Visible Light Communication Assisted Secure and Efficient Architecture For Autonomous Platoon

A thesis submitted in fulfilment of the requirements for the degree of

PhD in Computer Science and Engineering

Koç University, February 2017

Seyhan Uçar

Graduate School of Sciences and Engineering

Koç University

Istanbul, Turkey

Koç University

Graduate School of Sciences and Engineering

This is to certify that I have examined this copy of a doctoral dissertation by

Seyhan Uçar

and have found it is complete and satisfactory in all respects, and that any and all revisions required by the final examining committee have been made.

Committee Members:

Assoc. Prof. Dr. Sinem Çöleri Ergen (Advisor)

Assoc. Prof. Dr. Öznur Özkasap (Advisor)

Prof. Dr. Attila Gürsoy

Prof. Dr. Özgür Barış Akan

Asst. Prof. Dr. Didem Unat

Prof. Dr. Murat Uysal

Assoc. Prof. Dr. Berk Canberk

24.02.2017

aileme

Acknowledgements

I would like to express my sincere gratitude and profound respect to my advisers Assoc. Prof. Dr. Sinem Çöleri Ergen and Assoc. Prof. Dr. Öznur Özkasap for their reliable guidance, inspiration, patience and valuable support. I am also grateful to members of my thesis committee Prof. Özgür Barış Akan, Prof. Dr. Attila Gürsoy, Asst. Prof. Dr. Didem Unat, Prof. Dr. Murat Uysal and Assoc. Prof. Dr. Berk Canberk for their valuable comments and serving on my defense committee.

Ph.D. is a long journey that I will never forget in my life. Listing people name seems to me harder than Ph.D. Instead, I will follow one of my favorite author's acknowledgment solution. There are lots of people in my mind and I always find making a list of people that I want to thank as a difficult task. In this part, I again try to write all the names that are in my memory and the list is longer than I imagine. As I think, names come to my mind and I delete all of them. Instead of doing a list of people;

I want to thank all of the people that touch my life either positive or negative. My family, my friends, my teacher, people that show me the way in very dark of my life, my students, my advisees, my advisers, people that love me, people that I hate, people that I dream about, people that I broke their dream, people that I touch their heart, people that touch my heart, people that I upset, people that make me upset. Without these people, I could not be me. Apart from these, I present my gratitude to the "Creator" who gave me the strength and intelligence that brings me to this level and make me write these lines.

I also acknowledge the support of Ford Otosan, Argela and Turk Telekom under Grant Number #11315-07

Abstract

Autonomous vehicles use a variety of sensors together with advanced software to drive without any human input. Autonomous vehicle platoon is an enhancement of autonomous behaviour where vehicles are organized into groups of close proximity through wireless communication with the goal of improving traffic throughput, transportation safety, fuel consumption and emissions. The chain of platoons that follow each other, on the other hand, refer to multiplatoon. Autonomous platoon and multiplatoon systems mostly adopt the current dominant vehicular radio frequency (RF) technology, IEEE 802.11p (DSRC), for communication among vehicles. However, DSRC suffers from problems of performance degradation due to congestion, the scarcity of RF and security. Visible Light Communication (VLC) is a recently proposed alternative communication technology with the potential of addressing problems by exploiting the directivity and impermeability of light. However, utilizing only VLC in vehicle platoon may degrade platoon stability since VLC is sensitive to environmental effects, i.e. fog, and might have short-term unreachability due to the increase in the inter-vehicle distance and/or loss of line-of-sight on a curvy road. In this thesis, hybrid usage of DSRC and VLC is investigated to achieve secure and efficient architecture for the vehicular platoons.

First, we experimentally analyze the characteristics of vehicular VLC in different scenarios including single and dual channel data transmission considering various light dimming level and bearing angle of values with the goal of determining the usage limitation of VLC in the vehicular environment. We demonstrate that state of the art Lambertian radiation pattern does not represent the automotive light emitting diode (LED) radiation pattern

accurately. Dual channel usage increases the angular limitation by up to 10° compared to the single channel VLC and dimming is a key parameter in VLC, which affects data dissemination and received power signal strength.

Second, we propose an DSRC and VLC based hybrid security protocol for platoon communication, namely SP-VLC, with the goal of ensuring platoon stability and securing platoon maneuvers under data packet forgery, data packet replay, fake maneuver packet and jamming attacks. We define platoon maneuver attack based on the identification of various scenarios where a fake maneuver request packet or a fake maneuver response packet is transmitted by a malicious actor on the road side. SP-VLC includes mechanisms for secret key establishment and periodic update via VLC to ensure the participation of only the target vehicle in communication; authentication using of message authentication code to ensure the packet integrity; data transmission over both DSRC and VLC incorporating the encryption and decryption of the packets using the secret key generated between consecutive platoon members to exploit the complementary propagation characteristics of data transmission; jamming detection and reaction to switch to VLC only communication based on packet reception characteristics; and secure platoon maneuvering based on the joint usage of DSRC and VLC. We demonstrate the functionality of the proposed SP-VLC protocol under all possible security attacks by both providing a detailed analysis and performing extensive simulations. We develop a simulation platform combining realistic vehicle mobility model, realistic VLC and DSRC channel models and vehicle platoon management and demonstrate that SP-VLC protocol generates less than 0.1% difference in the speed and distance variation of platoon members during attacks in comparison to 25% and 10% in that of previously proposed DSRC and DSRC-VLC hybrid protocols, respectively.

Third, we propose a DSRC and VLC based safety message dissemination protocol for multiplatoon to satisfy the hard delay and high packet delivery ratio constraints of the safety application under application level data traffic. Vehicles utilize VLC for safety message dissemination within the platoon when the multiplatoon has high vehicle density leading to high medium contention. DSRC is adopted for platoon based data dissemination when

VLC is disconnected within the dissemination distance. We demonstrate that the proposed hybrid protocol improves both packet delivery ratio and delay by limiting the contention to the line-of-sight vehicles.

Özetçe

Otonom taşıtlar bir çok sensörü birlikte kullanarak ileri yazılım sistemleri tarafından insan girdisi olmaksızın seyahat etmektedir. Otonom taşıt grupları otonom davranışın gelişmiş hali olup, taşıtların kablosuz iletişim vasıtası ile yakın mesafelerde trafik verimliliğini, seyahat güvenliğini, yakıt tüketimini ve gaz emisyonunu iyileştimeyi hedeflemektedir. Diğer taraftan, birbirini takip eden otonom taşıt grupları çoklu otonom taşıt grupları olarak bilinmektedir. Otonom taşıt grupları ve çoklu otonom taşıt grupları yürürlükte olan radyo frekans (RF) bazlı IEEE 802.11p'yi (DSRC) taşıtlar arası iletişim için kullanmaktadır. Fakat, DSRC tıkanıklık kaynaklı başarım verim kaybı, RF kıtlığı ve güvenlik gibi problemlerden olumsuz yönde etkilenmektedir. Görünür Işık ile İletişim (VLC) oldukça yeni bir alternatif teknoloji olup, ışık yönlülük ve geçirmezlik özellikleri ile DSRC problemlerini hedeflemekte ümit vadetmektedir. Fakat, otonom taşıt gruplarında VLC kullanımı VLC'nin dış ortam koşullarna duyarlılığı örneğin sis, taşıtlar arası uzaklık ve/veya virajlı yol kaynaklı kısa süreli iletişim kesintileri nedeni ile otonom taşıt grubu kararlılığını sekteye uğratmaktadır. Bu tez kapsamında melez DSRC ve VLC kullanım temelli güvenli ve verimli iletişim yapılarına odaklanmaktayız.

İlk olarak, VLC iletişim sınırlarını belirleyebilmek için taşıtsal VLC iletişim nitelikleri deneysel olarak tekil ve ikili kanal bazlı veri iletimi halinde olacak şekilde değişken ışık karartma düzeyleri ve açılarında taşıtsal ortamda analiz edilmiştir. Yapılan deneysel çalışma Lambertian ışınım modelinin hızlı anahtarlama diyot içeren lamba (LED) ışınım modelini doğru bir şekilde yansıtmadığını, ikili kanal kullanımının açısal sınırı tekil kanal veri iletimine göre 10 derece arttırdığını ve ışık karartma seviyesinin VLC veri iletimini ve ölçümlenen sinyal gücünü etkilediği gösterilmiştir.

