引用格式：XU Yuru, WU Yating, ZHENG Guoxin, et al. Infrastructure-assisted Secure Vehicle-to-vehicle Visible Light Communications[J]. Acta Photonica Sinica, 2026, 55(1):0106007
许玉茹,吴雅婷,郑国莘,等.基于基础设施与车辆协作的车车可见光通信安全[J].光子学报,2026,55(1):0106007

基于基础设施与车辆协作的车车可见光通信安全

许玉茹,吴雅婷,郑国莘,孙彦赞
(上海大学 通信与信息工程学院 上海大学特种光纤与光接入网重点实验室,特种光纤与先进通信国际合作联合实验室,上海 200444)

摘　要:针对开放道路场景下车车可见光通信系统面临的物理层安全挑战,提出一种基于交通基础设施协同的新型人工噪声辅助传输方案。该方案聚焦于交叉路口等复杂交通场景中窃听者随机分布所引发的安全威胁,利用道路基础设施如信号灯作为可信干扰节点,构建源车辆与基础设施协同的干扰信号生成机制。通过约束优化设计,人工噪声在合法目标车辆接收端实现干扰抵消,从而在保障合法通信链路质量的前提下,最大化抑制潜在窃听者的信号接收性能。鉴于窃听者位置具有随机性与不可预知性,采用窃听区域离散化建模方法,结合凹凸过程算法,构建以最小化最坏情况下窃听者信干噪比为目标的优化模型。仿真结果表明,相较于传统空间干扰方案,所提方案可显著降低窃听者的信干噪比,提升系统的保密通信速率,有效增强车车可见光通信系统的物理层安全性能。

关键词:可见光通信;车车通信;物理层安全;人工噪声;保密速率
中图分类号:TN929.12　　**文献标识码**:A　　**doi**:10.3788/gzxb20265501.0106007

0　引言

车车可见光通信(Vehicle-to-Vehicle Visible Light Communication,V2V-VLC)作为一种基于LED光源的新型车联网通信技术,正成为智能交通系统中高可靠、低延迟通信的重要研究方向。该技术通过调制车辆灯光信号实现短距离通信,复用现有车灯系统有效降低硬件成本,在密集交通中既可缓解频谱竞争,又能通过抑制多径效应提升信道稳定性,同时兼具绿色节能与高传输速率优势[1-2]。在此背景下,近年来众多研究开始探索将道路基础设施纳入智能交通架构以协助车辆通信。例如,文献[3]和[4]研究了以路灯作为接入点的基础设施和车辆间可见光通信系统性能,验证了道路基础设施辅助车联网通信的可行性,然而两者均未涉及V2V通信场景下的物理层安全问题。

在V2V-VLC系统中,车辆通过前照灯、尾灯传输包含位置、速度、自动驾驶指令等敏感数据的协同决策信息[5]。这些信息一旦被非法截获,可能会导致隐私泄露和行车事故[6]。针对VLC的安全技术,传统方案多聚焦于通信系统MAC层或更高层[7-10]。例如,XIE Qi等[9]提出了一种基于区块链的身份认证方案,实现了车辆与基础设施(Vehicle-to-Infrastructure,V2I)认证、V2I切换认证以及V2V广播认证;QIU Junchao等[10]设计了一种高级加密标准交织辅助的多用户接入方案,解决了VLC系统安全性问题。在动态V2V-VLC场景中,若仅有MAC层及以上安全方案,一旦密文被截获将面临被破解的长期风险。相较之下,物理层安全基于信道物理特性,在信号传输层面主动干扰窃听者,使其难以获取有效信号,结合上层安全方案可实现“防窃听”与“防解密”。当物理层与上层安全方案形成协同防护时,物理层确保信号传输安全,MAC层及以上确保数据与身份安全,二者在信号维度与数据维度构建的双重安全屏障可从根本上提升动态V2V-

基金项目:上海市自然科学基金(22ZR1422200),国家重点研发计划项目(2022YFB2902005),上海无人驾驶列车控制系统工程技术研究中心开放课题(SUTC-2024KT-04),高等学校学科创新引智计划(D20031)
第一作者:许玉茹,xv_yuru@shu.edu.cn
通讯作者:吴雅婷,ytwu@shu.edu.cn
收稿日期:2025-07-30;**录用日期**:2025-11-14

VLC系统在开放信道环境下的安全性。

现有VLC物理层安全技术主要基于室内静态场景设计，使用发光二极管（Light Emitting Diode，LED）作为光源，利用LED光源的固定位置以及空间结构的封闭性特征构建安全边界。例如，WANG Jinyuan等[11]在室内可见光通信网络中，深入剖析了不同光强条件下保密容量的变化规律，LU Meng等[12]解决了广义空间调制的室内多输入单输出可见光通信下行链路的物理层安全问题。然而，V2V-VLC因开放道路环境复杂，车辆移动与动态拓扑使信号暴露不可控，宽波束照明扩大攻击面，易致数据泄露或篡改，相比室内VLC面临更大的安全挑战。

针对上述问题，本文聚焦于交叉路口区域这一车车可见光通信易受窃听的典型场景，考虑窃听者可能随机出现在交叉口任意位置的高风险场景进行建模。为增强通信安全性，提出一种基于基础设施协同的人工噪声（Artificial Noise，AN）干扰机制，联合源车辆与交叉口基础设施生成干扰信号。基础设施包括交通信号灯、道路标识与标牌、路侧单元等，本文采用交通信号灯作为协同干扰源。通过该机制最大程度削弱潜在窃听者的信号接收质量。同时，为消除人工噪声对合法接收车辆通信性能的负面影响，通过对干扰信号的优化设计，使其在目标车辆位置相互抵消，以保障合法通信。结合以上安全增强手段，最终构建了以最小化最坏情况下窃听者信干噪比（Signal to Interference plus Noise Ratio，SINR）为目标的约束优化问题，以提升系统整体的保密速率。仿真实验结果表明，所提联合干扰策略在确保合法通信质量的前提下，能够显著降低窃听者的信号接收性能，从而有效增强系统的物理层安全性能。

1 系统模型

1.1 可见光信道模型

图1展示了交叉路口V2V-VLC系统模型架构：源车辆S通过前照灯（N_S个LED阵列）建立安全通信链路，目标车辆D配置K个光电探测器（Photo Detector，PD）实现信号解码；当车辆转弯引发光束偏离时，随机分布的窃听者易捕获散射信号。为此，部署交通信号灯J（N_J个LED单元）作为协同干扰源发射干扰信号，在抑制窃听者接收机性能的同时保障合法链路正常通信。

