerabilities for Outdoor Vehicular Visible Light Communication in Secure Platoon Network: Review, Power Distribution, and Signal-to-Noise Ratio Analysis. *Phys. Commun.* **2020**, *40*, 101094. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.