İkinci olarak, veri çarpıtma, veri yeniden gönderme, sahte grup manevra paketi oluşturma ve sinyal boğma saldırıları altında otonom taşıt grubu kararlılığı ve güvenli grup manevraları sağlanması için melez DSRC ve VLC temelli, SP-VLC isimli güvenlik protokolü önermekteyiz. Farklı senaryolarda sahte grup isteği ve sahte grup yanıtı veri paketlerinin yol kenarında varsayılan saldırgan tarafından gönderildiği sahte otonom grup manevra saldırısı tanımlanmıştır. SP-VLC sadece hedeflenen taşıt ile iletişim için gizli anahtar oluşturumu ve VLC ile peryodik anahtar güncellemesi, mesaj aslıyla aynılık kodu kullanımı ile paket bozulmamışlığı ve aslıyla aynılık kanıtlanımı, ardışık taşıtlar arasında oluşturulan gizli anahtar ile şifrelenen ve çözülen verinin DSR ve VLC tümleyici nitelikleri kullanımı ile iletilmesi, paket alınım nitelikleri temelli sinyal boğma saldırısı saptanımı ve sadece VLC ile iletişime geçiş ve ortak DSRC ve VLC kullanımı ile güvenli otonom taşıt grubu manevra gerçeklenim süreçlerini içermektedir. Önerilen SP-VLC protokol işlevselliği detaylı analizler yapılarak var olan tüm saldırılar altında gösterilmiştir. Gerçekçi taşıt devinimlik, VLC ve DSRC kanal modelleri ve otonom taşıt grubu yönetimi kullanılarak simülasyon platformu geliştirilmiş, daha önce önerilen ve otonom taşıt grubu üyeleri arasında hız ve uzaklık değişiminin sırası ile 25% ve 10% olduğu DSRC ve DSRC-VLC melez yönetim protokollerine göre SP-VLC otonom grup üyeleri arasında 0.1%'den az hız ve uzaklık değişimi ile grup kararlılığını sağlamıştır.

Üçüncü olarak, uygulama katmanı veri trafiği altında gecikme süresi ve veri paketi dağıtım yüzdesi gereksinimlerini sağlamak için DSRC ve VLC temelli çoklu otonom taşıt grubu veri iletim protokolü önermekteyiz. Taşıt yoğunluğun yüksek ve kanal tıkanıklığına neden olduğu çoklu otonom taşıt gruplarında grup üyeleri veri iletimi için VLC kullanmaktadır. Önerilen melez veri iletim protokolünün kanal erişim çekişmesini görüş açısında bulunan taşıtlara kısıtlayarak veri paketi dağıtım yüzdesini ve gecikme süresini iyileştirdiği gösterilmiştir.

Contents

Chapter 1

Introduction

1.1 Vehicular Ad Hoc Networks

Advances in the automobile industry and urbanization make vehicles connected with each other as well as with city infrastructure. There exist more than a billion vehicles in worldwide and it is believed that the number would get doubled within the next 10 to 20 years. Expanding on this vision, it is expected that in near future a series of critical issues such as transportation safety, traffic congestion, traffic accident, energy waste and pollution are becoming far more important in modern Intelligent Transportation System (ITS) and Intelligent Traffic System (ITF). The lack of traffic information, slow reaction of drivers to the events are the major causes of these problems that require alternative solutions. Vehicular ad hoc network (VANET) is proposed to mitigate these problems by the communication between vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) or both [1] based on DSRC.

The enhanced vehicular connectivity in ITS and ITF aims to increase the traffic safety, reduce traffic congestion, prevent traffic accidents, decrease energy waste and pollution by providing timely and efficient data dissemination about events like accidents, road condition and traffic jams beyond the driver knowledge. An autonomous vehicle, on the other hand, is a new vehicular technology that offers the possibility fundamentally changing the ITS and ITF and it has the potential to substantially affect the vehicular

networks. Autonomous vehicles have recently gained popularity with the successful demonstration by Google where a self-driving car has completed 700.000 miles across the United Sates [2]. Starting from this, automation has become an active research field in the automotive industry where the mainstream manufacturers are currently investing on it.

Apart from these, developments in wireless technology bring autonomous platoon and multiplatoon into the reality. An autonomous vehicle platoon is a group of cooperative adaptive cruise control (CACC) vehicles kept in close proximity through wireless communication [3,4] based on IEEE 802.11p (DSRC). The chain of platoons that follow one-another instead of organizing vehicles as one big platoon, on the other hand, refers to multiplatoon [5, 6]. It is expected that with the increased demand for autonomous vehicles, platoons and multiplatoons would be the large part of our lives in the near feature. These, however, create new challenges that need to be addressed such that scarcity of radio frequency (RF) spectrum, DSRC performance degradation due to congestion, the security vulnerabilities of DSRC, timely and reliable safety message dissemination over a multiplatoon. These challenges suggest the use of security protocols and data dissemination techniques in conjunction with alternative communication technologies for the vehicular environment such as Visible Light Communication (VLC). VLC is a relatively new communication technology that uses modulated optical radiation in the visible light spectrum to carry digital information. The distinguished propagation characteristics of light make VLC a promising complementary technology with the potential to address DSRC problems [7].

In order to satisfy the security and safety message dissemination requirements, hybrid protocols in which DSRC and VLC are used collaboratively is of paramount importance. This thesis investigates the hybrid usage of DSRC and VLC in autonomous platoon/multiplatoon with the goal of achieving secure and efficient communication architecture. This thesis is organized as different chapters focusing on the variety of aspect with different security and efficiency related objectives and requirements.

1.2 Original Contributions

The original contributions of the thesis are as follows:

- Characteristics of vehicular VLC links are experimentally analyzed with different scenarios including single channel and dual channel data transmission considering various light dimming level and the bearing angle of values with the goal of determining the usage limitation of VLC in vehicular communication. It is demonstrated that state of the art Lambertian radiation pattern does not represent the automotive light emitting diode (LED) radiation pattern accurately. Dual channel usage increases the angular limitation by up to 10°compared to the single channel VLC and dimming is a key parameter in VLC, which affects data dissemination and received power signal strength.

- A military light communication-based security protocol, namely SecVLC, is proposed to secure vehicular military visible light communication where directionality of light is used with a key exchange mechanism to ensure only the participating vehicles understand the contents of the messages. The SecVLC is experimentally evaluated in the vehicular environment with a malicious insider to ensure fully reliable communication. It is demonstrated that despite VLC limits the data reception due to its directional transmission, it still possible to receive and decode the data packet if the adversary locates in light coverage. On the other hand, secret key enabled SecVLC prevents adversary packet reception and achieves confidential data transmission with short delay and high rate of packet delivery.

- DSRC and VLC based hybrid security protocol for platoon communication, namely SP-VLC, is proposed with the goal of ensuring platoon stability and enabling platoon maneuvers under data packet forgery, data packet replay, fake maneuver packet and jamming attacks. It is demonstrated that DSRC based platoon management is highly vulnerable to attacks from adversaries. VLC reduces the effect of adversaries due to the light directivity decreasing the coverage of adversaries.

However, adversaries can still ruin the platoon stability degrade the traffic throughput when vehicles are in both DSRC and VLC transmission range of malicious actors. SP-VLC, on the other hand, includes mechanisms for secret key establishment and periodic update via the usage of VLC to ensure the participation of only the target vehicle in communication; authentication with the usage of message authentication code to ensure the integrity of the packets; data transmission over both DSRC and VLC incorporating the encryption and decryption of the packets using the secret key generated between consecutive platoon members in the vehicle platoon to exploit the complementary propagation characteristics of data transmission over these protocols; jamming detection and reaction to switch to VLC only communication based on packet reception characteristics; and secure platoon maneuvering based on the joint usage of DSRC and VLC while exploiting the directionality, limited range and impermeability properties of VLC. SP-VLC achieves less than 0.1% difference in the speed and performs any maneuvers without interference from attackers.

- DSRC and VLC based safety message dissemination protocol is introduced to satisfy the hard delay and high packet delivery ratio constraints of the safety application under application level data traffic. Vehicles utilize VLC for safety message dissemination within the platoon when the multiplatoon has high vehicle density leading to high medium contention. DSRC is adopted for platoon based data dissemination when VLC is disconnected within the dissemination distance. We demonstrate that the proposed hybrid protocol improves both packet delivery ratio and delay by limiting the contention to the line-of-sight vehicles. It is demonstrated that proposed hybrid protocol improves both packet delivery ratio and delay by limiting the contention to the line-of-sight vehicles.