在V2V-VLC系统中，通常使用视距链路模型来表征VLC信道响应特性。发射端源车辆S的第n个LED到目标车辆D的第k个PD之间的信道增益[13]可表示为

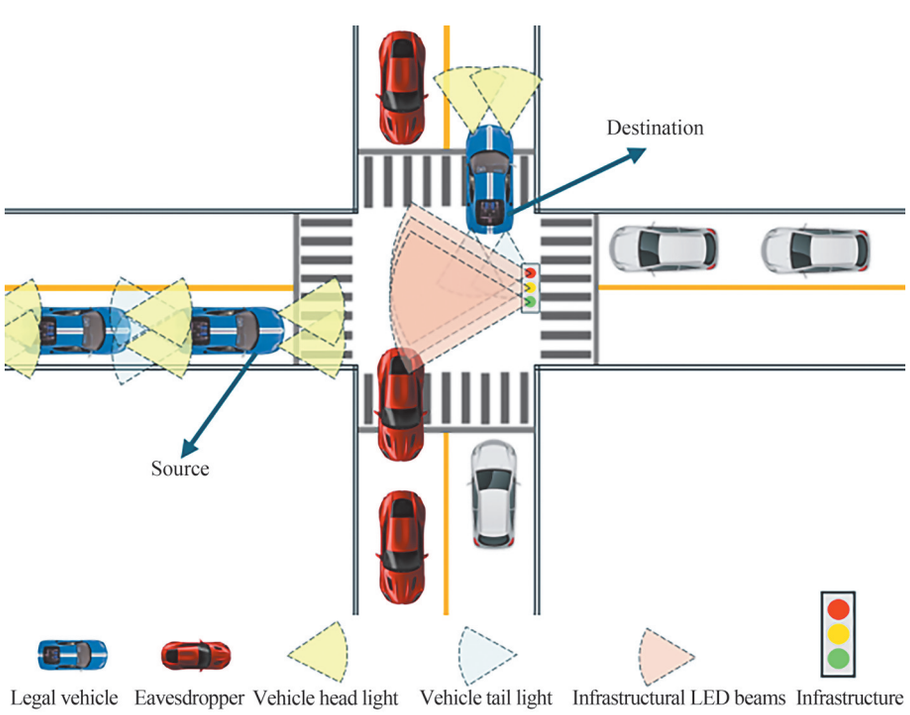


图1 V2V-VLC系统模型

Fig. 1 V2V-VLC system model

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

式中，η是LED的光电转换率，ζ为PD的响应度。d为LED到PD的直线距离，A_{PD}为PD的接收面积。$m=-\ln 2/\ln(\cos\theta_{1/2})$是描述LED辐射方向性的辐射模式阶数（由LED的半功率角$\theta_{1/2}$决定）。LED辐射角ϕ和PD入射角ψ、光学滤波器增益$T(\psi)$、集中器增益$G(\psi)$共同构成信道系数。具体来说，$G(\psi)$的物理模型为

$$G(\psi)=\begin{cases}\dfrac{\kappa^{2}}{\sin^{2}\psi_{\mathrm{FOV}}}, & 0\leqslant\psi\leqslant\psi_{\mathrm{FOV}}\\ 0, & \psi>\psi_{\mathrm{FOV}}\end{cases} \tag{2}$$

式中，κ为光学集中器的折射率，ψ_{FOV}为PD视场角。

1.2 联合干扰方案及优化问题

基于前文所述，本文提出一种依托基础设施的AN联合干扰方案，旨在增强V2V-VLC系统于复杂环境中的物理层安全性。如图2所示，源车辆S通过其LED向目标车辆D传输机密信息之际，协同道路交叉口的交通信号灯J的N_{J}个LED发射干扰信号，以最大化削弱窃听者对机密信号的截获能力。该方案中，人工噪声信号由精心设计的噪声生成器调控，确保对目标车辆D零干扰，保障其准确接收机密信号，提升系统保密性能。

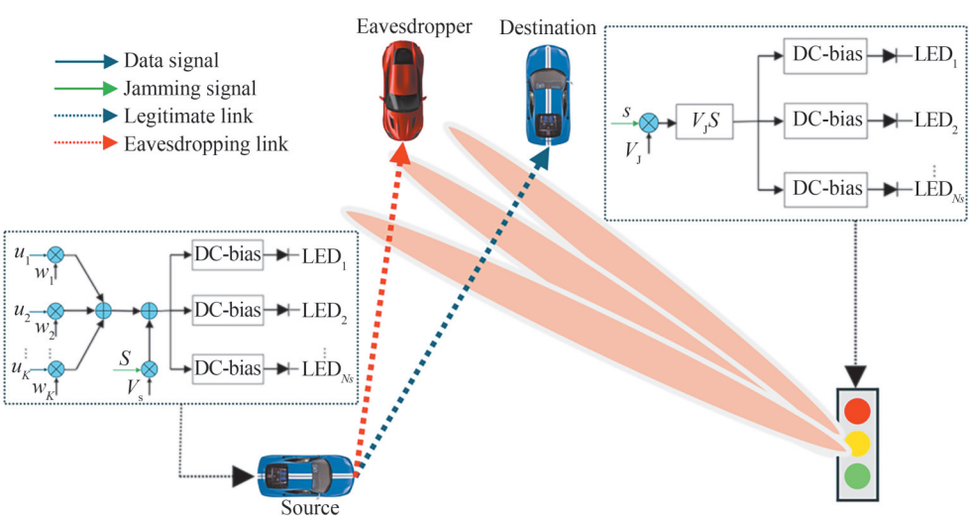


图2 基于基础设施的AN干扰方案

Fig. 2 Infrastructure-based AN jamming scheme

具体而言，源车辆S处LED发射的机密数据符号表示为$\boldsymbol{u}=[u_1,u_2,\cdots,u_k]^{\mathrm{T}}$，$k=1,2,\cdots,K$，其中$u_k$是发送给第$k$个PD的数据符号。人工噪声是人为添加到原始信号中的已知且可控的干扰信号，假设源车辆S和交通信号灯J发送的干扰数据为$\boldsymbol{S}$。在不影响问题一般性的前提下，假定发送数据符号$\boldsymbol{u}_k$和干扰信号$\boldsymbol{S}$的均值为0，其取值范围为$[-1,1]$，其方差分别为σ_{U}^{2}和σ_{S}^{2}，其中$\sigma_{\mathrm{U}}^{2}=\sigma_{\mathrm{S}}^{2}$。机密信号$\boldsymbol{u}_k$的预编码器为$\boldsymbol{w}_k=[w_{1,k},w_{2,k},\cdots,w_{N\mathrm{S},k}]^{\mathrm{T}}$，其中$|w_{n,k}|\leqslant 1$，$n=1,2,\cdots,N_{\mathrm{S}}$，$\boldsymbol{w}_k$对机密信号进行编码以适应信道特性。发射端源车辆S和交通信号灯J的噪声生成器分别表示为$\boldsymbol{v}_{\mathrm{S}}=[v_1,v_2,\cdots,v_{N\mathrm{S}}]^{\mathrm{T}}$和$\boldsymbol{v}_{\mathrm{J}}=[v_1,v_2,\cdots,v_{N\mathrm{J}}]^{\mathrm{T}}$，用于生成干扰窃听者接收的人工噪声信号。

