Enhancing Security in 6G Vehicular Networks: Leveraging VLC and MMW Integration and Cooperative Relaying Technique

Selma Yahia, Valeria Loscri, Prakriti Saxena

2023 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech) | 979-8-3503-0460-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/DASC/PICOM/CBDCOM/CY59711.2023.10361417

Enhancing Security in 6G Vehicular Networks: Leveraging VLC and MMW Integration and Cooperative Relaying Technique

Selma Yahia[1], Valeria Loscri[1], and Prakriti Saxena[1]
[1]Inria Lille- Nord Europe Lille, 59000 France
E-mail: selma.yahia@inria.fr

***Abstract*—Future sixth-generation (6G) networks aim to support high-performance vehicular applications with ultra-high throughput, massive connectivity, low latency, and reliable quality of service. Emerging technologies like visible light communication (VLC) and millimeter wave (MMW) transmission show promise in meeting these demands. However, security remains a critical open challenge for their individual deployment in vehicular domains. To address this, we propose an innovative algorithm that integrates VLC and MMW to enhance security. Our algorithm selects the most suitable technology for communication based on secrecy capacity levels in various road scenarios. Additionally, we introduce a fail-safe solution using a decode and forward relaying scheme for enhanced security if direct VLC/MMW transmission fails to meet security requirements. Our results demonstrate the effectiveness of the algorithm in ensuring robust security and connectivity among vehicles, advancing 6G wireless networks.**

***Index Terms*—Vehicular network security, visible light communication, millimeter-wave, cooperative relays, secrecy capacity**

I. Introduction

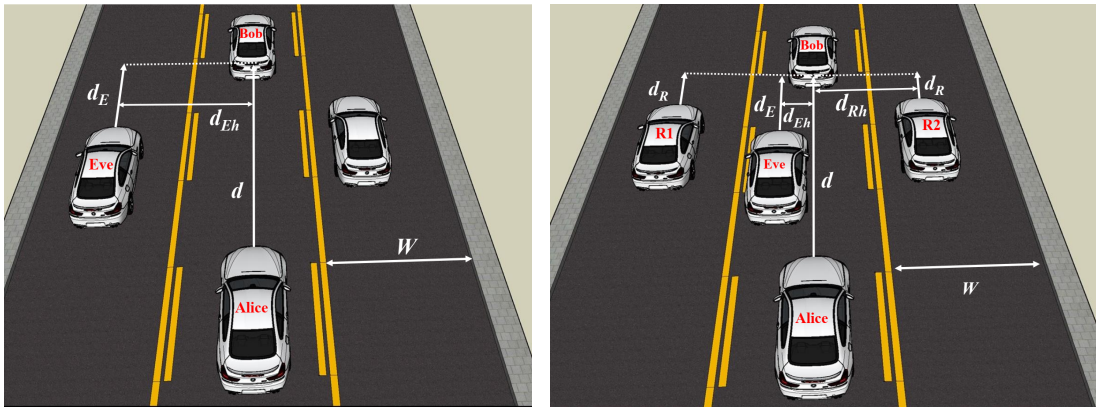
Connected vehicle technology stands as a pivotal enabler in shaping the future landscape of smart cities and intelligent transportation systems. This innovation fosters seamless information exchange among vehicles, ushering in substantial advancements in road safety, efficient time utilization, fuel conservation, and an elevated driving experience [1]. In the realm of data transmission that facilitates the authorization of vehicle-to-vehicle (V2V) connectivity, radio frequency (RF) technologies emerge prominently. At present, dedicated short-range communication (DSRC) and cellular vehicle-to-everything (C-V2X) take center stage as the utilized RF technologies [2], [3]. On the horizon, the upcoming sixth-generation (6G) technology will leverage frequencies beyond the millimeter wave (MMW) range, including optical bands such as visible light [4], [5]. Both MMW communication and Visible Light Communication (VLC) are strong contenders for V2V communication.

