Secrecy Capacity and Pressure in Multiple-Lane Vehicle-to-Vehicle Visible Light Communication Channel: An Empirical Analysis

Farah Mahdi Al-Sallami, *Member, IEEE*, Harpreet Singh Ghatorhe, Xianglin Pu, Seong Ki Yoo, *Senior Member, IEEE*, Sujan Rajbhandari, *Senior Member, IEEE*, and Sinem Coleri, *Fellow, IEEE*

***Abstract*—In vehicle-to-vehicle visible light communication (V2V-VLC), the irregular shape of the vehicle headlight radiation pattern, dynamic traffic conditions and ambient noise variation at different times of the day contribute to a built-in physical-layer security (PLS) for the system. In this paper, we investigate the secrecy capacity of the V2V-VLC system based on an empirical model of the multiple-lane V2V-VLC configuration. The study considers the variations in the received optical power at positions that emulate the trajectories of vehicles obtained from the Next Generation Simulation (NGSIM) initiative of the Federal Highway Administration in the USA. In addition, we investigate the secrecy pressure that forecasts the probability of the eavesdropper (Eve) presence at certain positions around the legitimate receiver (Bob). Closed-form expressions of the lower and upper bounds on the secrecy capacity and secrecy pressure are derived and evaluated based on the measurements. The results confirm the inherent security characteristics of dynamic V2V-VLC systems using headlights as transmitters because the channel conditions between the transmitter (Alice) and Bob which differs from the conditions between Alice and Eve. The position-dependent channel conditions result in varying secrecy capacities across different lanes and relative positions of Bob and Eve to Alice. The attained secrecy capacity can reach up to 1 nats/s/Hz, corresponding to the scenario when Bob is in the highest received power area on the middle lane at a distance of 9 m from Alice, and Eve is in the lowest received power area on the right-hand lane with a separation distance of 40 m from Alice. The secrecy pressure on the middle lane is lower than the right-hand and left-hand lanes.**

***Index Terms*—Secrecy capacity, physical-layer security, empirical channel model, vehicular communications, visible light communication.**

I. Introduction

VEHICULAR communication has been proposed as an essential element of the intelligent transportation system. It facilitates an advanced driver-assistance system (ADAS) that promises safe driving conditions. In addition, it addresses challenges associated with carbon footprint, road fatality, and adaptive traffic management [1]–[3]. Various radio frequency (RF)-enabled vehicular technologies have been suggested for establishing ubiquitous vehicles-to-everything (V2X) connections [4]. However, the increasing demand for RF-based communication introduces susceptibility to interference and bandwidth limitations [5]–[7]. In response to these challenges, vehicle-to-vehicle visible light communication (V2V-VLC) systems emerged as complementary to RF-based wireless schemes in 6G and beyond. V2V-VLC utilizes vehicles' head and tail-lights to undertake inter-vehicular communications, freeing the RF spectrum for alternative applications and reducing co-band interference [7].

The configuration of V2V-VLC links depends heavily on the geometry of street layouts and the radiation pattern of vehicle lights [7], [8]. Because of its irregular radiation pattern, this study focuses specifically on the headlights, which introduce geometric variations reinforced by vehicle movement. Additionally, the channel response undergoes fluctuating gain due to vehicles moving at various speeds and manoeuvring between lanes. This results in potentially unique position-dependent channel conditions between legitimate transmitters and receivers which distinct from those between the transmitter and the eavesdropper. This observation supports the hypothesis of a potential built-in physical-layer security (PLS) in V2V-VLC employing headlights as transmitters. Security is a pivotal requirement for communication between legitimate transmitters and receivers in vehicular systems in the presence of surrounding vehicles that could potentially eavesdrop the link, passively or actively [9]–[11].

The following section reviews relevant literature that delves into works related to VLC PLS and secrecy capacity under transmitted optical peak and average power constraints.

A. Related Works

Secrecy performance of indoor VLC systems were extensively investigated in the literature. The works in [12], [13] studied PLS of indoor VLC systems and derived the secrecy capacity assuming a static legitimate transmitter (Alice), legitimate receiver (Bob) and eavesdropper (Eve). The studies considered the amplitude constraint without considering the average power constraint. The works in [14], [15] investigated the secrecy capacity of indoor VLC systems subject to amplitude and average power constraints. The works in [16],

F. M. Al-Sallami is with the School of Electronic and Electrical Engineering, University of Leeds, Leeds, UK. (E-mail: f.al-sallami@leeds.ac.uk).

H. S. Ghatorhe is with the School of Future Transport, Coventry University, Coventry CV1 5FB, UK. (E-mail: ghatorheh@uni.coventry.ac.uk.

X. Pu is with the School of Electronic and Electrical Engineering, University of Leeds, Leeds, UK and Dept of Electrical Engineering, Columbia University, New York, USA. (E-mail: xp2221@columbia.edu.

S. K. Yoo is with the Centre for Future Transport and Cities, Coventry University, Coventry CV1 5FB, UK. (E-mail: ad3869@coventry.ac.uk).

S. Rajbhandari is with the Institute of Photonics, University of Strathclyde, Glasgow G1 1RD, UK (E-mail: sujan.rajbhandari@strath.ac.uk)

S. Coleri is with the Department of Electrical and Electronics Engineering, Koc¸ University, Istanbul 34450, Turkey (e-mail: scoleri@ku.edu.tr).

[17] considered PLS for indoor VLC systems when Eve has random location. In [16], the secrecy outage probability of the system was derived considering the randomness of Eve position, while the legitimate receiver location was fixed. In [17], the secrecy performance was derived for randomly located colluding Eve. In [18], the upper and lower bounds on secrecy capacity were derived for indoor 3-D mobile multiuser VLC-based network, where the locations of the users and access points (APs) were modeled as 2-D independent and homogeneous Poisson point processes at distinct heights. The study revealed that while cooperation among APs offers only a marginal increase in secure rate, overall securing the zones surrounding APs significantly improves the security of the network. In [19], the average achievable secrecy rate was derived for the single-input-multiple-output (SIMO) indoor VLC wiretap channel when channel input is characterized by a truncated generalized normal (TGN) distribution. Eve was assumed to be static and randomly located. Furthermore, authors in [20] derived the average achievable secrecy rate for the multiple-input-multiple-output (MIMO) when channel input is characterized by a truncated discrete generalized normal (TDGN) distribution and Eve was assumed to be static and randomly located. All the aforementioned studies utilised Lambertian model, which is appropriate for describing the radiation pattern of indoor light, but not suitable for V2V-VLC systems due to the asymmetrical nature of the headlight emission pattern.

Several PLS techniques were proposed for indoor VLC systems in the literature. Compared with RF communication system, VLC has inherent advantages. The low-power signal transmitted from VLC sources, such as light emitting diodes (LEDs), is less susceptible to eavesdropping, as it can be physically blocked or requires a certain distance from the legitimate receiver to intercept. Beamforming was proposed to secure transmission in VLC systems. Compared to RF signals, it is challenging to steer the optical signal without employing optical components, such as lenses and reflectors. Hence, [21] used optical lenses to confine the transmitting light into certain area to achieve PLS. Similarly, [22] shows angle-diversity of transmitter improves the secrecy. In aforementioned approaches, there are still chances for Eve to receive the signal if it is positioned close to the legitimate receiver. Therefore, [23] used friendly jamming signal to further increase the secrecy of the legitimate channel. The work in [24] used artificial noise (AN) directed to legitimate receiver's null space by using multiple-input-single-output (MISO) system. This ensures that only legitimate receiver can receive information bearing signal with good signal-to-interference-noise ratio (SINR), while Eve may still receive the signal but with degraded noisy channel. In [25], reinforcement learning (RL)-based beamforming method was used to secure MISO indoor VLC system. This study considered the indoor channel model which relies on the Lambertian model.

Innovative PLS concepts for indoor VLC systems were presented by the recent works in [26]–[28]. An intelligent reflecting mirror array (IRMA)-aided PLS for indoor VLC systems was proposed in [26]. The study established the secrecy capacity when the average and peak constraints were imposed and when average and optical intensity constraints were considered. In order to improve secrecy capacity, the study optimised the IRMA assignment technique. A Chinese reminder theorem (CRT)-based PLS was used for DC-biased optical-orthogonal frequency division multiplexing (DCO-OFDM) in [27]. In order to reduce the clipping noise, the study recovered the original, undistorted OFDM time samples using a Bayesian estimation. The study in [28] suggested an RL algorithm to optimise the MISO VLC system's PLS precoder and M-PAM modulation order. The RL agent's reward was designed to maximize Bob's secrecy capacity while minimising the bit-error rate (BER) at Eve. The method assumes that Bob and Eve have a perfect knowledge of the CSI channels.

These research efforts were limited to indoor environment often assuming static transmitters, receivers and eavesdroppers. None of these previous studies investigated the security of outdoor V2V-VLC system, considering the irregular radiation pattern of the headlights and geometric variations of the link due to vehicle movement [2], [29].