源车辆S和交通信号灯J的发射信号可分别表示为

$$\begin{cases}\boldsymbol{x}_{\mathrm{S}}=\alpha_1\left[\dfrac{\rho}{K}\displaystyle\sum_{k=1}^{K}\boldsymbol{w}_k\boldsymbol{u}_k+(1-\rho)\boldsymbol{v}_{\mathrm{S}}\boldsymbol{s}\right]+I_{\mathrm{D}}\mathbf{1}_{N_{\mathrm{S}}}\\ \boldsymbol{x}_{\mathrm{J}}=\alpha_2\boldsymbol{v}_{\mathrm{J}}\boldsymbol{s}+I_{\mathrm{D}}\mathbf{1}_{N_{\mathrm{J}}}\end{cases} \tag{3}$$

式中，α_1和α_2为幅值系数（需符合LED动态范围约束），$\rho\in[0,1]$是光功率调制因子。I_{D}为确保工作点位于线性区的直流偏置。$\mathbf{1}_{N\mathrm{S}}$和$\mathbf{1}_{N\mathrm{J}}$是全1向量。常规发光二极管固有的非线性特性会引入信号失真，在其限定动态范围$[I_{\min},I_{\max}]$内，常采用预失真补偿策略。设直流偏置点为动态范围的中值$I_{\mathrm{D}}=1/2(I_{\min}+I_{\max})$，信号的最大允许幅值为$A_{\mathrm{m}}$。为确保LED在直流偏置点线性区间内运行，输入信号的瞬时幅度必须严格满足其动态范围的约束

$$\begin{cases}\alpha_1\left[\dfrac{\rho}{K}\left\|\sum_{k=1}^{K}|\boldsymbol{w}_k|\right\|_\infty+(1-\rho)\|\boldsymbol{v}_\mathrm{S}\|_\infty\right]\leqslant A_\mathrm{m}\\ \alpha_2\|\boldsymbol{v}_\mathrm{J}\|_\infty\leqslant A_\mathrm{m}\end{cases}\tag{4}$$

式中，最大信号幅值A_m满足$A_\mathrm{m}=1/2(I_{\min}+I_{\max})$。该约束避免了信号的削波失真。此外，预失真补偿策略保证信号在传输过程中尽量不受失真影响，保持较高的传输质量和安全性。

目标车辆D的第k个PD经过交流耦合移除直流分量后获取的基带信号为

$$\begin{aligned}\boldsymbol{y}_{\mathrm{D},k}=\boldsymbol{h}_{\mathrm{SD},k}^{\mathrm{T}}\boldsymbol{x}_\mathrm{S}+\boldsymbol{h}_{\mathrm{JD},k}^{\mathrm{T}}\boldsymbol{x}_\mathrm{J}+n_{\mathrm{D},k}=\alpha_1\frac{\rho}{K}\left(\boldsymbol{h}_{\mathrm{SD},k}^{\mathrm{T}}\boldsymbol{w}_k u_k+\boldsymbol{h}_{\mathrm{SD},k}^{\mathrm{T}}\sum_{i=1,i\neq k}^{K}\boldsymbol{w}_i u_i\right)+\\ \alpha_1(1-\rho)\boldsymbol{h}_{\mathrm{SD},k}^{\mathrm{T}}\boldsymbol{v}_\mathrm{S}s+\alpha_2\boldsymbol{h}_{\mathrm{JD},k}^{\mathrm{T}}\boldsymbol{v}_\mathrm{J}s+n_{\mathrm{D},k}\end{aligned}\tag{5}$$

式中，$k=1,2,\cdots,K$。$\boldsymbol{h}_{\mathrm{SD},k}$为发射端源车辆S的LED到接收端目标车辆D的第$k$个PD的信道增益向量，$\boldsymbol{h}_{\mathrm{JD},k}$为交通信号灯LED到接收端车辆第$k$个PD的信道增益向量，$n_{\mathrm{D},k}$表示叠加在接收信号上的加性高斯白噪声，其平均功率为σ_N^2。第m个潜在窃听者接收信号的表达式为

$$\begin{aligned}\boldsymbol{y}_{\mathrm{E},m}=\boldsymbol{h}_{\mathrm{SE},m}^{\mathrm{T}}\boldsymbol{x}_\mathrm{S}+\boldsymbol{h}_{\mathrm{JE},m}^{\mathrm{T}}\boldsymbol{x}_\mathrm{J}+n_\mathrm{E}=\alpha_1\frac{\rho}{K}\left(\boldsymbol{h}_{\mathrm{SE},m}^{\mathrm{T}}\boldsymbol{w}_k\boldsymbol{u}_k+\boldsymbol{h}_{\mathrm{SE},m}^{\mathrm{T}}\sum_{i=1,i\neq k}^{K}\boldsymbol{w}_i\boldsymbol{u}_i\right)+\\ \alpha_1(1-\rho)\boldsymbol{h}_{\mathrm{SE},m}^{\mathrm{T}}\boldsymbol{v}_\mathrm{S}\boldsymbol{s}+\alpha_2\boldsymbol{h}_{\mathrm{JE},m}^{\mathrm{T}}\boldsymbol{v}_\mathrm{J}\boldsymbol{s}+n_\mathrm{E}\end{aligned}\tag{6}$$

式中，$\boldsymbol{h}_{\mathrm{SE},m}$为源车辆S的LED到垂直道路上第$m$个潜在窃听者的信道增益向量，$\boldsymbol{h}_{\mathrm{JE},m}$为交通信号灯J的LED到第$m$个潜在窃听者的信道增益向量。$n_\mathrm{E}$表示叠加在窃听者接收信号上的加性高斯白噪声，其平均功率为σ_N^2。

在垂直道路场景中，窃听者是随机分布的，这导致源车辆S与交通信号灯的LED至窃听者的可见光信道特性无法被准确估计，难以建立精确的信道状态信息估计模型。在这种情况下，为确保在接收端目标车辆的第k个PD处机密信号$\boldsymbol{u}_k$的信号强度最大化，取$\boldsymbol{w}_k=\boldsymbol{h}_{\mathrm{SD},k}/\|\boldsymbol{h}_{\mathrm{SD},k}\|$。为使源车辆S与交通信号灯J发射的协同干扰信号在目标车辆PD处实现互相抵消，噪声生成器$\boldsymbol{v}_\mathrm{S}$和$\boldsymbol{v}_\mathrm{J}$应满足约束条件

$$\alpha_1(1-\rho)\boldsymbol{h}_{\mathrm{SD},k}^{\mathrm{T}}\boldsymbol{v}_\mathrm{S}+\alpha_2\boldsymbol{h}_{\mathrm{JD},k}^{\mathrm{T}}\boldsymbol{v}_\mathrm{J}=0\tag{7}$$