1.3 Organization

The rest of the thesis is organized as follows;

- Chapter 2 presents dual channel vehicular VLC for enhanced vehicular connectivity and demonstrates the limitation of single and dual channel data dissemination. The objective of this chapter is to experimentally analyze the state of the art Lambertian radiation pattern and model the channel characteristics of single and dual channel data dissemination for vehicular VLC in outdoor scenarios [8,9]. We demonstrate that state of the art Lambertian radiation pattern does not represent the automotive light emitting diode (LED) radiation pattern accurately. Dual channel usage increases the angular limitation by up to 10°compared to the single channel VLC.

- Chapter 3 analyzes the effect of headlight dimming utility in vehicular VLC. The objective of this chapter is to analyze the auto-dimmable headlights, which gain attention due to danger caused by sudden glare on drivers at night conditions and experimentally demonstrate the effect of dimming on vehicular VLC [10]. It is demonstrated that dimming is a key parameter in VLC, which affects data dissemination and received power signal strength.

- Chapter 4 proposes a secure light communication protocol (SecVLC) for military ad hoc network on roadways where directionality of light is used with a key exchange mechanism to ensure only the participating vehicles understand the contents of the messages [11, 12]. The objective of this chapter is to experimentally evaluate the SecVLC in the vehicular environment with a malicious insider to ensure fully reliable communication. We demonstrate that despite VLC limits the data reception due to its directional transmission, it still possible to receive and decode the data packet if the adversary locates in light coverage. On the other hand, secret key enabled SecVLC prevents adversary packet reception and achieves confidential data transmission with short delay and high rate of packet delivery.

- Chapter 5 analyzes the security vulnerabilities of the autonomous platoon and proposes DSRC and VLC based hybrid security protocol for platoon communication, namely SP-VLC. The objective of this chapter is to categorize the attacks from adversaries, to analyze the behavior of the autonomous system under security attacks and propose a hybrid security protocol that achieves confidentiality, authenticity, resilience to jamming and secure platoon maneuvering based on the joint usage of DSRC and VLC [13–16]. We develop a simulation platform combining realistic vehicle mobility model, realistic VLC and DSRC channel models and vehicle platoon management for the first time in the literature. We show that DSRC based platoon management is highly vulnerable to attacks from adversaries. VLC reduces the effect of adversaries due to the light directivity decreasing the coverage of adversaries. However, adversaries can still ruin the platoon stability degrade the traffic throughput when vehicles are in both DSRC and VLC transmission range of malicious actors. SP-VLC achieves less than 0.1% difference in the speed and performs any maneuvers without interference from attackers.

- Chapter 6 proposes hybrid DSRC and VLC based dissemination protocol for multiplatoon to satisfy the delay and packet delivery ratio requirements of safety applications. The objective of this chapter is to analyze the safety message dissemination schemes on multiplatoon under application level data traffic [17, 18]. We demonstrate that the packet loss results in low packet delivery ratio in DSRC based multiplatoon. VLC is utilized for intra-platoon communication when the multiplatoon has high vehicle density leading to high medium contention. Although VLC increases the safety message dissemination performance, hybrid DSRC-VLC platoon architecture still suffers from the disconnected network.

- Chapter 7 presents the concluding remarks and possible research directions.

Chapter 2

Dual Channel Visible Light Communications For Enhanced Vehicular Connectivity

2.1 Introduction

The enhanced connectivity among vehicles in Intelligent Transportation Systems (ITS) aims to reduce traffic accidents by providing timely and efficient data dissemination about events like accidents, road conditions and traffic jams beyond the driver's knowledge. Current vehicular communication architectures mainly adopt Dedicated Short Range Communication (DSRC), Long Term Evolution (LTE) or a hybrid of both [1]. Recently, as an alternative to DSRC and LTE, the usage of VLC technologies has been investigated. VLC uses modulated optical radiation in the visible light spectrum to carry digital information in free space. LED has become very common in automotive lighting due to its long service life, high resistance to vibration, and better safety performance. LEDs are used in the stop lamps, brake lights, turn signals, and headlamps of many vehicles. VLC provides a low cost alternative to the radio frequency (RF) based wireless communication. Moreover, VLC communication is robust to malicious attacks such as intentional jamming from surrounding, and does not cause any electromagnetic interference.

Vehicular VLC has been investigated for its channel characteristics [19–22], handover capabilities [23], requirements [24–27] and feasibility in a hybrid architecture together with DSRC [28, 29]. Proposed vehicular VLC schemes are studied either experimentally [19–21, 24, 26] by using a single LED light or via computer based simulations [22, 23, 25, 27–29] using Lambertian property of LEDs. However, in [19], it is demonstrated that Lambertian property does not hold for the off-the-shelf scooter tail light. Also, none of the studies have experimentally analyzed the single automotive LED light usage limitations for separate channel usage and dual automotive LED light utilization for extended connectivity.

It is foreseen that remote controlling of vehicles in closed formations such as platoon will efficiently reduce traffic jam and fuel consumption [30]. However, one of the key challenges in highly autonomous platooning is to provide a secure communication robust to intentional jamming from surrounding, where VLC is a strong candidate technology for the solution [25]. Despite its jam-free nature, the limited range of angles over which PD can collect data, known as field of view (FOV) limitation, is a debated topic regarding the VLC suitability for platooning. Thus, few studies investigated VLC FOV limitations [27–29]. [27] studied methods to enhance FOV for platooning by using the Lambertian property of LEDs and employing optical arms in a simulation environment. Authors in [28], [29] considered complementing VLC with RF based technologies, ending up with a hybrid framework to overcome FOV limitations and increase communication reliability. None of the proposed studies, nevertheless, performed outdoor experimental evaluations. Moreover, the mechanisms proposed to improve FOV require additional hardware such as optical arms and RF front-end.

The goal of this chapter is to experimentally evaluate the dependency of the single channel received optical power on angular and spatial variations, and compare dual channel VLC with single channel VLC performance to determine vehicular VLC limitations by using LED fog lights in varying road curvature conditions. The original contribution of this chapter is threefold. First, the characteristics of the VLC link in line of sight (LoS) is investigated and compared with its Lambertian model. Second, the usage limitations of

single LED fog light are defined for separate channel use cases. Third, the effect of the dual channel usage of VLC in varying inter-vehicular distances and angles is analyzed. We demonstrate that dual channel usage can improve the angular limitation and reliability of VLC in certain scenarios.

The rest of the chapter is organized as follows. Section 2.2 describes the experimental setup for VLC communication. Section 2.3 introduces the Lambertian model and the switching limit calculation from single to dual channel VLC. Section 2.4 presents the experimental results. Finally, conclusions and future work are given in Section 2.5.

2.2 Experimental Setup

Figure 2.1: Vehicular VLC Experimental Setup

In the experimental setup, two symmetrical LED fog lights [31] are connected to Li-1st [32] transmitter unit (TU) and PD based receiver unit (RU) as shown in Fig. 2.1. Dual symmetrical LED fog lights are mounted on tripods with 36 cm height and 150 cm separation distance. Automotive fog lights are preferred to provide reliable communication from the following vehicle to the leading vehicle under degraded visibility conditions since they have wide and flat illumination pattern to minimize reflection by fog. Li-1st TU is used for driving LED fog lights in order to illuminate and transfer custom created 150 byte length data packets. As TU is able to provide more

voltage but less current required to operate fog light properly, it is terminated with 20 W 50Ω power resistor, decreasing the nominal light intensity by 8 dBm. Despite this intensity degradation, transmission pattern of the LED fog light did not show any deviation when compared to nominal intensity. TU utilizes Pulse Amplitude Modulation (PAM) scheme along with Reed-Solomon coding operating at a sample rate of 2.5 Mbps, allowing 5 Mbps data rate with 4PAM.