Due to the broadcast nature of wireless channels in MMW and VLC communication, privacy and security concerns have become more significant [6]. The main objective of secure communications is to ensure that the intended recipient can access the source information successfully, while preventing eavesdroppers (wire-tappers) from understanding the transmitted data. Security measures can be deployed at higher layers of the network architecture, utilizing methods like access control, password protection, and end-to-end encryption. These strategies are considered to be effective in maintaining security, provided that the storage capacity and computational capabilities of potential eavesdroppers remain below certain limits [7]. Additionally, physical layer security (PLS) has recently emerged as a promising area of research to complement conventional encryption techniques and provide a first line of defense against eavesdropping attacks [8]. It involves utilizing information-theoretic principles to leverage the inherent physical properties of the wireless channel to transmit messages securely. In essence, PLS aims to exploit the characteristics of the wireless medium to enhance the confidentiality and integrity of the transmitted data.

Lately, there has been a surge of research dedicated to exploring the potential of PLS in both MMW and VLC systems [9]–[12]. For instance, in [9], two innovative PLS techniques were introduced for MMW vehicular communication systems. These methods employ multiple antennas for transmitting information symbols and noise-like signals, resulting in significantly higher secrecy rates compared to conventional approaches. Similarly, the authors in [10] proposed a low-complexity PLS scheme for MMV communication within Vehicle-to-Everything (V2X) applications. This scheme harnesses PLS techniques to enhance communication reliability while reducing computational complexity. In [11], the authors experimentally, leveraged the received signal strengths (RSSs) of multi-nodes to perform continuous authentication among the nodes. Moreover, a handful of security-oriented investigations have been carried out in the realm of vehicular VLC. Notably, an endeavor to address PLS within the V2V VLC context is outlined in [12]. The study proposes an enhanced V2V VLC model for outdoor vehicular communication that improves the received power distribution and security in a V2V VLC system.

However, it's worth noting that none of the aforementioned studies [9]–[12] have explored the synergistic potential of integrating both MMW and VLC technologies to enhance security within vehicular communication systems. Also, these studies don't consider realistic channel modeling for vehicular MMW and VLC systems. It has shown in [13]–[16] that vehicular MMW and VLC channels are substantially different from traditional RF and indoor VLC channels, respectively.

Therefore, in this paper, we introduce a novel scheme designed to fortify V2V communication security through the



(a) (b)

Fig. 1: Considered V2V scenarios (a) Scenario 1 (b) Scenario 2.

integration of MMW and VLC technologies together with the cooperative relaying technology. The later acts as a fail-safe solution if the hybrid VLC/MMW transmission fails to meet security requirements. The core concept involves dynamically switching between three distinct solutions to guarantee communication security among vehicles on the road. Furthermore, to ensure accurate findings, we rely on the recent realistic MMW and VLC channel models obtained through the employment of cutting-edge ray tracing approaches using Remcom's Wireless Insite and Zemax's OpticStudio tools for modeling MMW and VLC channels, respectively [17]. Subsequently, we conduct a comprehensive analysis to evaluate the secrecy capacity performance of the proposed scheme across a spectrum of scenarios, shedding light on its potential benefits for enhancing security in V2V communication systems.

The paper is structured as follows. In Section II, we present the V2V system, scenarios, and MMW and VLC channel models. Section III introduces the proposed security scheme and the performance analysis. In Section VI, the numerical results are presented, and a comparative analysis of the proposed algorithm with each individual technology is conducted. Finally, Section V concludes the paper and gives further insights on future research directions.

II. System and Threat Models

A. System and Threat Scenarios

As shown in Fig. 1, we consider a V2V communication system in a three-lane road with a lane width of W. The transmitting vehicle, denoted as "Alice", establishes a wireless link to share data with the receiving vehicle "Bob". Alice and Bob travel at the middle lane and are separated with a distance of d. Additionally, we encounter a potential intrusion from a third vehicle, labeled 'Eve', which attempts to illicitly intercept and decipher the data being transmitted. Eve travels at a longitudinal distance of d_E and a lateral distance of d_{Eh} with respect to Bob vehicle. Moreover, we assume existing of two neighbor vehicles (**R1** and **R2**). They are moving at the right and left lanes with a lateral shift of d_{Rh} and a longitudinal distance of d_R with respect to Bob, and can act as intermediate relays to improve the security of the network. We further consider different threat scenarios described as the following:

- **Scenario 1:** Alice and Bob are traveling in the middle lane, while Eve occupies an adjacent lane, potentially offset by a lateral distance of $d_{Eh} = W$.
- **Scenario 2:** This scenario comprises two sub-cases to investigate the effect of partial and full line of sight (LoS) blockage.
  2a. Eve shares the same lane as Alice and Bob, with a lateral offset of $d_{Eh} \approx W/2$, resulting in a partial obstruction of the LoS between the latter two vehicles. We also assume the presence of two additional vehicles (R1 and R2) located in the right and left lanes with a lateral shift of $d_{Rh} = W$ and a separation distance of d_R from Bob, which act as intermediate relays.
  2b. Alice, Bob, and Eve are positioned in the same lane with perfect alignment, causing Eve to create a complete blockage in the LoS transmission between Alice and Bob. Also, intermediate vehicles labeled as R1 and R2 are placed in the adjacent lanes (right and left) with a lateral shift of $d_{Rh} = W$ and a separation distance of d_R.

B. Channel Modeling Methodology

In this work, we considered the most recent realistic channel models for VLC and MMW, which are based on the ray tracing capabilities of OpticStudio and Remcom's Wireless Insite software, respectively. Both tools, validated in [18], [19], enable the use of measured radiation patterns and wavelength-dependent material properties. This allows for an accurate characterization of signal propagation and interaction with the environment. The detailed steps of using OpticStudio and Wireless Insite to model VLC and MMV channels have been described in [17].

For a total number of paths N_w, the channel impulse responses (CIR) for the MMV link can be given as follows [17]:

$$h_{\mathrm{MMW}}(t) = \sum_{i=1}^{N_w} A_i \exp\left(j\psi_i\right) \delta\left(t - \tau_i\right), \tag{1}$$

here τ_i represents the delay of the ith path and δ signifies the Dirac delta function. The amplitude A_i and phase ψ_i of the channel coefficients related to the ith path are defined by

$$\begin{aligned} A_i &= E_{\theta,i} g_\theta(\theta_i, \phi_i) + E_{\phi,i} g_\theta(\theta_i, \phi_i), \\ \psi_i &= \tan^{-1}\left(\frac{\mathrm{Im}(A_i)}{\mathrm{Re}(A_i)}\right), \end{aligned} \tag{2}$$

where $E_{\theta,i}$ and $E_{\phi,i}$ are the so-called theta and phi components of the electric field of the ith path at the receiver point, whereas θ_i and ϕ_i are parameters associated with the direction of arrival ray.

Likewise, let N_v represent the number of rays emitted from the car headlamp and captured by the receiver. The CIR of the VLC link can be expressed as follows:

$$h_{\mathrm{VLC}}(t) = \sum_{k=1}^{N_v} P_k \delta(t - \tau_k), \tag{3}$$

where, P_k and τ_k are the power and the propagation delay of the kth ray for $k = 1, 2, .., N_v$.

III. Performance Metrics and Proposed Security Scheme

A. Performance Metrics

In this section, we analyze the security performance of the proposed scenarios. A key metric for quantifying security is secrecy capacity (SC), which indicates the system's ability to transmit information securely while minimizing the risk of eavesdropping. Specifically, SC represents the maximum rate at which information can be reliably recovered by the intended receiver while remaining inaccessible to the eavesdropper [20]. The concept of secrecy capacity was introduced by Wyner's wiretap channel model [21]. Wyner defined SC as the difference between the capacities of the main channel and the wiretap channel. Thus, the data is secure when the main channel capacity exceeds the wiretap channel capacity. Otherwise, the eavesdropper may partially or fully intercept the legitimate data. Mathematically, consider $j \in \{V, M\}$ denoting for the VLC link (i.e., $j = V$) and the MMV link (i.e., $j = M$). We then define C_j the secrecy capacity, which can be expressed as:

$$C_j = \max\{C_{B_j} - C_{E_j}, 0\}, \tag{4}$$

where C_{B_j} and C_{E_j} are the channel capacities for the legitimate receiver and eavesdropper, respectively. For a VLC link C_{B_V} and C_{E_V} are given as follows