满足约束条件后，目标车辆第k个PD的接收信号为

$$\boldsymbol{y}_{\mathrm{D},k}=\alpha_1\frac{\rho}{K}\boldsymbol{h}_{\mathrm{SD},k}^{\mathrm{T}}\boldsymbol{w}_k\boldsymbol{u}_k+\alpha_1\frac{\rho}{K}\boldsymbol{h}_{\mathrm{SD},k}^{\mathrm{T}}\sum_{i=1,i\neq k}^{K}\boldsymbol{w}_i\boldsymbol{u}_i+n_{\mathrm{D},k}\tag{8}$$

对应的信干噪比表征为

$$\gamma_{\mathrm{D},k}=\frac{\sigma_\mathrm{U}^2\lambda^2\left|\boldsymbol{h}_{\mathrm{SD},k}^{\mathrm{T}}\boldsymbol{w}_k\right|^2}{\sigma_\mathrm{U}^2\lambda^2\sum_{i=1,i\neq k}^{K}\left|\boldsymbol{h}_{\mathrm{SD},k}^{\mathrm{T}}\boldsymbol{w}_i\right|^2+\sigma_\mathrm{N}^2}\tag{9}$$

式中，$\lambda=\alpha_1\rho/K$。满足式(7)时，设计的联合干扰信号对目标车辆零干扰，同时保障了机密数据$\boldsymbol{u}_k$的信号强度可以取到最大值。在此干扰约束下，窃听者的接收信号会被最大程度地干扰，从而实现最小化窃听者的信干噪比。对于发送给目标车辆第k个PD的机密数据$\boldsymbol{u}_k$，第m个潜在窃听者的接收信号信干噪比可表征为

$$\gamma_{\mathrm{E},m,k}=\frac{\sigma_\mathrm{U}^2\lambda^2\left|\boldsymbol{h}_{\mathrm{SE},m}^{\mathrm{T}}\boldsymbol{w}_k\right|^2}{\sigma_\mathrm{U}^2\lambda^2\sum_{i=1,i\neq k}^{K}\left|\boldsymbol{h}_{\mathrm{SE},m}^{\mathrm{T}}\boldsymbol{w}_i\right|^2+\sigma_\mathrm{S}^2\alpha_1^2(1-\rho)^2\left|\boldsymbol{h}_{\mathrm{SE},m}^{\mathrm{T}}\boldsymbol{v}_\mathrm{S}\right|^2+\sigma_\mathrm{S}^2\alpha_2^2\left|\boldsymbol{h}_{\mathrm{JE},m}^{\mathrm{T}}\boldsymbol{v}_\mathrm{J}\right|^2+\sigma_\mathrm{N}^2}\tag{10}$$

鉴于窃听者在垂直道路上的位置是动态变化的，并且$\gamma_{\mathrm{E},m,k}$会随之变化，因此，为确保极端场景下系统的安全性能，以窃听者在最差条件下的信干噪比最小化为目标函数，构建如下优化问题

$$\begin{aligned}&\underset{\boldsymbol{v}_\mathrm{S},\boldsymbol{v}_\mathrm{J}}{\text{minimize}}\ \max_{m,k}\gamma_{\mathrm{E},m,k}\\ &\text{subject to}\begin{cases}\alpha_1(1-\rho)\boldsymbol{h}_{\mathrm{SD},k}^{\mathrm{T}}\boldsymbol{v}_\mathrm{S}+\alpha_2\boldsymbol{h}_{\mathrm{JD},k}^{\mathrm{T}}\boldsymbol{v}_\mathrm{J}=0,\ k=1,2,\cdots,K\\ \alpha_1\left[\dfrac{\rho}{K}\left\|\sum_{k=1}^{K}|\boldsymbol{w}_k|\right\|_\infty+(1-\rho)\|\boldsymbol{v}_\mathrm{S}\|_\infty\right]\leqslant A_\mathrm{m}\\ \alpha_2\|\boldsymbol{v}_\mathrm{J}\|_\infty\leqslant A_\mathrm{m}\end{cases}\end{aligned}\tag{11}$$

式中，$\boldsymbol{v}_\mathrm{S}$和$\boldsymbol{v}_\mathrm{J}$需满足式(7)，发送信号需满足式(4)。

2 优化问题的求解

式(11)属于经典的最小化最大值优化问题。针对该优化模型，需对窃听者所在的垂直道路区域实施离散化处理：在垂直道路上以等间距的方式选取I_{E}个采样点，将其作为潜在窃听者的所有位置。根据上述信道模型，可以推导得到源车辆S和交通信号灯J到第i_{E}个窃听者位置的信道状态信息$\boldsymbol{h}_{\mathrm{SE},i_{\mathrm{E}}}$和$\boldsymbol{h}_{\mathrm{JE},i_{\mathrm{E}}}$。根据式(10)定义的窃听者信干噪比，可求解第$i_{\mathrm{E}}$个位置处窃听者的信干噪比$\gamma_{\mathrm{E},i_{\mathrm{E}},k}$，其中$i_{\mathrm{E}}=1,2,\cdots,I_{\mathrm{E}}$，$k=1,2,\cdots,K$。引入松弛变量$\gamma_{\mathrm{EX}}$

$$\gamma_{\mathrm{EX}}=\max_{i_{\mathrm{E}},k}\gamma_{\mathrm{E},i_{\mathrm{E}},k} \tag{12}$$

待求解的优化问题(11)可重构为

$$\begin{aligned}&\underset{\boldsymbol{v}_{\mathrm{S}},\boldsymbol{v}_{\mathrm{J}}}{\text{minimize}}\ \ \gamma_{\mathrm{EX}}\\&\text{subject to}\begin{cases}\gamma_{\mathrm{E},i_{\mathrm{E}},k}\leqslant\gamma_{\mathrm{EX}},\ i_{\mathrm{E}}=1,2,\cdots,I_{\mathrm{E}};\ k=1,2,\cdots,K\\ \alpha_1(1-\rho)\boldsymbol{h}_{\mathrm{SD},k}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{S}}+\alpha_2\boldsymbol{h}_{\mathrm{JD},k}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{J}}=0,\ k=1,2,\cdots,K\\ \alpha_1\left[\dfrac{\rho}{K}\left\|\sum_{k=1}^{K}|\boldsymbol{w}_k|\right\|_{\infty}+(1-\rho)\|\boldsymbol{v}_{\mathrm{S}}\|_{\infty}\right]\leqslant A_{\mathrm{m}}\\ \alpha_2\|\boldsymbol{v}_{\mathrm{J}}\|_{\infty}\leqslant A_{\mathrm{m}}\end{cases}\end{aligned} \tag{13}$$