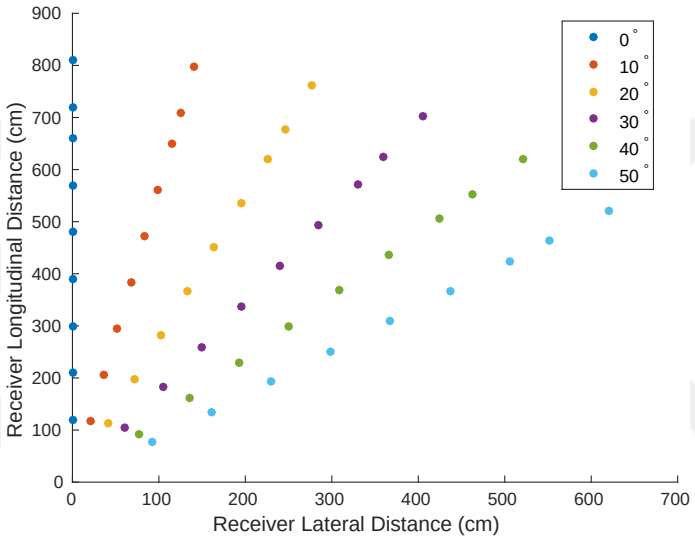


Figure 2.2: Receiver Locations

Received power is measured via OMM-6810B Optical Power Meter using OMH-6703B Si power head. Transmitted data is captured with Li-1st RU. Both TU and RU are connected to computers for evaluating communication performance. Night time outdoor measurements are executed to compensate shot noise, sourced by diurnal variations. RU and Si-power head of optical power meter is mounted on tripods with 36 cm height at the center of the leading vehicle's bumper. Both fog lights and RUs are placed between vehicles in an outdoor environment to take into account the reflections from vehicles and road. Measurements emulated the following vehicle disseminating safety critical message (i.e. slip, lane change intention) with LED fog lights, to the leading vehicle proceeding on a curved path. Thus, receiver distance is changed from 1.2 to 8.1 meters, with varying angles from 0° to

50°, as shown in Fig. 2.2, while LED fog lights are fixed.

Two different use case scenarios are considered. In the first single channel VLC scenario, one of the LED fog lights is turned on. This corresponds to the case where two separate LED fog lights transmit different messages on different channels simultaneously. In the second dual channel VLC scenario, both LED lights transmit identical messages at the same time to overcome single LED fog light limitations for enhanced connectivity. Hence, optimal switching limits between single and dual channel VLC depending on inter-vehicular distance and angle are defined for sustaining safety critical message link.

2.3 Communication Model

2.3.1 Lambertian Model

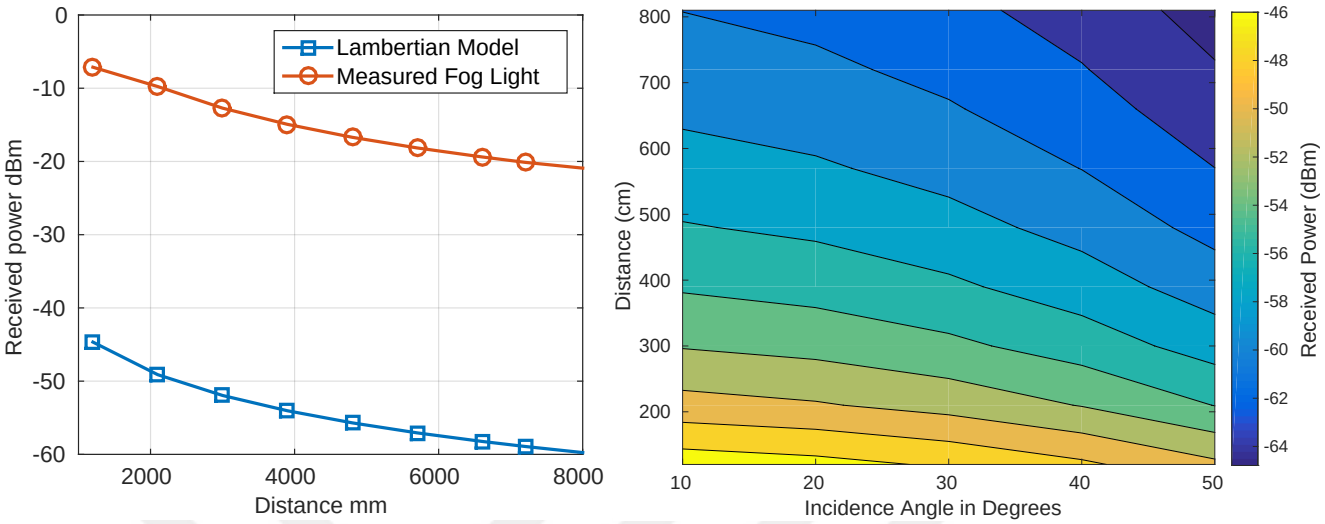
A single LED light usually as the Lambertian radiation pattern [33]. The optical channel DC gain $H(0)$ in this model is given as

$$H(0) = \begin{cases} \frac{(m+1)A_{pd}}{2\pi d^{\Gamma}} cos^{m}(\varphi) T_s(\Psi) g(\Psi) cos(\Psi), & 0 \leq \Psi \leq \\ \Psi_c & \\ 0, & \text{elsewhere} \end{cases} \tag{2.1}$$

where d is the inter-vehicle distance; φ is the irradiance angle; Ψ is the incidence angle; Ψ_c is the PD FOV; A_{pd} is the active receiver area of the PD; Γ is the path loss exponent; $T_s(\Psi)$ is the filter gain of value 1; $g(\Psi)$ is the gain of an optical concentrator calculated by,

$$g(\Psi) = \begin{cases} \frac{n^2}{sin^2(\Psi)}, & \text{if} |\Psi| \leq \Psi_c \\ 0, & \text{if} |\Psi| > \Psi_c \end{cases} \tag{2.2}$$

in which n is the internal refractive index of PD; m is the order of Lambertian model specifying the directivity of the transmitter and computed by $m = -\frac{ln2}{ln(cos\hat{\phi})}$, in which $\hat{\phi}$ is the half-intensity beam angle of LED. The coverage range and radiation pattern of single LED light is affected by the



(a) (b)

Figure 2.3: (a) Lambertian vs. Off-The-Shelf Fog Light (b) Estimated Lambertian Pattern

half-intensity beam angle $\hat{\phi}$ such that narrower $\hat{\phi}$ increases the illumination range. The average received optical power P_r is calculated by

$$P_r = H(0)P_t \tag{2.3}$$

The half-intensity beam angle and path loss exponent values are estimated by using linear least square methods based on the measured received power with varying distances up to 8.1 meters and incidence angles from 0 to 50° [19]. A_{pd} and n values are 28 mm^2 and 1, respectively. $\varphi = \Psi$ as both RU and TU are located at the same height, while P_t is 8 dBm for each LED fog light.

2.3.2 Usage Limitations Calculation

The receiver sensitivity levels for the received optical power are determined to be -33 and -30 dBm for single and dual LED fog lights, respectively, depending on the RU characteristics. As overlapped light intensity causes PD saturation and optical automatic gain control (AGC) is not utilized due to the complexity of gain characterization under various road lighting conditions,

receiver sensitivity level using dual LED fog lights is considered 3 dBm higher to ensure reliable reception. The received optical power measured at the optical power meter is first compared to these thresholds to calculate the spatial and angular limitations of single and dual LED lights. Then the data packet delivery ratio (DPDR) metric is inspected for validation purposes. DPDR is defined as the ratio of the number of successfully received data packets to the total number of transmitted data packets.