Several empirical studies provided experimental evidence for the V2V-VLC system. The study in [30] conducted an experiment to examine the feasibility of simultaneously transmitting the same data packet from two vehicles' fog lights. Compared to V2V-VLC systems with a single channel, the results demonstrated a transmission angle enhancement of ten degrees. The achievable transmission distance was 10 m. According to the experimental investigation in [31], 10 kbps is achievable over a 30 m distance. The receiver employed a colour filter to reduce the interference and denoise the optical signal. In [32], a cooperative V2V-VLC system that implemented DCO-OFDM-based MIMO transmission scheme was proposed. The empirical results showed a transmission distance between 2 m and 20 m. The study in [33] proposed a machine learning (ML)-based framework for channel modeling in V2V-VLC system, incorporating multiple mobility and environmental variables to improve path loss and channel frequency response accuracy. Comparing the performance of several ML methods, the model with multilayer perception neural network (MLP-NN) method achieved significantly better accuracy than traditional stochastic models, with root mean square error (RMSE) as low as 3.53 dB. The study in [34] used an optical lens to achieve a distance of 20 m. The work in [35] showed that an error-free bidirectional transmission with baud rates of 28-57 kbaud can be achieved over a distance of 12 m. A data rate of 8.23 Mb/s was demonstrated in [36] at a distance of 50 m between the transmitter and receiver. A MISO was shown in the experimental investigation in [37] when both vehicles travelled at a speed of 20 km/h; the experiment revealed an average delivered packet rate (DPR) of 89.58%. The study in [38] carried out measurements to characterize the infrastructure-to-vehicle VLC channel. The results showed that a probability of error of 10^{-3} is achievable at 30 m distance from the transmitter. In [39], the average bounds on channel capacity were established. The study relied on empirical measurements to model the channel variation due to dynamic traffic during different times of the day. The study revealed that log-normal distribution describes the variation closely. While all of these studies showed that communication

links are feasible, none of them conducted a practical research on the physical layer security of V2V communication.

B. Motivation and Original Contribution

This study is motivated by the need to fill the existing research gap in lack of understanding of secrecy capacity in V2V-VLC. The main objective is to investigate whether the asymmetrical emission pattern of vehicle headlights, coupled with the dynamic movement of vehicles at various speeds and maneuvering between lanes offer a built-in security in V2V-VLC systems.

The novelty and original contributions of this study are as follows:

- We carry out experimental measurements to determine the spatial distribution of received power in a dynamic multiple-lane V2V-VLC system, for the first time in the literature. Measurements are conducted over six days, considering realistic positions based on real-world traffic data from the Next Generation Simulation (NGSIM). The dataset comprises microscopic (second-by-second) vehicle trajectories with coordinates of moving vehicles on Lankershim Boulevard in Los Angeles, California, USA.
- We derive the closed-form expressions for the lower- and upper-bound on secrecy capacity in V2V-VLC systems, for the first time in the literature. The study is the first work to consider the non-negative real value of the optical signal and the average optical power constraints to derive the secrecy capacity expressions for the V2V-VLC system.
- We determine the lower- and upper-bound secrecy capacity of the V2V-VLC system considering the dynamic traffic and variable locations of Bob and Eve on different lanes, for the first time in the literature. The study is the first work that considers the measurement-based characteristics of asymmetric headlight radiation pattern and the dynamic nature of the V2V-VLC system in determining the upper and lower bounds of secrecy capacity.
- We determine the secrecy pressure for the V2V-VLC system considering the dynamic traffic, for the first time in the literature. This metric quantifies the spatial average of the secrecy capacity over the probability of the coexistence of Eve on the adjacent lanes. The study is the first work that considers Eve's traffic measurement-based probabilistic location in the V2V-VLC system.

The rest of the paper is organized as follows. The V2V-VLC empirical channel model is presented in Section II. The secrecy capacity bounds on the V2V-VLC channel are derived in Section III. Numerical results are provided in Section IV. Finally, conclusions are given in Section VI.

II. Empirical channel model for V2V-VLC

A realistic channel model is required to accurately estimate the secrecy capacity of V2V-VLC system. The model characterizes the impact of dynamic traffic and the irregular radiation pattern of the headlight on the received optical power across different lanes and inter-vehicular distances under various outdoor and weather ambient noise conditions.

Fig. 1 depicts the experimental setup designed to measure the received power of V2V-VLC across various lanes and positions, emulate a typical urban road with an asphalt-coated surface. The measurement campaign was conducted in an 11 m $\times$ 60 m size outdoor in an open road between two buildings. The measurements were collected between 15:00 and 18:00 hours in Coventry, UK, over six days. Table. I gives experiment dates and the number of vehicle trajectories on each day. A microscopic traffic dataset gathered on June 16, 2005, from the NGSIM initiative of the Federal Highway Administration, provides vehicle trajectories' x and y coordinates along Lankershim Boulevard in Los Angeles, California, USA [40]. The Dataset provides time-sampled detailed trajectories at a resolution of 10 samples per second, resulting in vehicles' coordinates every one-tenth of the second. This dataset also offers detailed information about driving dynamics and styles, including lane changes, speed, and acceleration. Therefore, low-speed vehicles have closer trajectory samples, while high-speed vehicles have larger gaps between trajectory samples. This facilitates reproducing vehicle trajectories by marking these samples on the measurement area floor, as illustrated in Fig. 2. Hence, power measurements simulate realistic spatial variation of the optical power along a vehicle's trajectory.

The temporal variation of vehicle position (0.1 seconds) [40] and VLC channel with coherence time (in millisecond) [41], [42] are considerably slower than the symbol duration of micro to nanosecond [41], [42]. Hence, it is reasonable to assume that the channel remains constant during the transmission block with codewords shorter than the coherence time of the channel [43]. This allows the channel state information and, hence, the optical power measurements to be considered time-invariant [43], [44] and collected at specific trajectory samples (measurement spots), as illustrated in Fig. 2. In total, 513 measurements were collected, effectively capturing the realistic spatial variation of the optical power along a vehicle's trajectory.

This study analyses the trajectories of 45 vehicles, as depicted in Fig. 3. This figure shows the dynamic nature of the traffic, where some vehicles follow a straight path along the lane while others maneuver and change lanes. The received power was analysed assuming the vehicles traverse the experiment field while maintaining a safety brake distance of 5 m from the headlight position. According to experimental studies [30], [31], [34], [36], [37], the maximum achieved transmission distance in V2V-VLC system is 50 m as reported in [36]. Hence, the measurements considered trajectories between 5 m and 55 m from the headlights.

According to US highways, the measurement area was divided into three lanes of 3.65 m (12 feet) width. However, the lanes were swapped because the traffic data belonged to a right-hand drive American system. Therefore, the traffic statistics for the first lane in the US were assumed to correlate to the third lane in the UK arrangement, and vice versa.

The transmitter consisted of headlights from a Ford Fiesta 2002-2005, equipped with H4 LED equivalent bulb to replace

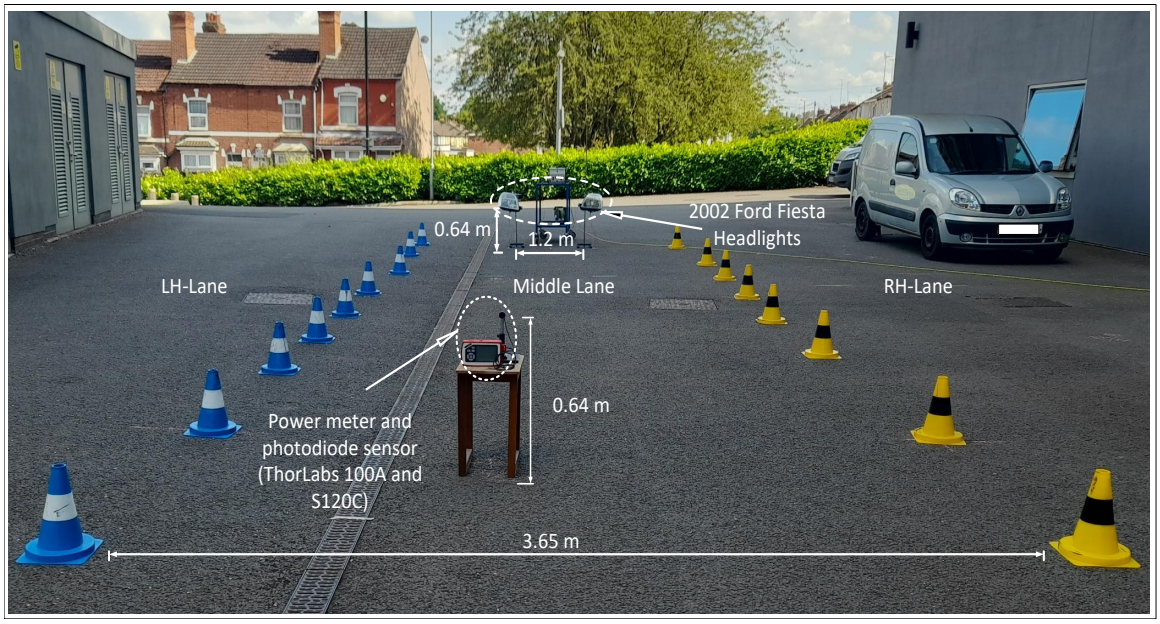


Fig. 1: The measurement setup.