$$\begin{aligned} C_{B_V} &= B\log_2\left(1 + \frac{P_t(\eta\Re H_{B_V})^2}{\sigma_n^2 + \sum_{l=1}^{N}(\eta\Re H_{\mathrm{V},l})^2 P_t}\right), \\ C_{E_V} &= B\log_2\left(1 + \frac{P_t(\eta\Re H_{E_V})^2}{\sigma_n^2 + \sum_{l=1}^{N}(\eta\Re H_{\mathrm{V},l})^2 P_t}\right), \end{aligned} \tag{5}$$

where B is the bandwidth, η is electrical-to-optical conversion ratio, P_t is the transmitter power, and $\Re$ is the receiver responsivity. Also, H_{B_V} and H_{E_V} are the channel gain of the main channel and the eavesdropping channel, respectively. $H_{\mathrm{V},l}$ is the channel gain for interfering links and σ_n^2 is the noise variance, $\sigma_n^2 = BN_0$, where N_0 is the spectral power density. Similarly, in the context of MMW communication, we can derive expressions for the capacities C_{B_M} and C_{E_M} as follows:

$$\begin{aligned} C_{B_M} &= B\log_2\left(1 + \frac{|H_{\mathrm{B_M}}|^2 P_t}{\sigma_n^2 + \sum_{l=1}^{N}|H_{\mathrm{M},l}|^2 P_t}\right), \\ C_{E_M} &= B\log_2\left(1 + \frac{|H_{\mathrm{E_M}}|^2 P_t}{\sigma_n^2 + \sum_{l=1}^{N}|H_{\mathrm{M},l}|^2 P_t}\right), \end{aligned} \tag{6}$$

where $H_{\mathrm{B_M}}$ and $H_{\mathrm{E_M}}$ are the magnitude of channel frequency response for the main and eavesdropper MMW channels, respectively. Furthermore, $H_{\mathrm{M},l}$ signifies the magnitude of the channel frequency response for the interfering links.

B. Proposed Security Scheme

In this section, we present the fundamental aspects of our innovative algorithm designed to ensure robust security measures along roadways. Our approach revolves around the development of a dynamic switching algorithm that alternates between two distinct technologies, VLC and MMV, to establish a secure communication channel between the sender (Alice) and the receiver (Bob). Additionally, we introduce a third-tier solution: intermediate relays. These relays serve as a backup in the event that both primary technologies fail to meet safety requirements, ensuring the continuous and robust security of our communication.

To begin, we address two primary conditions: daytime and nighttime. In the daytime condition, we assume that the default technology employed by vehicles for communication is MMV. The algorithm starts by assessing the availability of the communication spectrum, determining whether it is congested or not. In the event of spectrum congestion, the vehicle promptly switches to the alternate technology, VLC. Otherwise, it maintains its operation with MMV.

Furthermore, during these transitions, our algorithm takes potential eavesdropping threats into account. If an eavesdropper uses a different technology than MMV, the vehicle sticks with MMV as a precaution. However, if the eavesdropper operates on the same frequency band, the algorithm calculates the secrecy capacity, C_M, as defined by Eq. 4. If the calculated C_M exceeds a predefined threshold value C_M^{th}, the vehicle continues using the MMV link, as communication secrecy is sufficiently guaranteed. Conversely, if $C_M < C_M^{\mathrm{th}}$, the algorithm seamlessly initiates a switch to the VLC technology. Under this circumstance, the vehicle verifies the capacity acquired through the alternative link, C_V. If this value falls below a predefined threshold, denoted as C_V^{th}, the vehicle utilizes intermediate relays to ensure continuous and secure communication.

In the night condition, our algorithm functions inversely, with VLC being the default technology. The core principles remain intact, but the emphasis shifts to accommodate the specific characteristics of nighttime conditions. During the night, the default communication technology for vehicles is VLC. Similar to the daytime condition, the algorithm commences by