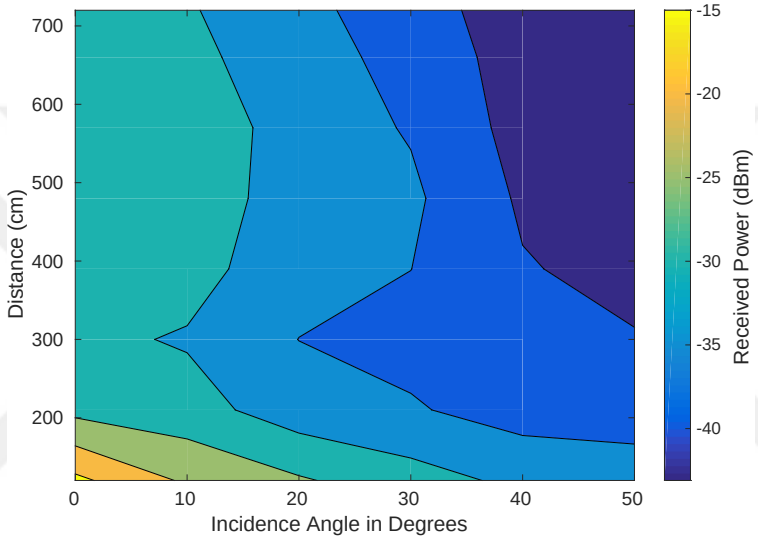


Figure 2.4: Single Channel Fog Light Pattern

2.4 Performance Evaluation

2.4.1 Single Channel VLC

Fig. 2.3 and Fig. 2.4 show the comparison of the Lambertian model to the single channel experimental data. The path loss exponent and half-intensity beam angle of the LED fog light are estimated to be as 1.8319 and 50.66°, respectively. Lambertian radiation pattern with estimated parameters is evaluated and compared with the measured model. We observe that Lambertian model is not appropriate for link modeling, as depicted in Fig. 2.3 (b) and Fig. 2.4. Even though the received power decrement patterns match for both

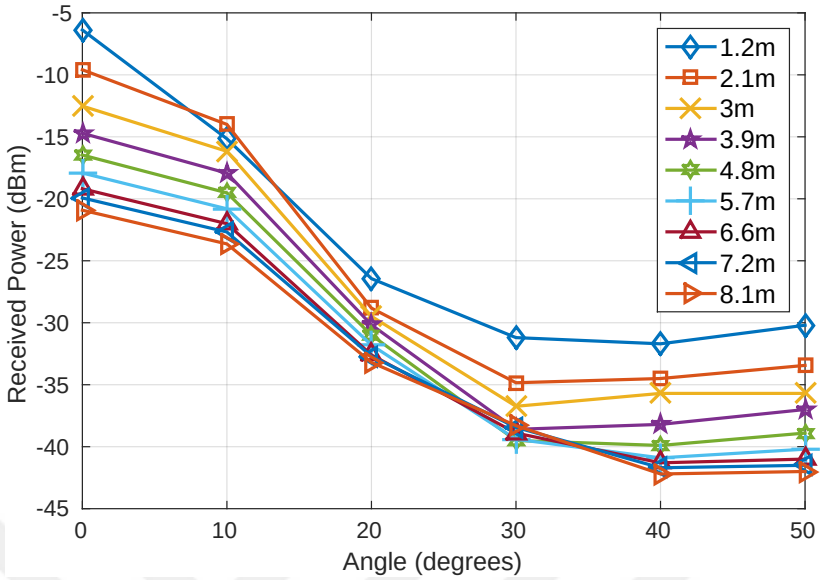


Figure 2.5: Received Power With Varying Angle and Distances

models, actual model provides more intensity due to the reflector and lens, as shown in Fig. 2.3 (a). Collimating and diffusing optics (i.e. reflector and lenses) are widely used on automotive LED lights to shape radiation pattern and achieve homogeneous lighting. Thus, despite its common acceptance, Lambertian radiation pattern is inaccurate to model vehicular VLC link.

Fig. 2.5 shows the received power at different distances and angles. We observe that received power exhibits similar degradation pattern with the increasing angle at all distances, which is consistent with the vehicle fog light regulation [34]. Results indicate that knowing the distance and angle from the leading vehicle with road curvature, following vehicle can decide switching from single to dual channel usage in order to ensure efficient safety critical message dissemination.

2.4.2 Dual Channel VLC

Fig. 2.6 shows the angular limits for single and dual channel VLC based reliable data transmission at different distances. The usage of dual channel VLC increases the angular limitation by up to 10°. This slight improvement in the

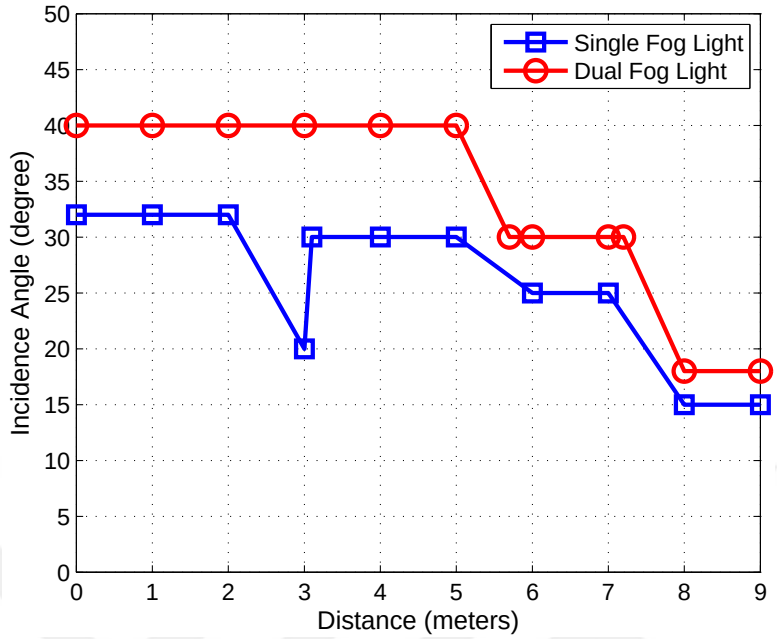


Figure 2.6: Single and Dual LED Fog Light Usage Limits

angular limits can be used for optimal switching between single and dual channel usage depending on the inter-vehicular distance and road curvature. Moreover, the angular limit of VLC communication decreases with the increasing distance for both single and dual channel communication. On the other hand, dual channel usage compensates for the 20° incidence angle limitation regarding 3 meters inter-vehicular distance which is mainly due to the collimation optics of single fog light.

Fig. 2.7 shows the DPDR performance of single and dual channel VLC as a function of distance at 0° incidence angle. Up to 6 meter distance, the dual channel VLC improves the DPDR performance due to the increase in Signal-to-Noise Ratio (SNR) by the simultaneous dual fog light usage for data transmission. For distances greater than 6 meters, PD reaches saturation due to the overlapping of fog lights, resulting in degraded efficiency. Thus, increased receiver sensitivity is considered for defining dual fog light reliable link limitations.

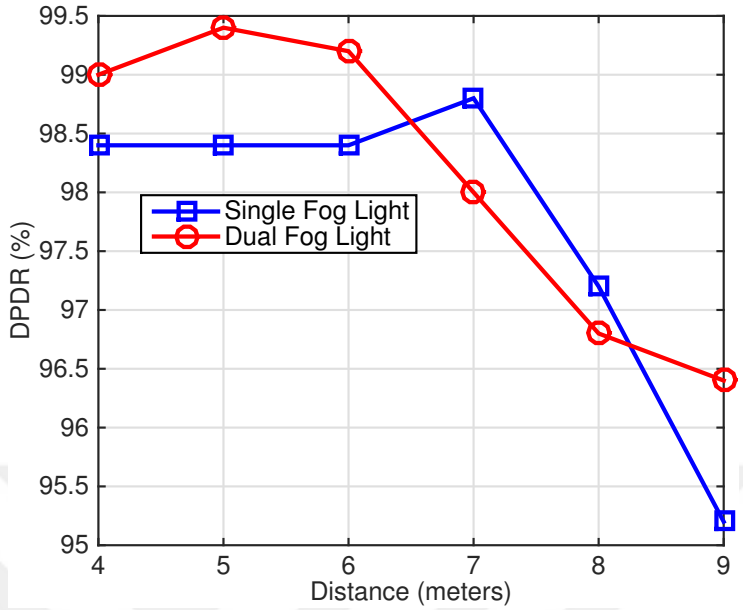


Figure 2.7: DPDR performance of single and dual channel VLC

2.5 Conclusion

VLC offers low cost, directional and jam-free LoS communication scheme viable for platooning. Due to their wide and flat illumination pattern, LED fog lights are good candidates for VLC data transmission under degraded visibility conditions. Considering the requirement for increased data transmission rates and enhanced link availability, we analyzed the limitations of reliable vehicular communication in single and dual channel VLC. Based on the outdoor experiments, we demonstrate that the dual channel usage increases the angular limitation up to 10° compared to the single channel VLC. We also show that dual channel improves the packet delivery error rate performance at only short distances due to the PD saturation sourced by light intensity overlapping at higher distances.