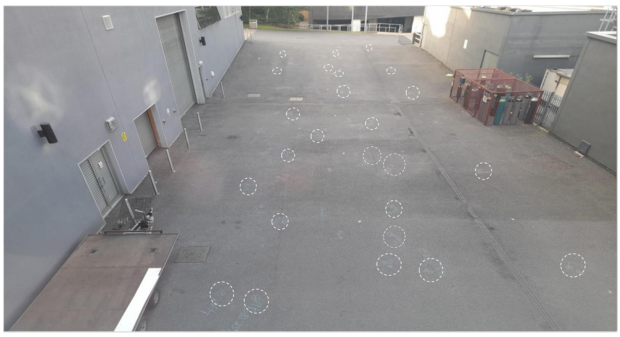


Fig. 2: Example measurement locations.

TABLE I: Experiment dates

Date of experiment	No. of vehicles trajectories
06/14/2023	2
06/16/2023	7
06/21/2023	11
06/26/2023	10
07/05/2023	10
07/06/2023	5
TOTAL	45

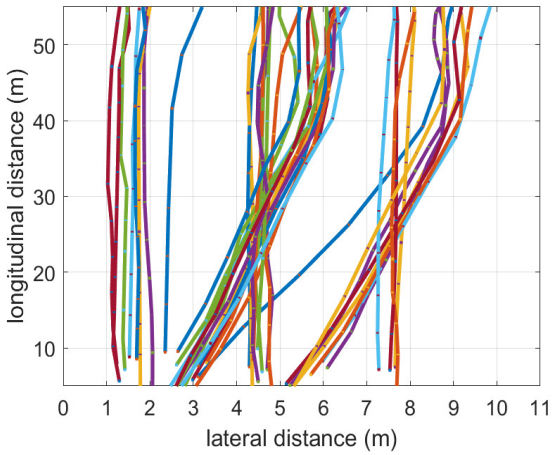


Fig. 3: Movement patterns and trajectories of vehicles on different lanes of the road.

the original low and high-beam halogen lamps. Prior to measurements, the alignment of the headlights was adjusted to comply with the ECE R112 regulations [45]. The headlights were horizontally separated by 1.2 m and mounted at a height of 0.64 m. The headlight was positioned at the beginning of the central lane, with coordinates (5.5 m, 0 m) within the measurement area's x-y plane. Mounted at the same height of the headlight, a power meter console connected to a photodiode sensor (Thorlabs 100D [46] and S120C [47]) was used to measure the received optical power. The measurements were conducted without direct exposure of the area and sensor to sunlight.

Fig. 4 shows a map of the average received power on right-hand (RH), middle and left-hand (LH) lanes from different vehicles. The map reveals a variation in power between lanes and along the lane, with distinct decay patterns. The power values observed in the right-hand lane were higher than those recorded in the middle and right-hand lanes. It decreases faster along the left-hand lane. This observation can be attributed to the UK-based headlight design employed in the experiment. In line with the right-hand driving scheme common in the UK, these headlights are designed to focus their low-beam, which has a shorter range, more on the left side of the road. Conversely, the high-beam illuminates the middle lane for longer distances.

III. Secrecy capacity and pressure in V2V-VLC

After characterizing the spatial distribution of the received power per lane in the previous section, this section focuses on

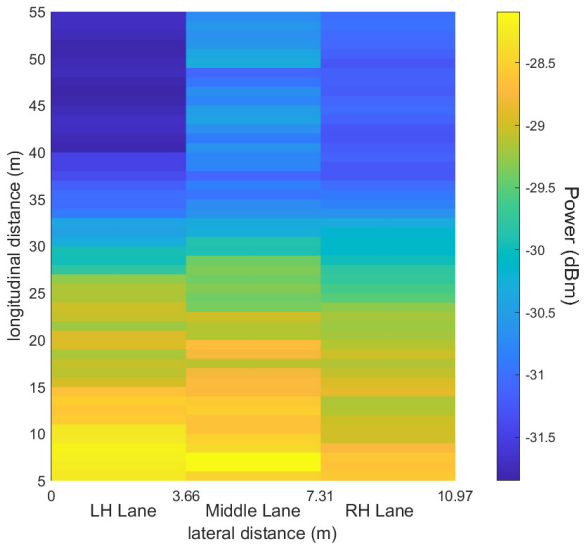


Fig. 4: Average received power map per lane.

deriving the lower and upper bounds of secrecy capacity and pressure.

The system consists of a transmitter vehicle (Alice), a legitimate receiver vehicle (Bob), and a passive eavesdropper vehicle (Eve) that also receives Alice's signals. If Alice's headlights are utilized for transmission with low-beams and high-beams modulated by the same electrical signal without using secret-key encryption, the received intensity signals at Bob and Eve, respectively, are given by

$$Y = h_B \gamma_B X + n_B, \tag{1}$$

$$Z = h_E \gamma_E X + n_E, \tag{2}$$

where X is the transmitted optical signal; γ_B and γ_E are the responsivity of the receiver at Bob and Eve, respectively; h_B is the main channel gain between Alice and Bob; h_E is the eavesdropping channel gain between Alice and Eve; n_B and n_E are independent and identically distributed additive white Gaussian noise (AWGN) at Bob and Eve, each with zero mean and a variance of σ_n^2.

The system employs intensity modulation and direct detection (IM/DD). Hence, X must be positive (i.e., $X > 0$). In addition, safety and practical considerations impose restrictions on both the average and peak power of the transmitted optical signal. These constraints stated that the probability of optical peak power exceed a predetermined value A ($P_r[X > A]$) and average optical power $E[X]$ satisfy the following conditions [43], [48]:

$$P_r[X > A] = 0, \tag{3}$$

$$E[X] \leq \mathcal{E}, \tag{4}$$

where $\mathcal{E}$ is a constant. In addition, the ratio between $\mathcal{E}$ and A is defined as

$$\alpha \triangleq \frac{\mathcal{E}}{A}, \tag{5}$$

where $\alpha \in$[0,1].

In Wyner's wiretap channel, secure communication between Alice and Bob over a noisy, memoryless channel is achievable. The secrecy capacity is defined as the difference between the supremum of the mutual information between the channel input X and the output Y at Bob and the mutual information leakage between X and the output Z at Eve across all input Laws:

$$\begin{aligned} C_s(A,\mathcal{E}) &= \sup_{\mathbb{P}_X}(I(X,Y) - I(X,Z)) \\ s.t. &\int_0^\infty \mathbb{P}_X(x)dx = 1 \\ &P_r[X > A] = 0 \\ &E[X] \leq \mathcal{E}, \end{aligned} \tag{6}$$

where $\mathbb{P}_X(x)$ is the distribution of X.

In the following sections, we present upper and lower bounds on the secrecy capacity $C_s(A,\mathcal{E})$ using different methods and considering A and $\mathcal{E}$ constraints.

A. The secrecy capacity lower bound

The lower bound on channel secrecy capacity is derived under the condition that the difference of the supremum of functions is less than the supremum of the difference of functions [13], [15].

The lower bound of Eq. (6) is expressed as

$$\sup_{\mathbb{P}_X}(I(X,Y) - I(X,Z)) \geq \sup_{\mathbb{P}_X}(I(X,Y)) - \sup_{\mathbb{P}_X}(I(X,Z)). \tag{7}$$

By definition, Eq. (7) indicates that the lower bound on the secrecy capacity is given by the difference between the channel capacity lower bound at Bob and the channel capacity upper bound at Eve [29]. Since the properties of channel capacity with a peak constraint are similar to those with average and peak constraints when $\mathcal{E} = \frac{A}{2}$, studying the channel capacity under $\alpha < 0.5$ is sufficient to determine Bob's and Eve's channel capacity [43].

Considering the channel capacity lower and upper bounds in [48], Eq. (7) is given by:

$$\begin{aligned} C_s(A,\mathcal{E}) \geq{}& \frac{1}{2}\ln\left(1+\frac{h_B^2A^2e^{2\mu^*}}{2\pi e\sigma_B^2}\left(\frac{1-e^{-\mu^*}}{\mu^*}\right)^2\right) - \frac{\delta e^{\frac{\delta}{2\sigma_E^2}}}{\sqrt{2\pi}\sigma_E} \\ &-\mu\alpha\left(1-2Q\left(\frac{\delta+\frac{Ah_E}{2}}{\sigma_E}\right)\right) - \frac{\sigma_E\mu}{Ah_E\sqrt{2\pi}}\left(e^{-\frac{\delta^2}{2\sigma_E^2}} - e^{\frac{-(A+\delta)^2}{2\sigma_E^2}}\right) \\ &-Q\left(\frac{\delta}{\sigma_E}\right)+\frac{1}{2}-\left(1-Q\left(\frac{\delta+\alpha h_EA}{\sigma_E}\right)-Q\left(\frac{\delta(1-\alpha)h_EA}{\sigma_E}\right)\right) \\ &\ln\left(\frac{Ah_E\left(e^{\frac{\mu\delta}{Ah_E}} - e^{-\mu(1+\frac{\delta}{Ah_E})}\right)}{\sqrt{2\pi}\sigma_E\mu\left(1-2Q\left(\frac{\delta}{\sigma_E}\right)\right)}\right), \end{aligned} \tag{8}$$

where, $\delta = \sigma_n \ln(1 + (A/\sigma_n))$, $\sigma_n = \sigma_B = \sigma_E$, $\mu = \mu^*(-e^{\alpha\delta^2/2\sigma_n^2})$, Q$(\cdot)$ is the Q-function and $\mu^* > 0$ is an optimized parameter given as a unique solution of $\alpha = 1/\mu^* - \mu^*/(1 - e^{-\mu^*})$ [43], [48].