Algorithm 1 Technology Switching Based on Security and Spectrum Conditions

Initialize:
Define threshold values: C_M^{th} and C_V^{th}.
procedure SWITCHING ALGORITHM
  if Day Condition **then**
    Set default technology to MMW.
    if MMW band is not crowded **then**
      if Eve doesn't use MMV technology **then**
        Use MMW technology.
      else
        Calculate C_M using Eq (4)
        if $C_M > C_M^{th}$ **then**
          Use MMW technology.
        else
          Switch to VLC technology.
          if $C_V < C_V^{th}$ **then**
            Use intermediate relays
          end if
        end if
      end if
    else if VLC band is not crowded **then**
      Calculate C_V using Eq (4)
      if $C_V > C_V^{th}$ **then**
        Switch to VLC technology.
      else
        Use intermediate relays
      end if
    end if
  else
    Set default technology to VLC.
    if VLC band is not crowded **then**
      if Eve doesn't use VLC technology **then**
        Use VLC technology.
      else
        Calculate C_V using Eq (4)
        if $C_V > C_V^{th}$ **then**
          Use VLC technology
        else
          Switch to MMW technology
          if $C_M < C_M^{th}$ **then**
            Use intermediate relays
          end if
        end if
      end if
    else if MMV band is not crowded **then**
      Calculate C_M using Eq (4).
      if $C_M > C_M^{th}$ **then**
        Switch to MMW technology.
      else
        Use intermediate relays
      end if
    end if
  end if
end procedure

assessing the spectrum availability. If the spectrum is identified as congested, implying potential interference, the vehicle promptly transitions to the alternative MMV technology to maintain effective communication. However, if the spectrum isn't congested and is deemed secure for VLC transmission, the vehicle continues with VLC-based communication. As before, the algorithm remains vigilant against potential eavesdropping threats. If an eavesdropper operates using MMV or any technology other than VLC, the vehicle prudently sticks with the default VLC technology. However, in instances where the eavesdropper operates within the VLC frequency band, the algorithm computes the secrecy capacity following the framework outlined in Eq. 4. The calculated secrecy capacity is then compared against the predefined threshold value (C_V^{th}), mirroring the decision-making process in the daytime condition. In other words, if the calculated secrecy capacity exceeds this threshold, the vehicle persists with VLC technology. On the other hand, if the calculated secrecy capacity falls short of the threshold, the algorithm triggers a seamless transition to the more secure MMV technology. In this step, the vehicle verifies the capacity obtained via the alternative link, C_M. If this value falls below a predefined threshold (C_M^{th}), the vehicle employs intermediate relays to ensure uninterrupted secure communication.

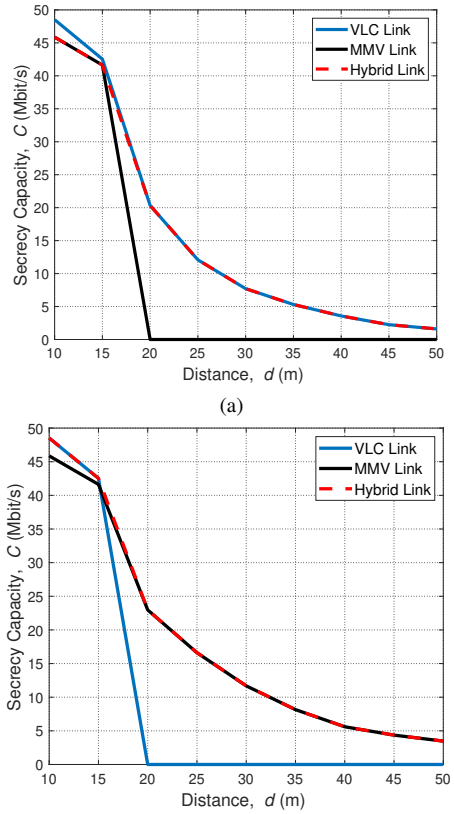


Fig. 2: Secrecy capacity of Scenario 1 at (a) Day Conditions (b) Night Conditions.

IV. Performance Results and Discussions

In this section, we present the simulation results of the introduced algorithm for vehicular scenarios under consideration. For simulation analysis, we consider W = 3.75 m, η = 0.5 W/A, $\Re$ = 0.5 A/W, P_t = 40 W, N_0 = 10^{-21}, and B = 5 MHz. Also, C_M^{th} = 10 Mbit/s, and C_M^{th} = 10 Mbit/s. Different lateral shifts, i.e., d_{Eh} = 0 m, 2 m, 3.75 m are considered.