上述优化问题旨在求解目标函数的最小值，然而首个约束条件形成了非凸集。针对此类非凸优化问题，本文采用凹凸过程(Convex-Concave Procedure，CCP)[14]求解其局部最优解，并通过迭代机制找到全局最优解。具体而言，将式(13)中的第一个约束条件展开为

$$\lambda^2\left|\boldsymbol{h}_{\mathrm{SE},i_{\mathrm{E}}}^{\mathrm{T}}\boldsymbol{w}_k\right|^2-\gamma_{\mathrm{EX}}\left(\lambda^2\sum_{i=1,i\neq k}^{K}\left|\boldsymbol{h}_{\mathrm{SE},i_{\mathrm{E}}}^{\mathrm{T}}\boldsymbol{w}_i\right|^2-\sigma_{\mathrm{N}}^2/\sigma_{\mathrm{U}}^2\right)\leqslant\gamma_{\mathrm{EX}}\left(\alpha_1^2(1-\rho)^2\left|\boldsymbol{h}_{\mathrm{SE},i_{\mathrm{E}}}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{S}}\right|^2+\alpha_2^2\left|\boldsymbol{h}_{\mathrm{JE},i_{\mathrm{E}}}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{J}}\right|^2\right) \tag{14}$$

对式(14)中的$\left|\boldsymbol{h}_{\mathrm{SE},i_{\mathrm{E}}}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{S}}\right|^2$进行泰勒级数展开，可得

$$\left|\boldsymbol{h}_{\mathrm{SE},i_{\mathrm{E}}}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{S}}\right|^2\geqslant\boldsymbol{v}_{\mathrm{S},0}^{\mathrm{T}}\boldsymbol{h}_{\mathrm{SE},i_{\mathrm{E}}}\boldsymbol{h}_{\mathrm{SE},i_{\mathrm{E}}}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{S},0}+2\left(\boldsymbol{h}_{\mathrm{SE},i_{\mathrm{E}}}\boldsymbol{h}_{\mathrm{SE},i_{\mathrm{E}}}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{S},0}\right)^{\mathrm{T}}\left(\boldsymbol{v}_{\mathrm{S}}-\boldsymbol{v}_{\mathrm{S},0}\right) \tag{15}$$

式中，$\boldsymbol{v}_{\mathrm{S},0}$为预设的初始可行解。将式(15)代入式(14)，采用顺序二次规划(Sequential Quadratic Programming，SQP)[15]标准优化算法，基于该下界求解最优解。接下来，将迭代求解得到的最优解中$\boldsymbol{v}_{\mathrm{S}}$的值传递给$\boldsymbol{v}_{\mathrm{S},1}$，进行下一轮迭代，直至目标函数的改进小于预设阈值$\varepsilon$。该算法的实施步骤详见表1。

表1 凹凸过程算法

Table 1 Concave-convex procedure algorithm

The CCP algorithm for solving Eq. (13)
Input: Initial feasible points $\boldsymbol{v}_{\mathrm{S},0}$; index $i=0$; convergence accuracyε
1: **Set**: Constraints on AN generator $\boldsymbol{v}_{\mathrm{S}}$, $\boldsymbol{v}_{\mathrm{J}}$; objective function in (13)
2: **Generate** confidential signal $\boldsymbol{u}$ and artificial noise $\boldsymbol{S}$
3: **Calculate**: The channel gain in the LoS path
4: **Repeat**:
5: **Convexify** form
$f_i(\boldsymbol{v}_{\mathrm{S}},\boldsymbol{v}_{\mathrm{S},i})=\boldsymbol{v}_{\mathrm{S},i}^{\mathrm{T}}\boldsymbol{h}_{\mathrm{SE},i_{\mathrm{E}}}\boldsymbol{h}_{\mathrm{SE},i_{\mathrm{E}}}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{S},i}+2\left(\boldsymbol{h}_{\mathrm{SE},i_{\mathrm{E}}}\boldsymbol{h}_{\mathrm{SE},i_{\mathrm{E}}}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{S},i}\right)^{\mathrm{T}}\left(\boldsymbol{v}_{\mathrm{S}}-\boldsymbol{v}_{\mathrm{S},i}\right),i_E=1,2,\cdots,I_E$
The concave function part is linearized at current point $\boldsymbol{v}_{\mathrm{S},i}$ via 1st-order Taylor expansion, and the original function is approximated by its linear upper bound.
6: **Solve** the convex problem in Eq. (13)
Set the value of $\boldsymbol{v}_{\mathrm{S},i+1}$ to the solution of the convex problem
7: **Update** iteration $i=i+1$
8: **Until** convergence
9: **Output** the optimum value of the objection function γ_{EX}

3 仿真结果与分析

为评估所提出的系统安全方案的性能，设定如下车辆参数：以平均车宽2 m表征车辆尺寸；源车辆前照灯LED固定于距地0.8 m处，间距1.6 m，符合标准汽车照明配置；接收端PD安装在目标车辆后保险杠（距地0.8 m），视场角设为60°，为车载光学接收器典型参数[16]。系统其余具体参数详见表2。

表2 系统参数

Table 2 System parameters

Parameters	Value
Number of LEDs of the source vehicle N_S	2
Number of LEDs for traffic lights N_J	3
Number of PDs of the target vehicle K	2
Half power Angle of LED $\theta_{1/2}$/(°)	60
Dynamic range of LED $[I_{min}, I_{max}]/A$	[1, 5]
Active area of PD A_{PD}/cm^2	1
Conversion factor of LED η/(W•A^{-1})	0.4
Responsivity of PD ζ/(A•W^{-1})	0.54
Gain of optical filter $T(\psi)$	1
Refractive index of lens κ	1.5
Average noise power σ_N^2/dBm	−95
Variance of signal σ_U^2	1/3
Optical power coefficient ρ	0.5

图3是基于基础设施的AN干扰方案下窃听者SINR的分布特性，其中，图3(a)、(b)分别对应仅有LED1传输机密信号（场景一）和仅有LED2传输机密信号（场景二）时，窃听者沿垂直道路方向移动时的SINR变化规律。研究表明，窃听者邻近机密LED时，由于直射路径主导信号传输，其SINR呈现显著高值；随着距离增大，SINR因路径损耗呈单调递减且离散性增强，这源于信号衰减与干扰增强的双重作用。值得注意的是，靠近交通信号灯的区域出现SINR局部峰值，此异常源于LED指向性辐射特性：当窃听者方位角超出探测器视场角时，干扰信号信道增益趋零，导致SINR显著提升。

表3对比了相同场景不同人工噪声生成方法下窃听者SINR的最大值、最小值与均值。研究显示，本方案在SINR最大值、最小值及均值三项指标上均优于空间干扰方案[17]。其中，表征最坏情况的SINR最大值（−7.07 dB）较对比方案降低8.77 dB，证实本方案在最小化窃听者峰值SINR的优化目标中具有显著优势。