Alternatively, considering the entropy-power inequality (EPI), the lower bound on C_s is given by

$$\begin{aligned} C_s(A,\varepsilon) &= \sup_{\mathbb{P}_X}(I(X,Y)-I(X,Z)) \\ &= \sup_{\mathbb{P}_X}(\mathcal{H}(Y)-\mathcal{H}(Y|X)-\mathcal{H}(Z)+\mathcal{H}(Z|X)) \\ &\geq \sup_{\mathbb{P}_X}(\mathcal{H}(Y)-\mathcal{H}(Z)) \\ &\geq \sup_{\mathbb{P}_X}\left(\frac{1}{2}\ln\left(\frac{e^{2\mathcal{H}(h_B X)}+e^{2\mathcal{H}(n_B)}}{2\pi e\mathbb{VAR}(Z)}\right)\right), \end{aligned} \tag{9}$$

where $\mathcal{H}(\cdot)$ and $\mathbb{VAR}(\cdot)$ denotes the differential entropy and variance, respectively. The lower bound in Eq. (9) is derived by dropping the supremum and selecting an input distribution $\mathbb{P}_X$ that yield a tight lower bound [49]. In [13], $\mathbb{P}_X$ was assumed to have a uniform distribution over [-A,A], and the lower bound in Eq. (9) is determined as

$$C_s(A,\varepsilon) \geq \frac{1}{2}\ln\left(\frac{6h_B^2A^2+3\pi e\sigma_B^2}{\pi e h_E^2A^2+3\pi e\sigma_E^2}\right). \tag{10}$$

B. The secrecy capacity upper bound

The duality principle is used to derive the upper bound on the secrecy capacity of the V2V-VLC channel.

The upper bound on the secrecy capacity is given by the expectation $E_{\mathbb{P}_X,\mathbb{P}_{Z|X}}$ (over a capacity maximizing input distribution $\mathbb{P}_X$ and eavesdropping minimizing conditional distribution, $\mathbb{P}_{Z|X}$) of the relative entropy $D(\cdot||\cdot)$ between the degraded Gaussian wiretap channel $f_{Y|X,Z}(y|X,Z)$ and the conditional distribution $g_{Y|Z}(y|Z)$. It is mathematically expressed as [49]

$$C_s(A,\varepsilon) \leq E_{\mathbb{P}_X,\mathbb{P}_{Z|X}}\left[D(f_{Y|X,Z}(y|X,Z)||g_{Y|Z}(y|Z))\right]. \tag{11}$$

Theorem 1: Using the duality principle, the upper secrecy bound is given as:

$$C_s(A,\varepsilon) \leq \frac{1}{2}\ln\frac{(\sigma_E^2-\frac{h_E^2}{h_B^2}\sigma_B^2)(h_B^2A\varepsilon+\sigma_B^2)}{\sigma_B^2(h_E^2A\varepsilon+\sigma_E^2)\left(1-\frac{h_E^2\sigma_B^2}{h_B^2\sigma_E^2}\right)}. \tag{12}$$

Proof: See Appendix A.

From the lower bound and upper bound equations given by Eq. (8) and Eq. (12), respectively, a secure transmission can be achieved when $h_B > h_E$. Otherwise, the physical-layer security fails.

C. Secrecy pressure

Secrecy pressure is a metric proposed in [50] to forecast the probability of Eve's presence and its impact on the secrecy capacity. The metric aims to eliminate the dependency of the secrecy capacity on Eve's position by calculating the spatial average instead of the conventional temporal average of the secrecy capacity. Considering the importance of the link geometry directly affected by Eve's probabilistic location in Bob's vicinity establishing this metric is crucial for the V2V-VLC system. As this system is confined by the road, the presence and absence of Eve in the adjacent lanes can be inferred from the probability of the coexistence of other vehicles in those lanes, denoted by L [51]. In this case, L acts as an indicator of Eve's (hence, their channel h_E) existence. Therefore, the upper bound on the secrecy capacity in Eq. (12) is rewritten as

$$C_s(A,\varepsilon,L) \leq \frac{1}{2}\ln\frac{(\sigma_E^2-\frac{Lh_E^2}{h_B^2}\sigma_B^2)(h_B^2A\varepsilon+\sigma_B^2)}{\sigma_B^2(Lh_E^2A\varepsilon+\sigma_E^2)\left(1-\frac{Lh_E^2\sigma_B^2}{h_B^2\sigma_E^2}\right)}. \tag{13}$$

Based on realistic traffic measurements in [51], L was shown to have a log-normal distribution that is expressed as

$$P_L(L) = \frac{1}{\delta_L\sqrt{2\pi}}\frac{1}{L}\exp\Big(-\frac{(\ln(L)-\mu_L)^2}{2\delta_L^2}\Big), \tag{14}$$

where μ_L and δ_L are the distribution parameters , which vary depending on the vehicle's position across different lanes.

The secrecy pressure, p_{sec}, as the spatial average of the secrecy capacity over Eve's presence in the adjacent lanes is given as

$$p_{\text{sec}} = \int_0^\infty C(A,\varepsilon,L)P_L(L)dL. \tag{15}$$

Theorem 2: The secrecy pressure is given as

$$\begin{aligned} p_{\text{sec}} &= 0.5\ln\left(\frac{h_B^2A\varepsilon}{\sigma_n^2}+1\right)-0.5\exp\left(\frac{-\mu_d^2}{2\delta_L^2}\right) \\ &\times\sum_{k=1}^{+\infty}\frac{(-1)^{k+1}}{k}\left[\text{erfcx}\left(\frac{\delta_L k}{\sqrt{2}}+\frac{\mu_d}{\sqrt{2}\delta_L}\right)+\text{erfcx}\left(\frac{\delta_L k}{\sqrt{2}}-\frac{\mu_d}{\sqrt{2}\delta_L}\right)\right] \\ &+\frac{2\delta_L}{\sqrt{2\pi}}\exp\left(-\frac{\mu_d}{2\delta_L^2}\right)+\mu_d\,\text{erfc}\left(-\frac{\mu_d}{\sqrt{2}\delta_L}\right), \end{aligned} \tag{16}$$

Proof: See Appendix B.

Having derived the lower and the upper bounds on the secrecy capacity of the V2V-VLC channel and the secrecy pressure, the following section presents the results of the system considering the empirical channel model in Section II at different relative locations of Bob and Eve.

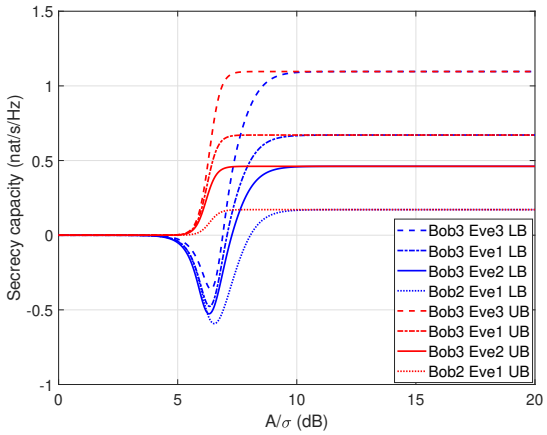


Fig. 5: The lower and upper bounds (LB and UB) on secrecy capacity. See Table. II for the label, position and received power.

TABLE II: Values of instantaneous locations of Bob and Eve and the received power at these locations.

Label	Receiver	Lane	Longitudinal position (m)	Received power (dBm)
Bob1	Bob	right-hand	43.3	-31.1
Bob2	Bob	middle-lane	29.3	-30.0
Bob3	Bob	left-hand	6.5	-27.8
Eve1	Eve	right-hand	55.4	-30.7
Eve2	Eve	middle-lane	34.1	-29.1
Eve3	Eve	left-hand	36.4	-32.6

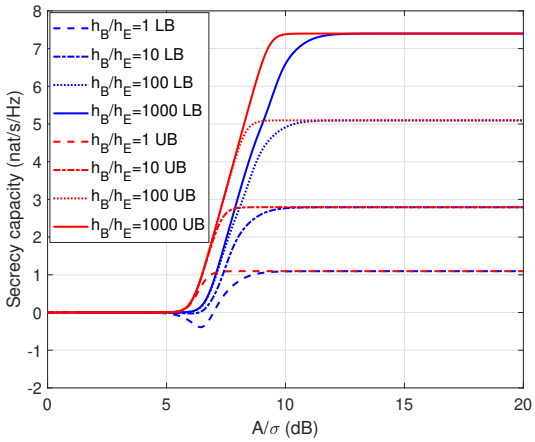


Fig. 6: The lower and upper bounds on secrecy capacity for different h_B/h_E values.

IV. NUMERICAL RESULTS AND DISCUSSION

The goal of this section is to evaluate the secrecy capacity bounds derived in Section III based on the measurements obtained in Section II. The evaluation considers realistic locations of Bob and Eve. The results are compared with the secrecy capacity bounds derived in [13] for indoor VLC systems.

The channel gain depends on the relative locations of Bob and Eve with respect to Alice, as illustrated in Fig. 4. We vary the peak signal to noise ratio, A/σ (dB) from 0 dB to 20 dB, $\alpha = 0.4$, according to the instantaneous locations of Bob and Eve, which are given in Table. II. The table provides numerical values of the received power (dBm) measured on different lanes and longitudinal distances as discussed in Section II and illustrated in Fig. 4.