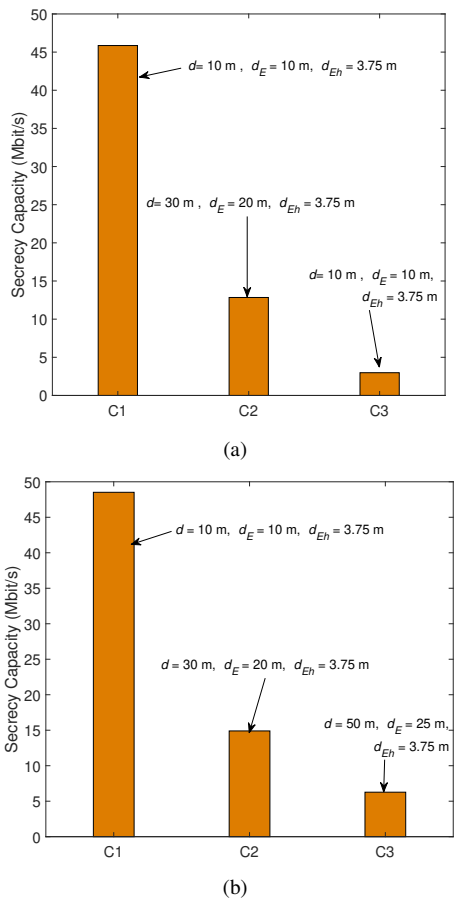


Fig. 3: Secrecy capacity of Scenario 1 at different configurations (a) Day Conditions (b) Night Conditions.

Fig. 2 illustrates the secrecy capacity versus the inter-vehicle distance across three distinct links: VLC link, MMV link, and the Hybrid link. These measurements are provided for both daytime and nighttime conditions, with the consideration that the eavesdropper utilizes the default technology. Notably, the hybrid system emerges as the most advantageous option in terms of achieving security along the roadway. Specifically, consider Scenario 1 and during the daylight (see Fig. 3(a)), the vehicle utilizes the default communication technology (MMV link) for a distance range from 10 to 15 m. Beyond a separation of d = 20 m, the secrecy capacity of the MMV links falls below the predetermined threshold (C_M^{th}). Consequently, the vehicle swiftly transitions to VLC communication through the hybrid system, guaranteeing a more robust and secure data exchange. For instance, if we take d = 10 m, the secrecy capacity C_M amounts to 46 Mbit/s, surpassing the necessary threshold, thereby allowing the vehicle to continue using the default MMV technology. As the distance extends to d = 25 m, C_M diminishes to 0, prompting an automatic shift to VLC technology (C_V = 12 Mbit/s). Similarly, during nighttime conditions, the communication initiation employs the default VLC technology. Once the distance reaches 15 m, C_V falls below the prescribed threshold C_V^{th}, compelling a transition to the alternative MMV technology. For example, consider the case of d = 15 meters: C_V is recorded at 43 Mbit/s, surpassing the requisite threshold. Beyond this point, the attained C_V dwindles to 0, failing to meet the established threshold. Consequently, the vehicle switches to the alternative MMV solution, whereby C_M amounts to 24 Mbit/s for d = 20 meters.

Fig. 3 illustrates the achieved secrecy capacity through the hybrid system during both daytime (Fig. 3(a)) and nighttime (Fig. 3(b)). In our analysis, we consider the presence of Eve, who attempts to eavesdrop on the communication between Alice and Bob while also interfering with Bob's reception. To investigate the impact of different spatial configurations, we examine three distinct cases: **C1**, **C2**, and **C3** as follows: **C1**: In this case, we assume d = 10 m, d_E = 10 m, and d_{Eh} = 3.75 m. **C2**: Here, we consider d = 30 m, d_E = 20 m, and d_{Eh} = 3.75 m. **C3**: We consider d = 50 m, d_E = 25 m, and d_{Eh} = 3.75 m. Our analysis reveals the significant impact of the spatial positions of the vehicles on the achieved secrecy capacity. Specifically, the relative distances between the sender (Alice) and receiver (Bob) and the lateral displacement of Eve play a pivotal role in determining the secrecy capacity. Notably, the close proximity of Alice and Bob, coupled with an increased lateral offset of Eve (i.e., **C1**), leads to a notable enhancement in secrecy capacity. This phenomenon can be attributed to the reduced visibility of reception from Eve's vantage point compared to Bob's, which introduces supplementary barriers that impede the successful interception and decoding of the transmitted information. In contrast, cases like **C2** and **C3** where the inter-vehicle distance between Alice and Bob is increased reveal an opposing trend in secrecy capacity. In these cases, the legitimate signal experiences more degradation over longer distances due to increased path loss and attenuation effects. On the flip side, Eve's reception enhances due to the improved field of vision established between Alice and Eve, creating a clearer transmission path and potentially facilitating Eve's interception efforts, which may reduce secrecy capacity. For example, the attained secrecy capacity measures 45.5 Mbit/s in the case of **C1**. This value diminishes to 14.9 Mbit/s and 6.2 Mbit/s for **C2** and **C3**, respectively.