Chapter 3

Dimming Support for Visible Light Communication in Intelligent Transportation and Traffic System

3.1 Introduction

Advances in the automobile industry and urbanization make vehicles connected with each other as well as with city infrastructure. There exist more than 1 billion motor vehicles in worldwide and it is believed the number would get doubled within the next 10 to 20 years. Moreover, developments in wireless technology bring autonomous driver-less cars [2] into the reality where vehicles are capable of cruising by themselves. As a result, VANET, a type of mobile ad hoc network (MANET) of covering vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I), is becoming one of the most relevant network technologies. In VANETs, vehicles communicate based on IEEE 802.11p, which forms the standard for Wireless Access for Vehicular Environments (WAVE). IEEE 802.11p provides data rate ranging from 6 Mbps to 27 Mbps at short radio transmission distance, around 300 m.

The enhanced vehicular connectivity in ITS and ITF aims to reduce traffic

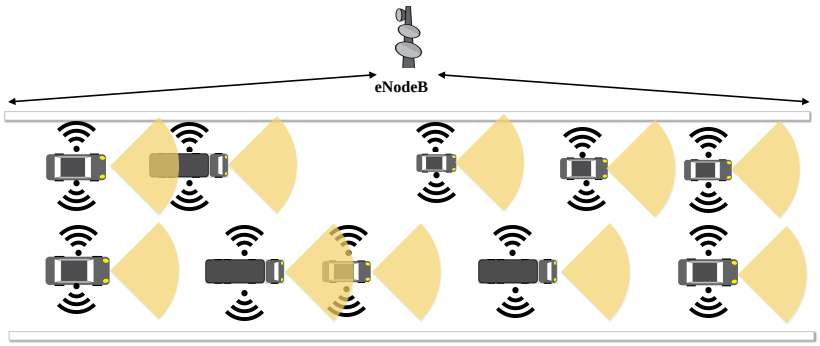


Figure 3.1: ITS and ITF System Architecture

congestion, traffic accidents, energy waste and pollution by providing timely and efficient data dissemination about events like accidents, road condition and traffic jams beyond the drivers' knowledge. Although the investment on road construction may solve the traffic congestion to some extent, it is not feasible due to reasons of high construction cost and limited availability of land. For instance, traffic congestion costs more than 100 billion annually due to wasted fuel and lost time in USA [35]. Moreover, vehicle emission caused by traffic congestion has a great detrimental effect on air pollution and haze in some large cities. On the other hand, ITS and ITF suffer from the scarcity of radio frequency (RF) where the increased wireless data traffic from the rapidly growing wireless mobile devices is creating pressure on RF spectrum. This scarcity problem leads researchers to investigate alternative technologies such as VLC, which uses modulated optical radiation in the visible light spectrum to carry digital information in free space. VLC uses fast switching light emitting diodes (LEDs) as its source and provides both illumination and communication in indoor and outdoor scenarios.

Fig. 3.1 demonstrates possible ITS and ITF architecture that mainly adopts Dedicated Short Range Communication (DSRC), Long Term Evolution (LTE) and VLC. A comparison of the key properties of both VLC and conventional RF-based (DSRC) technologies is presented in Table 3.1. DSRC is usually omnidirectional and can work both in line-of-sight (LoS) and non-line-of-sight (NLoS) scenarios in licensed frequency band 5.8 - 5.9 GHz with

Table 3.1: Comparison Of VLC and RF Key Properties

Type	**VLC**	**RF (DSRC)**
Communication Scenario	Typically LoS	Both LoS and NLoS
Transmission Range	Short Range and Highly Directional	Long Range and Usually Omnidirectional
Frequency Band	400 - 790 THz	5.8 - 5.9 GHz
Licensing	Free	Required
Cost	Low	High
Mobility	Medium	High
Weather Condition	Sensitive	Robust
Ambient Light	Sensitive	Not Affected

high mobility. VLC, on the other hand, is highly directional and typically works in LoS scenarios in short range, around 50-100 meters, with high sensitivity to weather condition and ambient light. As a wireless communication technology, VLC is beneficial due to reasons such as; it has no health concern, it does not cause any electromagnetic interference, it is license free and it can easily be integrated with existing LED equipped motor vehicles with low-cost additional onboard units. These distinguished characteristics make VLC attractive in both academia and industry where the IEEE 802.15 working group for wireless personal area networks (WPAN) standardized the PHY and MAC layer for VLC in the IEEE 802.15.7 task group [36].

In VANET settings, VLC is a suitable communication technology where most of the components that enable visible light communication are already equipped in vehicles. Any light emitting technology can be used as transmitter where modern vehicles have already started to use LEDs due to their long service life, high resistance to vibration and better safety performance. LEDs are used in the stop lamps, brake lights, turn signals and headlamps of many vehicles. On the other hand, VLC receivers are mostly either photo-diode (PD) [37, 38] or CMOS camera [39] which can be found in many vehicles as the front or rear camera for lane tracking and parking purposes. In literature, vehicular VLC has been investigated for different purposes such as channel characteristics [19–22], handover capabilities [23], requirements [8, 24–27, 40] and feasibility in a hybrid architecture together with DSRC [28, 29, 41]. Proposed vehicular VLC schemes were studied either experimentally [19–21, 24, 26, 40] by using a LED in outdoor condition or via

computer-based simulations [22, 23, 25, 27–29] using Lambertian property of LEDs.

To date, a majority of research concerning vehicular VLC was aimed at achieving high data rates via analyzing the channel characteristics. However, data rates with respect to lighting quality and its correlation with dimming utility had mostly been overlooked. Moreover, auto-dimmable headlights gain attention due to danger caused by high, bright beam of headlights which create a sudden glare while driving at night condition [42, 43]. This sudden glare has a crucial effect on driver where it causes a temporary blindness to a person resulting in road accidents. To prevent the driver from this blindness in vehicular VLC system, dimming is proposed where the light sources are arbitrarily dimmed. Dimming is beneficial in terms of energy efficiency and life span where dimmed lamp requires less current and it produces less heat which extends its lifetime. However, achieving efficient dimming control in VANET-VLC link is difficult since dimming has an adversary effect on communication [44]. Due to fixed average intensity, the achievable data rate is decreased. Dimming is provided via changing the forward current through the LED where forward current determines the brightness level. Lower brightness level has a crucial effect on both signal-to-noise ratio (SNR) and bit error rate (BER) where at lower brightness the achievable data rate and SNR are low and BER is relatively high. Moreover, external weather conditions such that fog, snow and rain may cause dimming which are needs to be considered in efficient dimming utility. As a result, detailed analysis of vehicular dimmed VLC and proper dimming techniques or protocols must developed to provide the right trade-off between illumination and communication. Analysis of dimming functionality and efficient dimming techniques in vehicular VLC systems will contribute to the safety and allow the vehicular system to have full control over the lighting output.

In this chapter, our goal is to present the latest concept of vehicular communication on ITS and ITF system and provide detailed overview of trending VLC which involves headlights dimming utility. The original contribution of this chapter is twofold. First, the characteristic of the vehicular VLC link in LoS is investigated with experimental scenarios. Second, the effect of VLC

dimming utility in varying inter-vehicular distance and dimming level is analyzed. We then demonstrate experimentally that dimming is one of the key parameters in VLC that affects the data dissemination and received power signal strength.

The rest of the chapter is organized as follows. Section 3.2 describes the experimental setup for vehicular VLC. Section 3.3 presents the experimental results. Finally, conclusion is given in Section 3.4.