Fig. 5 shows the lower bound and upper bound on secrecy capacity in Eq. (8) and Eq. (17) for different locations of Bob and Eve and the received power at these locations. It is obvious that the derived bound is tight for $A/\sigma > 10$ dB when different relative positions of Bob and Eve were considered. However, a noticeable gap between the lower and upper bounds is observed when 5 dB $< A/\sigma <$ 10 dB, where the lower bound takes negative values, indicating security failure. This performance is expected, given that the ratio h_B/h_E, according to our measurements, does not exceed 2. Higher secrecy capacity requires a higher disparity between the channels of Bob and Eve, hence, necessitating higher h_B/h_E values.

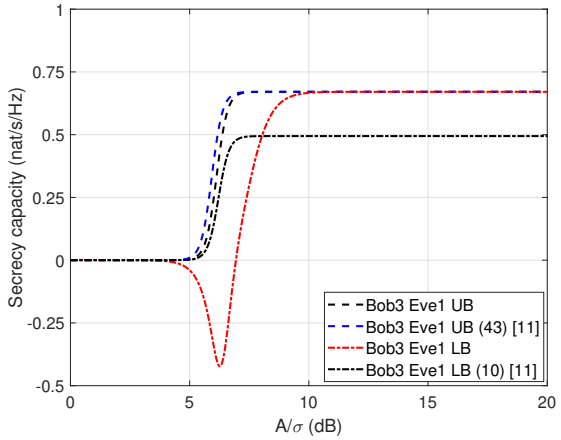


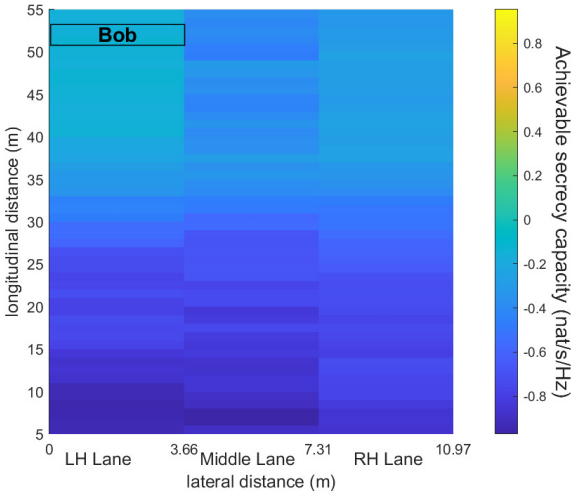
Fig. 7: A comparison between the lower and upper bounds on secrecy capacity in Eq. (8) and Eq. (12) with their counterparts in [13].

Fig. 6 depicts the secrecy capacity at different h_B/h_E values. As the figure indicates, to achieve at least 1 nat/s/Hz, the ratio h_B/h_E should be greater than or equal to 1. For example, when Bob is in the highest received power area on the middle lane at a distance of 9 m from Alice, and Eve is in the lowest received power area on the right-hand lane with a separation distance of 40 m from Alice, as illustrated in Fig. 4. Higher secrecy capacity is achievable at higher h_B/h_E values. For example, when $A/\sigma = 13$ dB, a secrecy capacity of 2.8 nat/s/Hz, 5.1 nat/s/Hz, and 7.4 nat/s/Hz can be achieved when the ratio h_B/h_E values are 10, 100, and 1000, respectively.

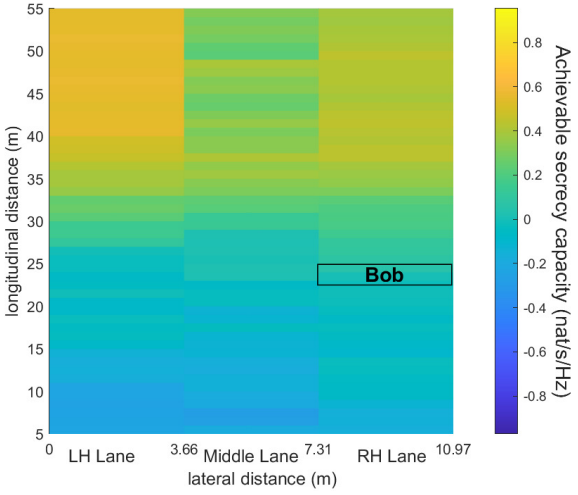
Fig. 7 provides a comparison between the lower and upper bounds in Eq. (8) and Eq. (12) with their counterparts in [13]. The upper bounds are close, with a noticeable gap observed when 5 dB$< A/\sigma <$ 8 dB. The upper bound gap diminishes when $A/\sigma >$ 8 dB, whereas the lower bound gap becomes more pronounced at higher SNR values. This performance difference is attributed to the contribution of α (given in Eq. (4)) to the lower bound in Eq. (8) and its absence in Eq. (10), considering the fact that [13] did not account for the average constraint in Eq. (4) and only considered the peak constraint in Eq. (3). In contrast, our derivations accounted for both safety constraints.

Fig. 8 illustrates the upper bound on secrecy capacity when Bob is positioned at locations with a) the lowest, b) median, and c) the highest received power values of -32.5 dBm, -29.3 dBm and -27.6 dBm, on the right-hand, left-hand and middle lanes and at longitudinal positions of 52.6 m, 24.0 m and 9.3 m, respectively. Eve could be positioned anywhere within the same road section. The figures reveal that the physical-layer security fails when Bob is in the darkest position, i.e., $h_B < h_E$. When Bob is in a position with high received power, i.e., $h_B > h_E$, a secrecy capacity is achievable throughout the road. When Bob is in the median position, security is achievable only if Bob is closer to Alice while Eve is farther apart.

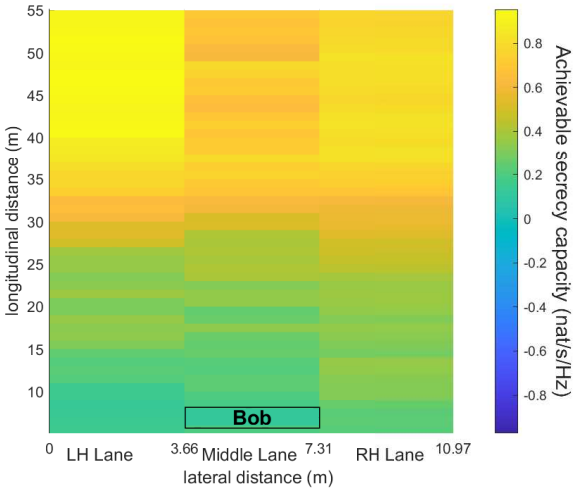
Fig. 8 assumes that Eve's position is unpredictable, with an equal probability of their existence on any lane at any time.



(a)



(b)



(c)

Fig. 8: The upper bound on secrecy capacity when Bob occupied a) lowest received power position on the right-hand lane, b) a median received power position on the left-hand lane and c) the highest received power position on the middle lane and Eve could be anywhere within the same road section.

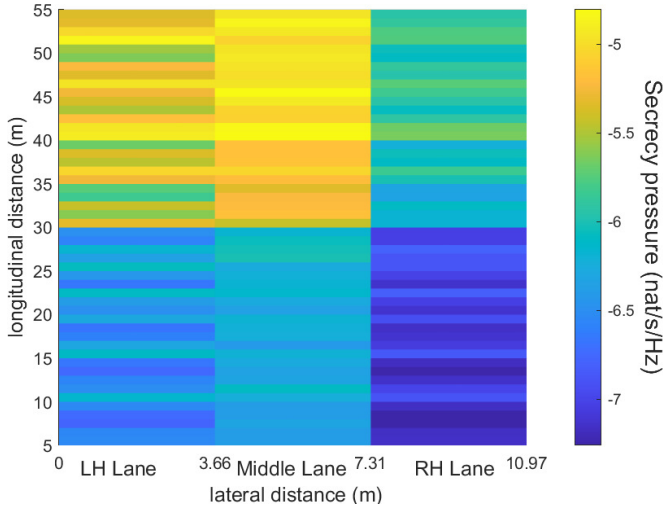


Fig. 9: Secrecy pressure.

However, considering a real traffic scenario studied in [51], the probability of coexistence of other vehicles in the adjacent lanes varies during the day, as shown in Table. III.

Fig. 9 shows the secrecy pressure in Eq.(16), when K=15 (according to the convergence analysis in Eqs.(27)-(30)), that accounts for the probabilistic presence of Eve in the adjacent lanes. The road is divided into two areas: a) high-density traffic area during peak hours from 5 m to 30 m, where the mean inter-vehicle distance is 12.37 m and b) low-density traffic area during off-peak hours from 30 m to 55 m with mean inter-vehicle distance of 48.72 m [52]. The figure illustrate six distinctive areas with varying secrecy pressure levels. Negative secrecy pressure shows the potential vulnerabilities (pressure) of PLS system due to Eve's existence. For example, in the high-density traffic area, secrecy pressure is higher when Bob is in the left-hand or right-hand lanes, while it is lower in the middle lane. This lower pressure in the middle lane is attributed to a lower probability of being surrounded by Eve, as indicated by Table. III, coupled with better channel conditions in the middle lane compared to left-hand or right-hand lanes and hence security pressure. Similarly, in the low-density traffic area, the middle lane exhibits lower pressure values than the other lanes and left-hand lane has the largest pressure value. This trend correlates with the mean values of L in Table. III. In the left-hand lane, although the channel conditions are poorer compared to other lanes, traveling in this lane during low-density traffic hours results in fewer surrounding vehicles, leading to lower security pressure. The secrecy pressure metric reveals that the radiation pattern of the headlight alone does not determine V2V link security. Considering the surrounding traffic is essential for generalizing the results and making them applicable to practical V2V-VLC communication. These results demonstrate that the radiation pattern of the headlight is not the only indicator of V2V link security and considering the surrounding traffic is crucial for comprehensive security assessment.