In Figure 4, we delve into the effectiveness of the third proposed solution presented by our algorithm. In essence, we investigate the efficiency of employing intermediate relays to ensure secure communication in situations where both VLC and MMV technologies fall short of establishing a reliable connection between vehicles. We consider the integration of either a single relay (R1) or dual relays (R1 and R2) in two distinct scenarios: 2a (Partial LoS Blockage) and 2b (Full LoS Blockage). This analysis spans across three specific configurations: **Ca**: We assume distances as follows: d = 45 m, d_E = 40 m, d_R = 25 m, and d_{Rh} = 3.75 m. **Cb**: Our assumptions are d = 50 m, d_E = 45 m, d_R = 25 m, and d_{Rh} = 3.75 m. **Cc**: We consider d = 55 m, d_E = 50 m, d_R = 25 m, and d_{Rh} = 3.75 m. The analysis reveals a notable enhancement in secrecy capacity for both Partial LoS Blockage and Full LoS Blockage scenarios through the utilization of intermediate vehicles as relays. This finding highlights the effectiveness

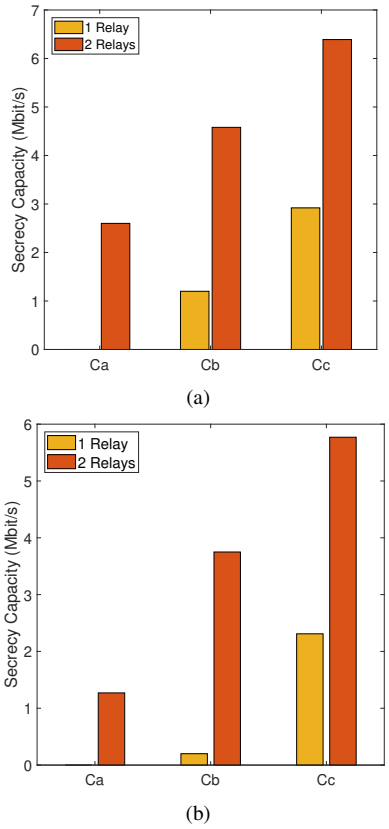


Fig. 4: Secrecy capacity of Scenario 2 (a) Partial LoS Blockage (Scenario 2.a) (b) Full LoS Blockage (Scenario 2.b), considering different configurations as follows: **Ca**: d = 45 m, d_E = 40 m, d_R = 25 m, and d_{Rh} = 3.75 m. **Cb**: d = 50 m, d_E = 45 m, d_R = 25 m, and d_{Rh} = 3.75 m. **Cc**: We consider d = 55 m, d_E = 50 m, d_R = 25 m, and d_{Rh} = 3.75 m.

of using relay vehicles to enhance communication security, even under LOS blockage conditions. Furthermore, the results clearly indicate that employing two intermediate relays can significantly boost the secrecy capacity when compared to using just one relay. For example, consider the configuration of **Cb** in the context of partial LoS blockage. Here, the secrecy capacity is recorded at 1.2 Mbit/s with the involvement of 1 relay. This capacity surges to 4.8 Mbit/s when 2 relays are deployed. Similarly, in the context of **Cc** and a full blockage scenario, the achieved secrecy capacities register as 2.2 Mbit/s and 5.8 Mbit/s for 1 relay and 2 relays, respectively.