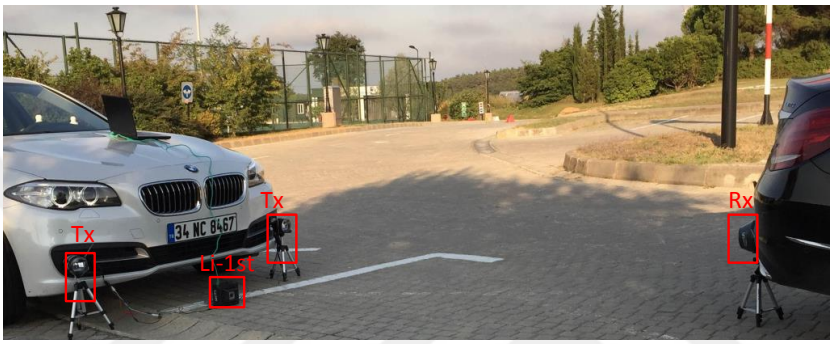


Figure 3.2: Vehicular VLC Experimental Setup

3.2 Experimental Setup

For the experiments of VLC system, two symmetrical LED fog lights [31] are connected to Li-1st [32] transmitter unit (Tx) and PD based receiver unit (Rx) as shown in Fig.3.2. Dual symmetrical LED fog lights are mounted on tripods with 36 cm height and 150 cm separation distance. In the experiments, automotive fog lights are preferred due to their wide and flat illumination pattern to minimize reflection by fog. Custom created 150-byte length data packets are transferred with the Li-1st Tx which is driven by LED fog lights. Tx utilizes Pulse Amplitude Modulation (PAM) scheme along with Reed-Solomon coding operating at a sample rate of 2.5 Mbps, allowing 5 Mbps data rate with 4PAM.

Received power is measured via OMM-6810B Optical Power Meter using OMH-6703B Si power head. Transmitted data is captured with Li-1st Rx.

Both Tx and Rx are connected to computers for evaluating communication performance. Night time outdoor measurements are executed to compensate shot noise, sourced by diurnal variations. Rx and Si-power head of optical power meter are mounted on tripods with 36 cm height at the center of the leading vehicle's bumper. Both fog lights and Rxs are placed between vehicles in an outdoor environment to take into account the reflections from vehicles and road. Measurements emulated the following vehicle disseminating safety critical message (i.e. slip, lane change intention) with LED fog lights, to the leading vehicle proceeding on a curved path. Thus, receiver distance is changed from 1 to 5 meters while LED fog lights are fixed.

To analyze the dimming functionality in vehicular VLC, fog lights are driven in different dimming level changing from 0 to 9 where 0 and 9 represent minimum and maximum brightness levels, respectively. In all brightness level scenarios, experiments are performed to investigate the dimming effect on vehicular VLC. For all experimented scenarios, 100 packets are sent from Li-1st Tx unit to Rx unit.

3.3 Performance Evaluation

Performance evaluation of dimmable vehicular VLC system is done by analysing two metrics, namely data packet delivery ratio (DPDR) and Li-1st Rx unit received power in dBm. DPDR is defined as the ratio of the number of successfully received data packets to the total number of transmitted data packets. In experiments, Li-1st Tx brightness level is changed from 0 to 9 where this change is macroscopic and detected by eyes. Maximum distance, where the data is transmitted with Li-1st in dim level 9, is 10 meters.

Received power analysis at different distances with different dimming levels is demonstrated in Fig. 3.3. We observe that the received power exhibits similar degradation patterns with the increasing distance and dim level plays a critical role in the received power. Moreover, there is no major received power difference between the dim level 0 and 4. On the other hand, received power dramatically changes in dim levels 6 and 9 which affects the overall vehicular VLC system performance. Results indicate that

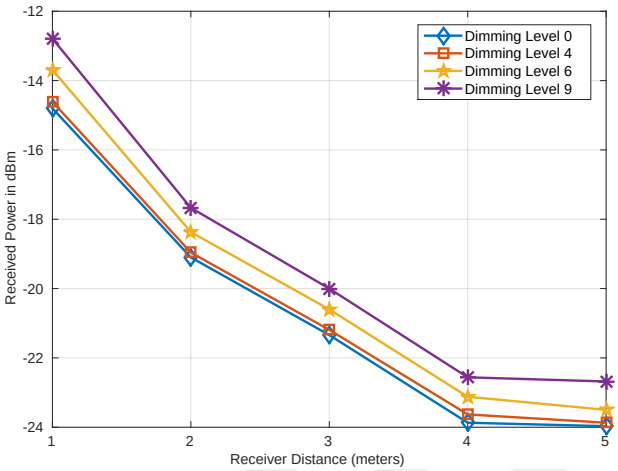


Figure 3.3: Received Power With Varying Dimming Level

knowing the distance from the leading vehicle with road information, vehicle can automatically change the dim level to ensure efficient data dissemination and prevent drivers from sudden glare at night condition.

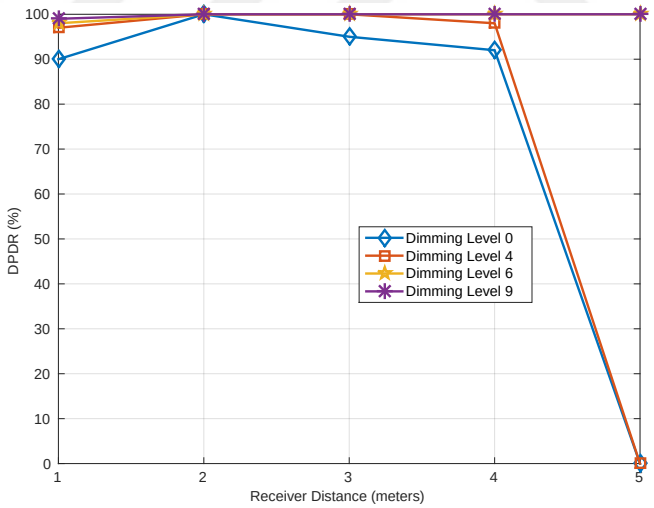


Figure 3.4: DPDR Performance of Different Dimming Level

Fig. 3.4 shows the DPDR performance of vehicular VLC system in different dim levels and distances. From DPDR analysis, it is observed that as the distance increased, the dim levels determines the DPDR value of system

whereas lower dim scenarios have lower DPDR values compared to high dim cases. For example, in scenario 5 meters where the dim levels are 0 and 4, the DPDR value is 0 where the light brightness is insufficient. Similar to dim level 0 and 4 , dim level 6 cannot transmit data after 5 meters whereas dim level 9 can transmit data up to 10 meters with 100% delivery ratio. Moreover, at short distances as the dim level increases, DPDR values also increases. Thus, dimming has crucial effect on the DPDR performance of vehicular VLC system where an adaptive dimming protocol is required to determine the desired DPDR value in safety applications.

3.4 Conclusion

Vehicular VLC is an alternative technology that offers low cost, directional and jam-free communication for ITS and ITF. To date, the majority of research concerning vehicular VLC was aimed at high data rates. However, data rates with respect to lighting quality and its correlation with dimming utility had mostly been overlooked. Sudden glare caused by high beam makes auto-dimmable headlight crucial in terms of data dissemination and safety. Considering the requirement of VLC and vehicular dimmable light, we analyzed the limitation of dimming utility in outdoor experiments. Based on the experiments, we demonstrate that dimming utility has a detrimental effect on vehicular VLC where in lower brightness level at high distances, communication is not possible. Moreover, dimming level plays a critical role in DPDR. As the dimming level increases, DPDR also increases. As part of future work, we aim to analyze different vehicle related parameters including; field of view that is the angle between the light line and the receiver, another light interference during the data transmission and vibration of vehicles. Based on the experimental analysis of vehicular parameter, we target to propose a realistic simulation platform for vehicular visible light communications.

Chapter 4

SecVLC: Secure Visible Light Communication for Military Vehicular Networks

4.1 Introduction

Technology coined as VANET is harmonizing with ITS and ITF. VANET is proposed to mitigate the problems of ITS and ITF as well as the traffic control and optimization. VANET is a type of ad hoc network that communicates vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) or both [1] based on IEEE 802.11p (DSRC), which forms the standard for Wireless Access for Vehicular Environments (WAVE). One application area of VANET is military service, namely military ad hoc network. The research in the military ad hoc network has gained popularity and expanded to commercial applications that are promising for future.