TABLE III: Parameters of the log-normal distributions that describes L [52].

Time	Lane	Mean Value (%)	μ_l	δ_l
00:00-03:00	left-hand	3.74	1.21	0.46
	middle	2.55	0.78	0.56
	right-hand	3.61	1.18	0.45
16:00-19:00	left-hand	19.9	2.71	0.70
	middle	16.7	2.44	0.87
	right-hand	17.4	2.58	0.74

V. Conclusions

This paper derives the upper and lower secrecy capacity and pressure for multiple-lane V2V-VLC channels. The study involves experimental measurements of the received power from vehicle headlights, capturing data from 45 accurate vehicle trajectories obtained from the NGSIM initiative of the Federal Highway Administration in the USA. The results reveal the inherent security of the system due to the vehicle headlight's irregular radiation pattern and vehicle positions on different lanes. Our closed-form expressions of secrecy capacity have been demonstrated to provide higher accuracy than those of the studies focusing on static indoor VLC. Moreover, a maximum secrecy capacity of 1 nat/s/Hz is achievable when the legitimate to wiretap channel ratio is beyond 1, and the security fails when the ratio is less than 1. However, evaluating V2V link security solely based on the headlight's irregular radiation pattern is insufficient without considering the probability of an eavesdropper (Eve) existing on adjacent lanes, which is captured by the secrecy pressure. The results of secrecy pressure analysis show that the middle lane offers higher security pressure compared to the left-hand and right-hand lanes. In addition, a key conclusion is that in a practical V2V-VLC, there is continuous pressure from the surrounding vehicles. Hence, although the headlight radiation pattern offers a physical security, further PLS techniques, such as beamforming, are required. This study recommend future implementation of physical-layer security scheme for V2V-VLC systems.

Acknowledgements

This work was supported by the Department of Science Innovation and Technology (DSIT) and the Engineering and Physical Sciences Research Council (EPSRC) under Grant EP/X040518/1 and EP/Y037421/1 (CHEDDAR). Dr Rajbhandari acknowledges the support by the Future Telecoms Research Hub, Platform for Driving Ultimate Connectivity (TITAN), sponsored by the Department of Science Innovation and Technology (DSIT) and the Engineering and Physical Sciences Research Council (EPSRC) under Grant EP/X04047X/1 and Grant EP/Y037243/1. Professor Sinem Coleri acknowledges the support provided by Ford Otosan.

References

[1] D. Hahn, A. Munir, and V. Behzadan, "Security and privacy issues in intelligent transportation systems: Classification and challenges," *IEEE Intelligent Transportation Systems Magazine*, vol. 13, no. 1, pp. 181–196, 2021.

[2] M. A. Arfaoui, M. D. Soltani, I. Tavakkolnia, A. Ghrayeb, M. Safari, C. Assi, and H. Haas, "Physical layer security for visible light communication systems: A survey," *IEEE Communications Surveys Tutorials*, pp. 1–1, 2020.

[3] G.-P. Antonio and C. Maria-Dolores, "Multi-agent deep reinforcement learning to manage connected autonomous vehicles at tomorrow's intersections," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 7, pp. 7033–7043, 2022.

[4] X. You, C.-X. Wang, J. Huang, X. Gao, Z. Zhang, M. Wang, Y. Huang, C. Zhang, Y. Jiang, J. Wang *et al.*, "Towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts," *Sci. China Inf. Sci.*, vol. 64, no. 1, pp. 1–74, Jan. 2021.

[5] M. Uysal, Z. Ghassemlooy, A. Bekkali, A. Kadri, and H. Menouar, "Visible light communication for vehicular networking: Performance study of a V2V system using a measured headlamp beam pattern model," *IEEE Vehicular Technology Magazine*, vol. 10, no. 4, pp. 45–53, Dec. 2015.

[6] B. Béchadergue, L. Chassagne, and H. Guan, "Simultaneous visible light communication and distance measurement based on the automotive lighting," *IEEE Transactions on Intelligent Vehicles*, vol. 4, no. 4, pp. 532–547, Aug. 2019.

[7] J. Chen and Z. Wang, "Topology control in hybrid VLC/RF vehicular Ad-Hoc network," *IEEE Transactions on Wireless Communications*, vol. 19, no. 3, pp. 1965–1976, Mar. 2020.

[8] S. Rehman, S. Ullah, P. Chong, S. Yongchareon, and D. Komosny, "Visible light communication: a system perspective—overview and challenges," *Sensors*, vol. 19, no. 5, p. 1153, Mar. 2019.

[9] D. Yu, S. Lee, R.-H. Hsu, and J. Lee, "Ensuring End-to-End Security With Fine-Grained Access Control for Connected and Autonomous Vehicles," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 6962–6977, 2024.

[10] G. Han, H. Choi, R. M. Kim, K. T. Nam, J. Choi, and T. A. Tsiftsis, "On the physical layer security of visible light communications empowered by gold nanoparticles," *Journal of Optical Communications and Networking*, vol. 16, no. 7, pp. 750–763, 2024.

[11] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6G security and privacy," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1094–1122, 2021.

[12] A. Mostafa and L. Lampe, "Physical-layer security for indoor visible light communications," in *2014 IEEE International Conference on Communications (ICC)*, 2014, pp. 3342–3347.

[13] A. Mostafa and L. Lampe, "Physical-layer security for MISO visible light communication channels," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 9, pp. 1806–1818, 2015.

[14] J.-Y. Wang, S.-H. Lin, C. Liu, J.-B. Wang, B. Zhu, and Y. Jiang, "Secrecy capacity of indoor visible light communication channels," in *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2018, pp. 1–6.

[15] J.-Y. Wang, C. Liu, J.-B. Wang, Y. Wu, M. Lin, and J. Cheng, "Physical-layer security for indoor visible light communications: Secrecy capacity analysis," *IEEE Transactions on Communications*, vol. 66, no. 12, pp. 6423–6436, 2018.

[16] S. Cho, G. Chen, and J. P. Coon, "Secrecy analysis in visible light communication systems with randomly located eavesdroppers," in *2017 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2017, pp. 475–480.

[17] S. Cho, and G. Chen, and J. Coon, "Physical layer security in visible light communication systems with randomly located colluding eavesdroppers," *IEEE Wireless Communications Letters*, vol. 7, no. 5, pp. 768–771, 2018.

[18] L. Yin and H. Haas, "Physical-layer security in multiuser visible light communication networks," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 1, pp. 162–174, 2018.

[19] M. A. Arfaoui, Z. Rezki, A. Ghrayeb, and M. S. Alouini, "On the secrecy capacity of MISO visible light communication channels," in *2016 IEEE Global Communications Conference (GLOBECOM)*, 2016, pp. 1–7.

[20] M. A. Arfaoui, A. Ghrayeb, and C. M. Assi, "Secrecy performance of the MIMO VLC wiretap channel with randomly located eavesdropper," *IEEE Transactions on Wireless Communications*, vol. 19, no. 1, pp. 265–278, 2020.

[21] O. Gürcüoğlu, M. C. Erdem, H. O. Çirkinoğlu, O. Ferhanoglu, G. K. Kurt, and E. Panayırcı, "Improved physical layer security in visible light communications by using focused light emitters," in *2021 29th Signal Processing and Communications Applications Conference (SIU)*, 2021, pp. 1–4.

[22] Z. Chen and H. Haas, "Physical layer security for optical attocell networks," in *2017 IEEE International Conference on Communications (ICC)*, 2017, pp. 1–6.

[23] A. Mostafa and L. Lampe, "Securing visible light communications via friendly jamming," in *2014 IEEE Globecom Workshops (GC Wkshps)*, 2014, pp. 524–529.

[24] M. A. Arfaoui, H. Zaid, Z. Rezki, A. Ghrayeb, A. Chaaban, and M.-S. Alouini, "Artificial noise-based beamforming for the MISO VLC wiretap channel," *IEEE Transactions on Communications*, vol. 67, no. 4, pp. 2866–2879, 2019.

[25] L. Xiao, G. Sheng, S. Liu, H. Dai, M. Peng, and J. Song, "Deep Reinforcement Learning-Enabled Secure Visible Light Communication Against Eavesdropping," *IEEE Transactions on Communications*, vol. 67, no. 10, pp. 6994–7005, 2019.

[26] J.-Y. Wang, L.-H. Hong, N. Liu, H.-N. Yang, P. Feng, and J. Ren, "Secrecy Analysis and Optimization for IRMA- and Jammer-Aided Visible Light Communications," *IEEE Wireless Communications Letters*, vol. 13, no. 7, pp. 1908–1912, 2024.

[27] E. Panayirci, E. B. Bektas, and H. V. Poor, "Physical Layer Security With DCO-OFDM-Based VLC Under the Effects of Clipping Noise and Imperfect CSI," *IEEE Transactions on Communications*, vol. 72, no. 7, pp. 4259–4273, 2024.