V. Conclusion

This paper introduced an innovative and secure algorithm that leverages hybrid technology to enhance the security of communication among vehicles on the road. Our proposed algorithm dynamically switches between three robust solutions: VLC technology, MMW technology, and Cooperative Relaying technology, ensuring a resilient and secure communication environment. We conducted an efficient channel modeling approach based on ray tracing feature of OpticStudio and Remcom's Wireless Insite softwares. A comprehensive analysis to evaluate the efficiency of the proposed algorithm across a spectrum of scenarios and settings is conducted. The results of our study demonstrate the remarkable efficiency of our proposed solution in ensuring secure communication between vehicles on the road. Furthermore, our findings reveal that employing intermediate vehicles as relays can be a promising strategy to bolster security in V2V communication networks.

References

[1] M. Noor-A-Rahim *et al.*, "6G for vehicle-to-everything (V2X) communications: Enabling technologies, challenges, and opportunities," *Proc. IEEE*, vol. 110, no. 6, pp. 712–734, 2022.

[2] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the united states," *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011.

[3] S. Chen *et al.*, *Cellular Vehicle-to-Everything (C-V2X)*. Springer Nature, 2023.

[4] M. Alsabah *et al.*, "6G wireless communications networks: A comprehensive survey," *IEEE Access*, vol. 9, pp. 148 191–148 243, 2021.

[5] Z. Zhang *et al.*, "6G wireless networks: Vision, requirements, architecture, and key technologies," *IEEE Veh. Technol. Mag.*, vol. 14, no. 3, pp. 28–41, 2019.

[6] A. Mukherjee *et al.*, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Survey Tuts.*, vol. 16, no. 3, pp. 1550–1573, 2014.

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

[8] J. M. Hamamreh *et al.*, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surv. Tutor.*, vol. 21, no. 2, pp. 1773–1828, 2018.

[9] M. E. Eltayeb *et al.*, "Enhancing secrecy with multiantenna transmission in millimeter wave vehicular communication systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 9, pp. 8139–8151, 2017.

[10] M. He *et al.*, "Low-complexity phased-array physical layer security in millimeter-wave communication for cybertwin-driven V2X applications," *IEEE Trans. Veh. Technol.*, vol. 71, no. 5, pp. 4573–4583, 2021.

[11] H. B. Eldeeb *et al.*, "Experimental evaluation of a lightweight RSS-based PLA scheme in multi-node multi-cell mesh networks," in *2023 IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*, 2023.

[12] R. Shaaban and S. Faruque, "Cyber security vulnerabilities for outdoor vehicular visible light communication in secure platoon network: Review, power distribution, and signal to noise ratio analysis," *Phys. Commun.*, vol. 40, p. 101094, 2020.

[13] M. T. Dabiri and M. Hasna, "3D uplink channel modeling of UAV-based mmWave fronthaul links for future small cell networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 2, pp. 1400–1413, 2023.

[14] X. Yang *et al.*, "Impact of UAV 3D wobbles on the non-stationary air-to-ground channels at sub-6 GHz bands," in *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, 2022, pp. 4473–4478.

[15] H. B. Eldeeb *et al.*, "Energy and spectral efficiency analysis for RIS-aided V2V-visible light communication," *IEEE Commun. Lett.*, vol. 27, no. 9, pp. 2373–2377, 2023.

[16] S. Yahia *et al.*, "Performance study and analysis of MIMO visible light communication-based V2V systems," *Opt. Quantum Electron.*, vol. 54, no. 9, p. 575, 2022.

[17] F. Aghaei *et al.*, "A comparative evaluation of propagation characteristics of vehicular VLC and MMW channels," *IEEE Trans. Veh. Technol.*, 2023.

[18] H. B. Eldeeb, S. M. Mana, V. Jungnickel, P. Hellwig, J. Hilt, and M. Uysal, "Distributed mimo for Li-Fi: Channel measurements, ray tracing and throughput analysis," *IEEE Photon. Technol. Lett.*, vol. 33, no. 16, pp. 916–919, 2021.

[19] G. Noh, J. Kim, S. Choi, N. Lee, H. Chung, and I. Kim, "Feasibility validation of a 5G-enabled mmwave vehicular communication system on a highway," *IEEE Access*, vol. 9, pp. 36 535–36 546, 2021.

[20] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, 2011.

[21] A. D. Wyner, "The wire-tap channel," *Bell Syst. tech. j.*, vol. 54, no. 8, pp. 1355–1387, 1975.