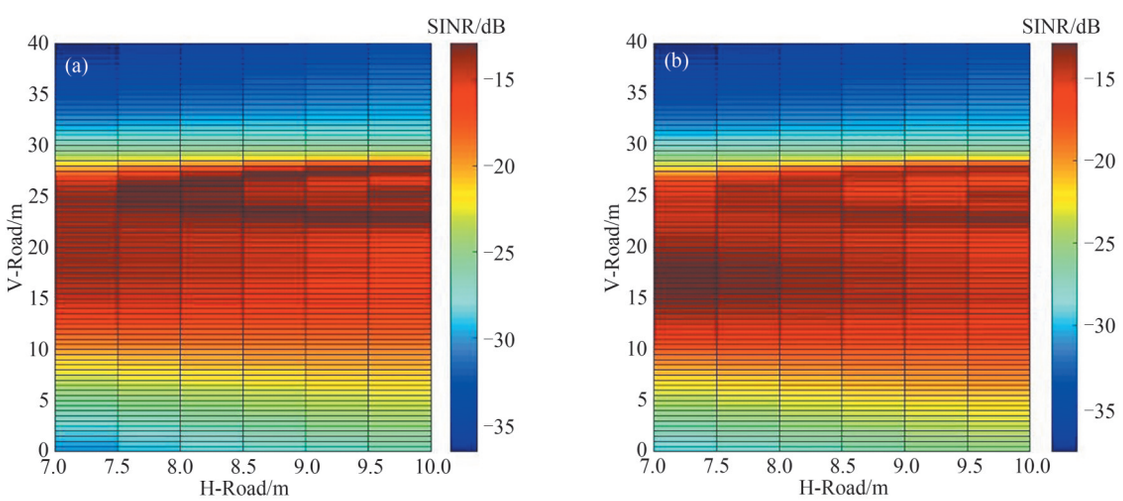


图3 窃听者的信干噪比。(a) LED_1所属机密信号；(b) LED_2所属机密信号

Fig. 3 Eavesdropper's SINR. (a) LED_1 transmitting confidential signal; (b) LED_2 transmitting confidential signal

表3　不同方案下窃听者的信干噪比

Table 3　Eavesdropper's SINR under different schemes

Scheme	Average/dB	Maximum/dB	Minimum/dB
Spatial jamming[17]	−0.81	1.70	−7.71
Proposed	−16.50	−7.07	−32.05

图4对比了两种干扰方案下窃听者SINR的空间分布特性。图4(a)、(b)分别对应场景一(LED1为信源)与场景二(LED2为信源)中，垂直道路方向窃听者SINR的空间演化规律。为便于量化比较，文中将窃听者按照与LED的空间距离分类，将V-Road方向上20 m～30 m这一靠近源LED的区域定义为近场，其余采样点则归类为远场。由于交叉道路口场景中窃听者位置随机，本文对窃听者所在的垂直道路区域实施离散化网格处理，在垂直道路上以等间距的方式选取120个采样点，将其作为潜在窃听者的所有位置。对每个采样点i，首先计算空间干扰方案与本方案下的SINR差值，然后分别对近场与远场窃听者集合求算术平均值。实验表明，两种方案下近场SINR均呈现高值特征，且随距离呈单调递减，验证了路径损耗的主导作用。

对比结果表明，基于基础设施的AN干扰方案在全区域SINR抑制效果显著优于空间干扰方案：近场窃听者在场景1和场景2的SINR分别降低11.25 dB和10.61 dB，而远场窃听者在场景1和场景2的SINR降幅达17.12 dB和17.41 dB。所提方案通过干扰信号定向辐射与基础设施协同，扩展干扰维度与优化空间分布，在保障V2V通信质量前提下显著提升了V2V-VLC通信系统的保密性。

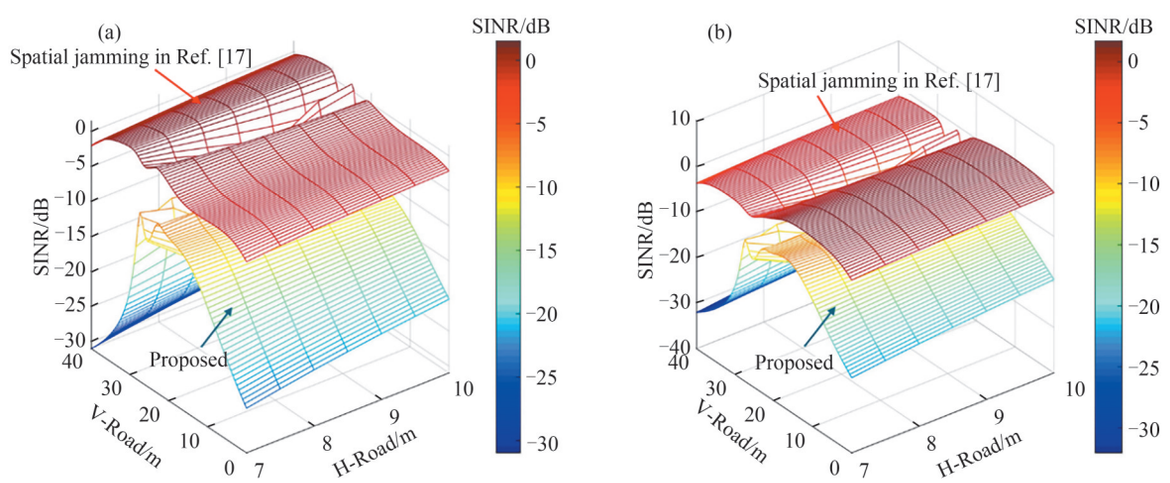


图4　不同方案下窃听者的信干噪比。(a) LED_1所属机密信号；(b) LED_2所属机密信号

Fig. 4　Eavesdropper's SINR under different schemes. (a) LED_1 transmitting confidential signal; (b) LED_2 transmitting confidential signal

为定量评估系统的安全性能，图5给出了当窃听者在垂直道路的各个位置时，采用不同方案时系统保密速率(Secrecy Rate)总和的仿真结果。保密速率总和的定义为[18]

$$R_{\mathrm{S}}=\sum_{k=1}^{K}\left[\left(R_{\mathrm{D},k}-R_{\mathrm{E},k}\right)\right]^{+} \tag{16}$$

式中，$[x]^{+}=\max(x,0)$。$R_{\mathrm{D},k}$为第k个PD的可达速率，$R_{\mathrm{E},k}$为对于发送给第k个PD的机密信号，窃听者的可达速率。若传输的机密信号在区间$[-1,1]$上均匀分布，可得$R_{\mathrm{D},k}$和$R_{\mathrm{E},k}$的表达式[18]为

$$R_{\mathrm{D},k}=\frac{1}{2}\log_2\left(4\lambda^2\sum_{i=1}^{K}\left|\boldsymbol{h}_{\mathrm{SD},i}^{\mathrm{T}}\boldsymbol{w}_k\right|^2+2\pi\mathrm{e}\sigma_{\mathrm{N}}^2\right)-\frac{1}{2}\log_2\left(\frac{2}{3}\pi\mathrm{e}\lambda^2\sum_{i=1,i\neq k}^{K}\left|\boldsymbol{h}_{\mathrm{SD},i}^{\mathrm{T}}\boldsymbol{w}_k\right|^2+2\pi\mathrm{e}\sigma_{\mathrm{N}}^2\right) \tag{17}$$

$$R_{\mathrm{E},k}=\frac{1}{2}\log_2\left(1+\gamma_{\mathrm{E},i_{\mathrm{E}},k}\right) \tag{18}$$