[28] D. M. T. Hoang, T. V. Pham, A. T. Pham, and C. T. Nguyen, "Joint Design of Adaptive Modulation and Precoding for Physical Layer Security in Visible Light Communications Using Reinforcement Learning," *IEEE Access*, vol. 12, pp. 82 318–82 332, 2024.

[29] G. Blinowski, "Security of Visible Light Communication systems—A survey," *Physical Communication*, vol. 34, pp. 246–260, 2019.

[30] B. Turan, S. Ucar, S. C. Ergen, and O. Ozkasap, "Dual channel visible light communications for enhanced vehicular connectivity," in *2015 IEEE Vehicular Networking Conference (VNC)*, 2015, pp. 84–87.

[31] Jong-Ho Yoo and Rimhwan Lee and Jun-Kyu Oh and Hyun-Wook Seo and Ju-Young Kim and Hyeon-Cheol Kim and Sung-Yoon Jung, "Demonstration of vehicular visible light communication based on LED headlamp," in *2013 Fifth International Conference on Ubiquitous and Future Networks (ICUFN)*, 2013, pp. 465–467.

[32] O. Narmanlioglu, B. Turan, S. C. Ergen, and M. Uysal, "Cooperative mimo-ofdm based inter-vehicular visible light communication using brake lights," *Computer Communications*, vol. 120, pp. 138–146, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366417305029

[33] B. Turan and S. Coleri, "Machine learning based channel modeling for vehicular visible light communication," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 10, pp. 9659–9672, 2021.

[34] B. Aly, M. Elamassie, and M. Uysal, "Vehicular VLC Channel Model for a Low-Beam Headlight Transmitter," in *2021 17th International Symposium on Wireless Communication Systems (ISWCS)*, 2021, pp. 1–5.

[35] M. Meucci, M. Seminara, T. Nawaz, S. Caputo, L. Mucchi, and J. Catani, "Bidirectional Vehicle-to-Vehicle Communication System Based on VLC: Outdoor Tests and Performance Analysis," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 8, pp. 11 465–11 475, 2022.

[36] D.-R. Kim, S.-H. Yang, H.-S. Kim, Y.-H. Son, and S.-K. Han, "Outdoor visible light communication for inter- vehicle communication using controller area network," in *2012 Fourth International Conference on Communications and Electronics (ICCE)*, 2012, pp. 31–34.

[37] D. K. Tettey, B. N. Ashfaq, M. Elamassie, and M. Uysal, "Experimental Investigation of MISO Vehicular Visible Light Communication Under Mobility Conditions," in *2023 IEEE Virtual Conference on Communications (VCC)*, 2023, pp. 276–281.

[38] S. Caputo, L. Mucchi, F. Cataliotti, M. Seminara, T. Nawaz, and J. Catani, "Measurement-based VLC channel characterization for I2V communications in a real urban scenario," *Vehicular Communications*, vol. 28, p. 100305, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214209620300760

[39] F. M. Al-Sallami, F. Benkhelifa, D. Ashour, Z. Ghassemlooy, O. C. Haas, Z. Ahmad, and S. Rajbhandari, "Average Channel Capacity Bounds of a Dynamic Vehicle-to-Vehicle Visible Light Communication System," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 2, pp. 1513–1523, 2024.

[40] U. D. of Transportation Federal Highway Administration, "Next generation simulation (NGSIM) vehicle trajectories and supporting data. [lankershim boulevard in los angeles, california]." 2016.

[41] A. Chen, H. Wu, Y. Wei, and H. Tsai, "Time variation in vehicle-to-vehicle visible light communication channels," in *2016 IEEE Vehicular Networking Conference (VNC)*, Dec 2016, pp. 1–8.

[42] S. Lee, J. K. Kwon, S.-Y. Jung, and Y.-H. Kwon, "Evaluation of visible light communication channel delay profiles for automotive applications," *EURASIP journal on Wireless Communications and Networking*, vol. 2012, no. 1, p. 370, 2012.

[43] A. Chaaban, Z. Rezki, and M.-S. Alouini, "On the capacity of intensity-modulation direct-detection Gaussian optical wireless communication channels: A tutorial," *IEEE Communications Surveys Tutorials*, vol. 24, no. 1, pp. 455–491, 2022.

[44] K. P. Peppas, A. N. Stassinakis, H. E. Nistazakis, and G. S. Tombras, "Capacity analysis of dual amplify-and-forward relayed free-space optical communication systems over turbulence channels with pointing errors," *Journal of Optical Communications and Networking*, vol. 5, no. 9, pp. 1032–1042, Sep 2013.

[45] United Nations, "United Nations Economic Commission for Europe vehicle regulations, Reg. 112-Rev.3," *UN*, no. 9789241565684, Jan. 2013. [Online]. Available: https://www.unece.org/fileadmin/DAM/trans/main/wp29/wp29regs/2013/R112r3e.pdf

[46] Thorlabs, *PM100D-Compact Power and Energy Meter Console, Digital 4 in LCD*, 2023. [Online]. Available: https://www.thorlabs.com/thorproduct.cfm?partnumber=PM100D

[47] Thorlabs, *S120C-Compact Photodiode Power Head with Silicon Detector*, 2016. [Online]. Available: https://www.thorlabs.com/thorproduct.cfm?partnumber=S120C

[48] A. Lapidoth, S. M. Moser, and M. A. Wigger, "On the capacity of free-space optical intensity channels," *IEEE Transactions on Information Theory*, vol. 55, no. 10, pp. 4449–4461, 2009.

[49] S. M. Moser, "Capacity results of an optical intensity channel with input-dependent gaussian noise," *IEEE Transactions on Information Theory*, vol. 58, no. 1, pp. 207–223, 2012.

[50] L. Mucchi, L. Ronga, X. Zhou, K. Huang, Y. Chen, and R. Wang, "A New Metric for Measuring the Security of an Environment: The Secrecy Pressure," *IEEE Transactions on Wireless Communications*, vol. 16, no. 5, pp. 3416–3430, 2017.

[51] F. M. Alsalami, O. C. Haas, A. Al-Kinani, C.-X. Wang, Z. Ahmad, and S. Rajbhandari, "Impact of Dynamic Traffic on Vehicle-to-Vehicle Visible Light Communication Systems," *IEEE Systems Journal*, vol. 16, no. 3, pp. 3512–3521, 2022.

[52] F. M. Alsalami, N. Aigoro, A. A. Mahmoud, Z. Ahmad, P. A. Haigh, O. C. Haas, and S. Rajbhandari, "Impact of Vehicle Headlights Radiation Pattern on Dynamic Vehicular VLC Channel," *Journal of Lightwave Technology*, vol. 39, no. 10, pp. 3162–3168, 2021.

[53] H. E. Nistazakis, E. A. Karagianni, A. D. Tsigopoulos, M. E. Fafalios, G. S. Tombras, and S. Member, "Average capacity of optical wireless communication systems over atmospheric turbulence channels," *in Journal of Lightwave Technology*, vol. 27, no. 8, pp. 974–979, 2009.

[54] A. Laourine, A. Stephenne, and S. Affes, "On the capacity of log-normal fading channels," *IEEE Transactions on Communications*, vol. 57, no. 6, pp. 1603–1607, 2009.

APPENDIX

A. Derivation of the upper bound on secrecy capacity of Theorem 1

By the definition of $D(\cdot||\cdot)$, Eq. (11) is expressed as:

$$
\begin{aligned}
&C_s(A,\varepsilon)\\
&\leq E_{\mathbb{P}_{X},\mathbb{P}_{Z|X}}\left[\int_{\mathcal{Y}} f_{Y|X,Z}(y|X,Z)\ln\frac{f_{Y|X,Z}(y|X,Z)}{g_{Y|Z}(y|Z)}dy\right]\\
&= \underbrace{E_{\mathbb{P}_X}\left[\int_{\mathcal{Y}}\int_{\mathcal{Z}} f_{YZ|X}(y,z|X)\ln f_{Y|X,Z}(y,z|X)dydz\right]}_{c_1}\\
&\quad - \underbrace{E_{\mathbb{P}_X}\left[\int_{\mathcal{Y}}\int_{\mathcal{Z}} f_{YZ|X}(y,z|X)\ln g_{Y|Z}(y|Z)dydz\right]}_{c_2}, \quad (17)
\end{aligned}
$$

where, c_1 represents the definition of $-\mathcal{H}(Y|X,Z)$. For degraded Gaussian wiretap channel, it is given by

$$
\begin{aligned}
&\mathcal{H}(Y|X,Z) = -\mathcal{H}(Y|X) + \mathcal{H}(Z|X,Y) - \mathcal{H}(Z|X)\\
&= -\frac{1}{2}\ln 2\pi e\sigma_B^2 + \frac{1}{2}\ln 2\pi e\Big(\sigma_E^2 - \frac{h_E^2}{h_B^2}\sigma_B^2\Big) - \frac{1}{2}\ln 2\pi e\sigma_E^2. \quad (18)
\end{aligned}
$$

Hence, c_1 is expressed as

$$c_1 = -\frac{1}{2}\ln 2\pi e\sigma_B^2\Big(1-\frac{h_E^2\sigma_B^2}{h_B^2\sigma_E^2}\Big). \tag{19}$$

To determine c_2 and establish an optimal upper bound, the conditional distribution of the channel output is selected to be [13], [15]:

$$g_{Y|Z}(y|z) = \frac{1}{\sqrt{2\pi\varsigma^2}}e^{\Big(-\frac{(y-\beta x)^2}{2\varsigma^2}\Big)}, \tag{20}$$

where β and ς are constants to be optimized. In addition, $f_{Z|XY}(z|x,y)$ is given by

$$f_{Z|XY}(z|x,y) = \frac{e^{-\frac{(y-h_Bx)^2}{2\sigma_B^2}}}{\sqrt{2\pi\sigma_B^2}}\frac{e^{-\frac{(z-\frac{h_E}{h_B}y)^2}{2\left(\sigma_E^2-\frac{h_E^2}{h_B^2}\sigma_B^2\right)}}}{\sqrt{2\pi(\sigma_E^2-\frac{h_E^2}{h_B^2}\sigma_B^2)}}. \tag{21}$$

As a result, c_2 is expressed as

$$\begin{aligned}
c_2 &= E_{\mathbb{P}_X}\Bigg[\int_{\mathcal{Y}}\int_{\mathcal{Z}}\frac{e^{-\frac{(y-h_Bx)^2}{2\sigma_B^2}}}{\sqrt{2\pi\sigma_B^2}}\frac{e^{-\frac{(z-\frac{h_E}{h_B}y)^2}{2\left(\sigma_E^2-\frac{h_E^2}{h_B^2}\sigma_B^2\right)}}}{\sqrt{2\pi(\sigma_E^2-\frac{h_E^2}{h_B^2}\sigma_B^2)}}\\
&\quad\times\left(\ln\Big(\frac{1}{\sqrt{2\pi\varsigma^2}}\Big)-\Big(\frac{(y-\beta z)^2}{2\varsigma^2}\Big)\right)dydz\Bigg]\\
&= -\frac{1}{2}\ln 2\pi\varsigma^2 - E_{\mathbb{P}_X}\Bigg[\int_{-\infty}^{\infty}\frac{e^{-\frac{(y-h_Bx)^2}{2\sigma_B^2}}}{2\varsigma^2\sqrt{2\pi\sigma_B^2}}\\
&\quad\times\Big(\beta^2\Big(\sigma_E^2-\frac{h_E^2}{h_B^2}\sigma_B^2\Big)+\Big(1-\frac{h_E}{h_B}\beta\Big)^2y^2\Big)dy\Bigg]\\
&= -\frac{1}{2}\ln 2\pi\varsigma^2 - E_{\mathbb{P}_X}\Bigg[\frac{1}{2\varsigma^2}\Big(\beta^2\Big(\sigma_E^2-\frac{h_E^2}{h_B^2}\sigma_B^2\Big)\\
&\quad+\Big(1-\frac{h_E}{h_B}\beta\Big)^2(h_Bx^2+\sigma_B^2)\Big)\Bigg].
\end{aligned} \tag{22}$$

Considering the concept of constraints relaxation in [43], $E_{\mathbb{P}_X}[x^2] = A\varepsilon$. In addition, $\beta = \frac{h_E}{h_B}(h_B^2A\varepsilon+\sigma_B^2)/(h_E^2A\varepsilon+\sigma_E^2)$ and $\varsigma^2 = (\sigma_E^2 - \frac{h_E^2}{h_B^2}\sigma_B^2)(h_B^2A\varepsilon+\sigma_B^2)/(h_E^2A\varepsilon+\sigma_E^2)$ are calculated as the critical values of c_2 (first derivative is zero). Therefore, c_2 is expressed as

$$c_2 = -\frac{1}{2}\ln 2\pi e\frac{(\sigma_E^2-\frac{h_E^2}{h_B^2}\sigma_B^2)(h_B^2A\varepsilon+\sigma_B^2)}{(h_E^2A\varepsilon+\sigma_E^2)}. \tag{23}$$

Hence, the upper secrecy bound as a combination on c_1 and c_2 in Eq. (19) and Eq. (23), is as provided in Eq. (12).

B. Derivation of the secrecy pressure

Considering Eqs. (13) and (14), the secrecy pressure in Eq. (15) is rewritten as

$$\begin{aligned}
p_{\text{sec}} = \int_0^{\infty}\frac{1}{2\delta_L L\sqrt{2\pi}}\ln\frac{(\sigma_E^2-\frac{Lh_E^2}{h_B^2}\sigma_B^2)(h_B^2A\varepsilon+\sigma_B^2)}{\sigma_B(Lh_E^2A\varepsilon+\sigma_E^2)\Big(1-\frac{Lh_E^2\sigma_B^2}{h_B^2\sigma_E^2}\Big)}\\
\exp\Big(-\frac{(\ln(L)-\mu_L)^2}{2\delta_L^2}\Big)dL,
\end{aligned} \tag{24}$$

When $\sigma_E = \sigma_B = \sigma_n$, the integration in Eq. (24) is given as

$$\begin{aligned}
p_{\text{sec}} &= \frac{1}{2\delta_L\sqrt{2\pi}}\ln\Big(\frac{h_B^2A\varepsilon}{\sigma_n^2}+1\Big)\\
&\quad-\int_0^{\infty}\frac{\ln\Big(\frac{Lh_E^2A\varepsilon}{\sigma_n^2}+1\Big)}{2\delta_L L\sqrt{2\pi}}\exp\Big(-\frac{(\ln(L)-\mu_L)^2}{2\delta_L^2}\Big)dL,
\end{aligned} \tag{25}$$

Assuming $x = \ln(Lh_E^2A\varepsilon/\sigma_n^2)$, $\omega_L = h_E^2A\varepsilon/\sigma_n^2$ and $\mu_d = \mu_L + \ln(\omega_L)$ [39], the second term in Eq. (25), is re-written as:

$$\begin{aligned}
p_{\text{sec}} &= \frac{1}{2\delta_L\sqrt{2\pi}}\ln\Big(\frac{h_B^2A\varepsilon}{\sigma_n^2}+1\Big)\\
&\quad-\int_0^{\infty}\frac{\ln(1+e^x)}{2\delta_L\sqrt{2\pi}}\exp\Big(-\frac{(x-\mu_d)^2}{2\delta_L^2}\Big)dz
\end{aligned} \tag{26}$$

Using these definitions $\ln(1+e^x) = \sum_{k=1}^{+\infty}(-1)^{k+1}x^k/k$ and $\text{erfcx}(x) = \exp(x^2)\text{erfc}(x)$, where $\text{erfcx}(x)$ is the scaled complementary error function [53], [54], Eq. (26) is solved as given in Eq. (16). However, the first term in Eq. (16) is infinite series expression and the convergence of this term is determined by rewriting it as

$$\begin{aligned}
&\sum_{k=1}^{+\infty}\frac{(-1)^{k+1}}{k}\left[\text{erfcx}\Big(\frac{\delta_Lk}{\sqrt{2}}+\frac{\mu_d}{\sqrt{2}\delta_L}\Big)+\text{erfcx}\Big(\frac{\delta_Lk}{\sqrt{2}}-\frac{\mu_d}{\sqrt{2}\delta_L}\Big)\right]\\
&=\underbrace{\sum_{k=1}^{+K}\frac{(-1)^{k+1}}{k}\left[\text{erfcx}\Big(\frac{\delta_Lk}{\sqrt{2}}+\frac{\mu_d}{\sqrt{2}\delta_L}\Big)+\text{erfcx}\Big(\frac{\delta_Lk}{\sqrt{2}}-\frac{\mu_d}{\sqrt{2}\delta_L}\Big)\right]}_{A}\\
&+\underbrace{\sum_{k=K+1}^{+\infty}\frac{(-1)^{k+1}}{k}\left[\text{erfcx}\Big(\frac{\delta_Lk}{\sqrt{2}}+\frac{\mu_d}{\sqrt{2}_{\delta_L}}\Big)+\text{erfcx}\Big(\frac{\delta_Lk}{\sqrt{2}}-\frac{\mu_d}{\sqrt{2}\delta_L}\Big)\right]}_{B}.
\end{aligned} \tag{27}$$

In B, the expression $\text{erfcx}(x)$ diverges to $\text{erfcx}(x) \simeq \frac{1}{x\sqrt{\pi}}$, when K has sufficiently large value. Hence, B is expressed as [54]:

$$B = \frac{2}{\delta_L\sqrt{2\pi}}\sum_{k=K+1}^{+\infty}\frac{(-1)^{k+1}}{k(k+\frac{\mu_d}{\delta_L^2})}+\sum_{k=K+1}^{+\infty}\frac{(-1)^{k+1}}{k(k-\frac{\mu_d}{\delta_L^2})}. \tag{28}$$

For positive μ_d values, B diverges to [54]:

$$B = \frac{2\delta_L}{\mu_d\sqrt{2\pi}}(-1)^K\left[\beta\Big(K+1-\frac{\mu_d}{\delta_L^2}\Big)-\beta\Big(K+1+\frac{\mu_d}{\delta_L^2}\Big)\right], \tag{29}$$

where $\beta(\cdot)$ is given by [54]:

$$\beta(x) = \frac{1}{2}\left(\frac{d}{dx}\ln\Gamma\Big(\frac{x+1}{2}-\frac{d}{dx}\Big)-\ln\Gamma\Big(\frac{x}{2}\Big)\right), \tag{30}$$

where $\Gamma(\cdot)$ is the Gamma function.