式中，$\lambda=\alpha_1\rho/K$，$\gamma_{E,i_{\mathrm{E}},k}$表示第$i_{\mathrm{E}}$个窃听者位置处的信干噪比，$i_{\mathrm{E}}=1,2,\cdots,I_{\mathrm{E}}$。

如图5所示，不同物理层安全方案的系统总保密容量空间分布呈现显著差异。系统平均安全容量为全区域窃听者位置下的系统保密速率总和的均值，对道路交叉口所有离散窃听位置(共120个采样点)的保密

速率总和取算术平均，从而量化该场景下系统安全性能的平均水平。实验数据表明，基础设施协同AN干扰方案较传统空间干扰方案有明显性能优势，系统平均安全容量提升0.68 bits/s/Hz。具体表现为：1）近场区域总容量受限，归因于窃听者高SINR的信道优势；2）随窃听距离增大，路径损耗效应主导导致总容量持续提升；3）当距离超过临界阈值后，总容量增速趋缓并渐近收敛于合法用户可达速率，符合Wyner安全定理的渐近收敛特性。实验结果证实方案在极端场景下仍具备可靠的安全通信保障。

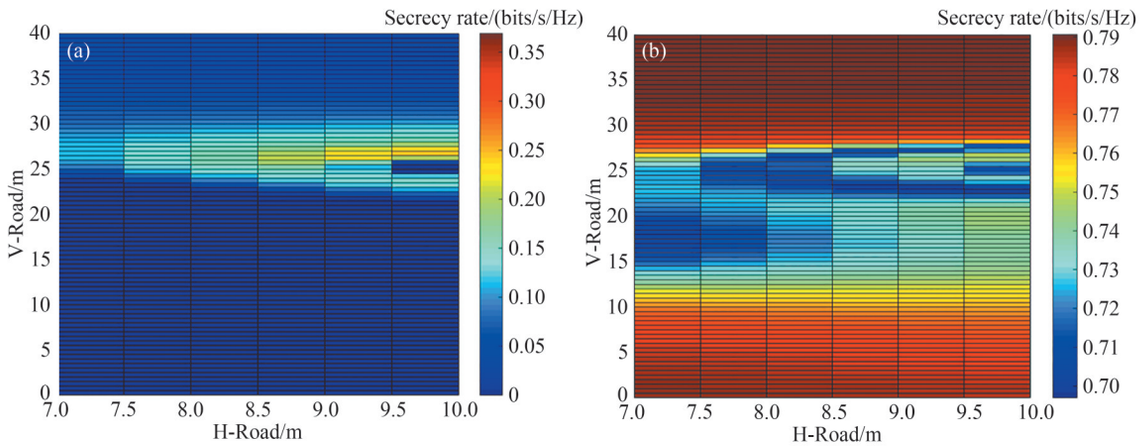


图5 不同方案下系统的保密速率总和。(a) 空间干扰方案；(b) 所提方案

Fig. 5 System secrecy sum-rate under different schemes. (a) Spatial jamming; (b) Proposed scheme

4 结论

本文针对车车可见光通信在开放道路场景下面临的物理层安全威胁，提出了一种基于基础设施协同的人工噪声干扰增强方案，以解决交叉路口等高动态区域中窃听者信号截获风险。通过联合优化源车辆与交通信号灯的干扰信号生成机制，在保障合法通信质量的前提下，实现了对潜在窃听者的多维度干扰抑制。仿真实验表明，所提方案将最坏情况窃听SINR抑制至－7.07 dB，较空间干扰方案降低8.77 dB，并且使窃听者SINR在全区域显著降低，其中近场窃听者SINR平均降幅达11.25 dB，远场窃听者SINR平均降幅达17.41 dB，同时系统保密速率有明显提高。相较于传统空间干扰方案，所提方案在典型城市道路场景下显著增强了V2V-VLC系统在复杂动态环境中的物理层安全防护能力。

参考文献

[1] AMINI C, AZMI P, KASHEF S S. PLS of relay-aided VLC with RIS-assisted eavesdropper[J]. IEEE Transactions on Wireless Communications, 2025: 3562119.

[2] GUO Jianing, WANG Chao, ZHANG Jian. Optimal constellation design for visible light communication with multi-color LED[J]. Acta Optica Sinica, 2025, 45(3): 0306005.
郭家宁, 王超, 张剑. 基于多色LED的可见光通信星座优化设计[J]. 光学学报, 2025, 45(3): 0306005.

[3] ELDEEB H B, ELAMASSIE M, SAIT S M, et al. Infrastructure-to-vehicle visible light communications: channel modelling and performance analysis[J]. IEEE Transactions on Vehicular Technology, 2022, 71(3): 2240-2250.

[4] YOU Xiaodi, ZHONG Yanjun, CHEN Jian, et al. Mobile channel estimation based on decision feedback in vehicle-to-infrastructure visible light communication systems[J]. Optics Communications, 2020, 462:125261.

[5] PLATTNER M, OSTERMAYER G. A camera-based vehicular visible light communication system using modulated taillights in public road scenarios[J]. Vehicular Communications, 2023, 43: 100651.

[6] LIU Sicong, LIU Xianbin, DU Xiaojiang, et al. Smart jamming for secrecy: deep reinforcement learning enabled secure visible light communication[J]. IEEE Transactions on Wireless Communications, 2024, 23(12): 3458046.

[7] RAPSON C J, SEET B C, CHONG P H J, et al. Safety assessment of radio frequency and visible light communication for vehicular networks[J]. IEEE Wireless Communications, 2019, 27(1): 186-192.

[8] MOUSA F I K, Al MAADEED N, BUSAWON K, et al. Secure MIMO visible light communication system based on user's location and encryption[J]. Journal of Lightwave Technology, 2017, 35(24): 5324-5334.

[9] XIE Qi, DING Zixuan, TANG Wen, et al. Provable secure and lightweight blockchain-based V2I handover authentication and V2V broadcast protocol for VANETs[J]. IEEE Transactions on Vehicular Technology, 2023, 72(12): 15200-15212.

[10] QIU Junchao, ZHANG Lin, LI Diyang, et al. High security chaotic multiple access scheme for visible light communication systems with advanced encryption standard interleaving[J]. Optical Engineering, 2016, 55(6): 066121.
[11] WANG Jinyuan, LIU Chen, WANG Junbo, et al. Physical-layer security for indoor visible light communications: Secrecy capacity analysis[J]. IEEE Transactions on Communications, 2018, 66(12): 6423-6436.
[12] LU Meng, WANG Fasong, LI Rui, et al. Physical layer security for indoor GSM VLC[J]. Digital Signal Processing, 2023, 132: 103824.
[13] KOMINE T, NAKAGAWA M. Fundamental analysis for visible-light communication system using LED lights[J]. IEEE Transactions on Consumer Electronics, 2004, 50(1): 100-107.
[14] TAKAYAMA Y, HASHIMOTO K, OHTSUKA T. STLCCP: Efficient convex optimization-based framework for signal temporal logic specifications[J]. IEEE Transactions on Automatic Control, 2025: 3555949.
[15] MA Yingjie, GAO Xi, LIU Chao, et al. Improved SQP and SLSQP algorithms for feasible path-based process optimisation[J]. Computers & Chemical Engineering, 2024, 188: 108751.
[16] SATORRES MARTÍNEZ S, MARTÍNEZ GILA D M, RICO S I, et al. Machine vision system for automatic adjustment of optical components in LED modules for automotive lighting[J]. Sensors, 2023, 23(21): 8988.
[17] CHO S, CHEN G, COON J P. Securing visible light communications with spatial jamming[C]. 2019 IEEE International Conference on Communications, IEEE, 2019: 1-6.
[18] YanglinBEN, CHEN Ming, CAO Binghao, et al. On secrecy sum-rate of artificial-noise-aided multi-user visible light communication systems[C]. 2021 IEEE International Conference on Communications Workshops, IEEE, 2021: 1-6.

Infrastructure-assisted Secure Vehicle-to-vehicle Visible Light Communications

XU Yuru, WU Yating, ZHENG Guoxin, SUN Yanzan
(*Key Laboratory of Specialty Fiber Optics and Optical Access Networks, Joint International Research Laboratory of Specialty Fiber Optics and Advanced Communication, Shanghai University, Shanghai* 200444, *China*)

Abstract: Vehicle-to-Vehicle Visible Light Communication (V2V-VLC) offers significant advantages in intelligent transportation systems, such as leveraging existing vehicular lighting, spectrum license exemption, low latency, and resistance to multipath interference. By transmitting critical information like vehicle position and driving instructions via LED light sources, V2V-VLC facilitates collaborative decision-making among vehicles. However, the open nature of optical transmissions exposes V2V-VLC to interception risks, leading to privacy breaches and traffic hazards. Current security measures primarily rely on higher-layer encryption and authentication, which fail to address vulnerabilities caused by physical-layer signal exposure. Physical Layer Security (PLS) complements existing methods by providing transparent protection across multiple data types. Yet, PLS research in VLC has been predominantly limited to static indoor environments, which are unsuitable for dynamic road scenarios characterized by high-speed mobility, variable topologies, and wide-beam light coverage. Particularly at intersections, extensive signal exposure and unpredictable eavesdropper locations exacerbate security risks.

This study proposes an Artificial Noise (AN) interference mechanism based on traffic infrastructure collaboration to minimize eavesdroppers′ Signal-to-Interference-plus-Noise Ratio (SINR) under worst-case conditions, thereby enhancing V2V-VLC security. To improve the physical-layer security of V2V-VLC in dynamic road environments, a collaborative AN jamming scheme coordinated by traffic infrastructure was introduced. As illustrated in Fig. 2, the source vehicle (S) transmits confidential data to the target vehicle (D) via LED headlights, while the traffic signal (J) concurrently emits controlled artificial noise. The jamming signals are optimized to avoid interference with legitimate vehicles while disrupting eavesdroppers′ reception. An optimization problem is formulated to minimize the worst-case SINR of eavesdroppers while maintaining the quality of legitimate communication. The concave-convex procedure (CCP) is employed to derive the optimal solution, ensuring effective suppression of eavesdropper signals and improving the system′s secrecy rate without degrading communication performance. Simulations validate the proposed scheme′s effectiveness in enhancing V2V-VLC security. Vehicle parameters are configured

as follows: the source vehicle′s LED headlights are mounted 0.8 m above the ground and spaced 1.6 m apart, while the receiver′s photodetector (PD) is installed on the target vehicle′s rear bumper, 0.8 m above the ground, with a field of view (FOV) of 60°. Detailed parameters are listed in Table 2. Results indicate that eavesdroppers′ SINR is highest near the source vehicle′s LED and decreases with distance due to path loss (Fig. 3). Localized SINR peaks occur near traffic signals due to the directional characteristics of their LEDs. The maximum SINR of eavesdroppers reaches −7.07 dB, 8.77 dB lower than the reference scheme (Table 3). Compared to traditional spatial jamming methods, the proposed scheme achieves superior SINR suppression across all regions. For near-field eavesdroppers, SINR is reduced by 11.25 dB and 10.61 dB in Scenarios 1 and 2, respectively. For far-field eavesdroppers, reductions of 17.12 dB and 17.41 dB are observed (Fig. 4). Furthermore, the system′s average secrecy capacity improves by 0.68 bits/s/Hz (Fig. 5). These findings confirm that minimizing the worst-case SINR effectively disrupts eavesdropper reception while preserving legitimate communication quality.

In summary, this study addresses physical-layer security challenges in V2V-VLC systems under dynamic road conditions. An infrastructure-assisted AN interference scheme is proposed to mitigate interception risks, particularly in high-risk areas like intersections. By optimizing interference generation from both source vehicles and traffic signals, the scheme achieves multidimensional suppression of eavesdropper signals while maintaining legitimate communication quality. Simulations show that the proposed method suppresses eavesdroppers′ worst-case SINR to −7.07 dB, 8.77 dB lower than traditional spatial jamming methods, with maximum SINR reductions of 11.25 dB and 17.41 dB for near-field and far-field eavesdroppers, respectively. The scheme also improves system secrecy capacity by 0.68 bits/s/Hz.

Compared to conventional methods, this approach offers superior physical-layer security for V2V-VLC systems in complex and dynamic road environments. Key innovations include: 1) Addressing security challenges in V2V-VLC systems with unknown and randomly distributed eavesdroppers at intersections. 2) Proposing a joint jamming scheme utilizing traffic infrastructure as a cooperative interference source, extending the spatial dimension of security. 3) Formulating and solving an optimization problem to minimize the worst-case SINR of eavesdroppers without interfering with legitimate users. This study provides theoretical and technical solutions for enhancing V2V-VLC security, laying a foundation for future research.

Key words: Visible light communication; Vehicle-to-vehicle communication; Physical layer security; Artificial noise; Secrecy rate

OCIS Codes: 060.2605; 060.4510; 060.2630

CSTR: 32255.14.gzxb20265501.0106007

Foundation item: Natural Science Foundation of Shanghai (22ZR1422200), National Key Research and Development Program Project (2022YFB2902005), Open Research Project of Shanghai Engineering Research Center of Unmanned Train Control System (SUTC-2024KT-04), 111 Project (D20031)