In military ad hoc networks, team member vehicles travel as a convoy or along a multi-lane linear road segment in highway or urban roadways and share data packets with each other. Fig. 4.1 demonstrates an example military ad hoc network structure on highway in a dashed ellipse that adopts DSRC as wireless communication technology. On the roadway, military vehicles obey the traffic rules and keep the convoy structure in order to pre-

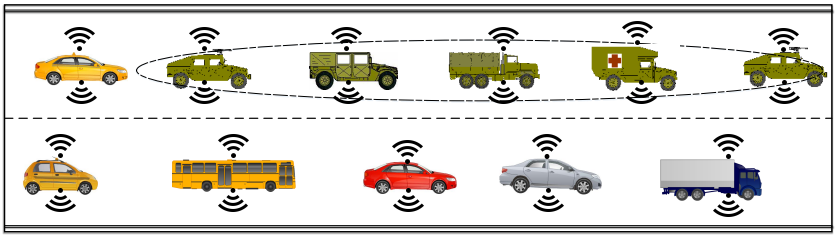


Figure 4.1: Military Ad Hoc Network Structure on Highways

vent any attack from adversary vehicles. During the transportation, tactical command vehicle that is the first or the last vehicle in the convoy initiates data transmission where the data contains the command or plan and requires timely and reliable delivery [45]. Moreover, the military ad hoc network must ensure that the disseminated data cannot be decoded by other vehicles in the communication range when data packets eavesdropped. As a result, military ad hoc network communication on roadways imposes strict requirements on the security of the communication channels used by vehicles and hence requires secure protocols.

Currently, VANET security solutions mainly focus on the dominant vehicular communication technology, DSRC which suffers from the scarcity of RF and it is open to security attacks such as jamming and spoofing. Any adversary device or vehicle within the transmission range can send the jamming signal to block the communication between military vehicles. In the spoofing attack, on the other hand, the adversary overhears the DSRC channel and impersonates another military vehicle in order to inject faulty information into a specific area. Although DSRC based VANET technologies have evolved over time [46], they suffer from the security vulnerabilities and they are not directly applicable to military communication. One example solution can be enabling the vehicle to have a daily key for communication. However, there exist some incidents where hackers succeed in acquiring the secret key [47] by eavesdropping the DSRC channel.

On the other hand, the scarcity of RF spectrum has led researchers to investigate alternative technologies. VLC is a relatively new communication technology that uses modulated optical radiation in the visible light spectrum

to carry digital information. Recently, many researchers are investigating vehicular VLC for different purposes such as channel characteristics [19, 22], requirements [8, 10, 40] and feasibility in a hybrid architecture with DSRC [41]. Proposed vehicular VLC schemes were studied either experimentally [8, 10, 19, 40] or via computer-based simulations using Lambertian property of LEDs [22].

One feature that makes VLC superior in comparison to DSRC is security. The light directivity and impermeability of the optical signal facilitate secure data communication where it is ensured that only target vehicles participate in the communication, making data difficult to receive rather than the light coverage. Furthermore, due to the directivity of the VLC transceivers, attackers need to direct strong light to saturate the receiver which can only be performed on a single VLC link, as opposed to all vehicles in the communication range in the case of DSRC. From this perspective, VLC is a promising technology to alleviate the security problems of DSRC in the vehicular environment. However, security implication of vehicular VLC had mostly been underrated and there exist only a few studies focusing on non-vehicular scenarios [48, 49]. On the other hand, secure light communication that ensures only the participating vehicles can extract and understand the content of the data is crucial for several vehicular applications.

In this part of our work, we propose a secure light communication protocol (SecVLC) for military ad hoc network on roadways where IR is utilized to share a secret key and VLC is used to receive encrypted data between vehicles. The contribution of this study is threefold. First, light directionality property is used for ensuring that only target vehicles participate in the communication. Second, vehicles use full-duplex communication where IR is the outgoing link to share a secret key and VLC is the incoming link to receive encrypted data. We experimentally evaluate the suitability of SecVLC in outdoor scenarios at varying inter-vehicular distances with key metrics of interest, including the security, data packet delivery ratio and delay. Third, to the best of our knowledge, the proposed protocol SecVLC is the first work to secure light communication in the vehicular environment.

The organization of the chapter is as follows. Section 4.2 presents the

state-of-the-art improvements in VLC technology. A detailed comparison of DSRC and VLC is demonstrated in Section 4.3. Section 4.4 describes the used system model. The details of SecVLC protocol are presented in Section 4.5, followed by the experimental results in Section 4.6. Finally, concluding remarks are given in Section 4.7.

4.2 VLC Technology

The field of VLC has undergone significant research advancements over the past decade which only serves to further emphasize the enormous potential of the technology for a wide range of applications. Gigabit-class connectivity has been demonstrated under laboratory conditions by means of commercially available LEDs [50, 51]. Similar speeds have also been demonstrated with a new class of LED devices, called micro-LEDs, with sizes in the order of tens of micrometers. The performance of these micro-LEDs indicates that potentially every pixel of every screen, as well as every indicator light on a device, can be transformed into a high-speed visible light communication transmitter. Further, impressive results in the field have shown that laser-based light sources have the potential to unlock wireless communication rates in the order of hundreds of Gigabits per second [52, 53]. Complementarily, the high-speed demonstrations of the optical transmitters' capabilities have been with a variety of photodetectors being employed. Avalanche photodiodes (APDs) have been widely adopted in high-speed applications where high sensitivity is required [54], whereas single photon avalanche photodiode (SPAD) based detectors are under development and have been demonstrated working with complex modulation schemes such as orthogonal frequency division multiplexing (OFDM) [55]. In addition, solar panels have also been successfully employed as energy-efficient photodetectors that can provide simultaneous energy harvesting and communication [56, 57]. Consequently, they can be used in a large variety of off-the-grid wireless communication applications. The significant research advancements in the field have been complemented with the release of the first LiFi wireless adaptor - the LiFi-X - which supports wireless links comparable to existing WiFi

Table 4.1: Comparison Of VLC and DSRC Properties

Property	**VLC**	**DSRC**
Communication Scenario	Typically LoS	Both LoS and NLoS
Transmission Range	Short Range and Highly Directional	Long Range and Usually Omnidirectional
Latency	Very Low	< 50 ms
Data Rate	Up to 400Mb/s	Up to 54Mb/s
Frequency Band	400 - 790 THz	5.8 - 5.9 GHz
Power Consumption	Relatively Low	Medium
Spatial Reuse Efficiency	High	Low
Electromagnetic Interference	No	Yes
Licensing	Free	Required
Coverage	Narrow	Wide
Cost	Low	High
Mobility	Medium	High
Weather Condition	Sensitive	Robust
Ambient Light	Sensitive	Not Affected

networks, however, in significantly denser deployment scenarios [58].

4.3 Comparison of DSRC and VLC

A comparison of the key properties of VLC and conventional DSRC is presented in Table 4.1. DSRC is usually omnidirectional and can work both in line-of-sight (LoS) and non-line-of-sight (NLoS) scenarios in licensed frequency band 5.8 - 5.9 GHz with high mobility. VLC, on the other hand, is highly directional and typically works in LoS scenarios at short range, around 25-50 meters, with high sensitivity to weather condition and ambient light. Compared to DSRC, the maximum range of VLC is much shorter as its effective free-space path loss is 4 instead 2 in the case of RF [59]. Therefore, VLC provides much higher spatial reuse efficiency with effective interference control at high vehicle density. Moreover, multipath fading is negligible in VLC even at high vehicle mobility [60]. VLC also brings several advantages of not causing any health concern nor any electromagnetic interference, being license-free and easy integration with existing LED equipped vehicles with low-cost additional onboard units. The IEEE 802.15 working group for wireless personal area networks (WPAN) standardized the PHY and MAC layer for VLC in the IEEE 802.15.7 task group.

A typical VLC system uses fast switching light emitting diodes (LEDs) as

the transmitter to simultaneously provide illumination and communication in indoor and outdoor scenarios. VLC is a promising technology for military ad hoc network with most of the communication components already existing within vehicles. Modern vehicles have already started to use LEDs due to their long service life, high resistance to vibration and better safety performance. LEDs are used in the stop lamps, brake lights, turn signals and headlamps of many vehicles. On the other hand, VLC receivers are mostly either photo-diode (PD) [38] or CMOS camera [39] which can be found in many vehicles as the front or rear camera for lane tracking and parking purposes.

In real-world vehicular VLC deployments, it is difficult to send messages directly from the front vehicle to all team members, which are traveling in a convoy. This is due to the sharp directivity and the vehicles' bodies as obstacles. Moreover, vehicles within the coverage of the transmitting vehicle can also eavesdrop the shared packets as in DSRC. From the military ad hoc network perspective, the successful decoding of military shared information by an adversary might have disastrous effects. Therefore, secure vehicular VLC that ensures only the participating vehicles can extract and understand the content of the data, is required.

4.4 System Model

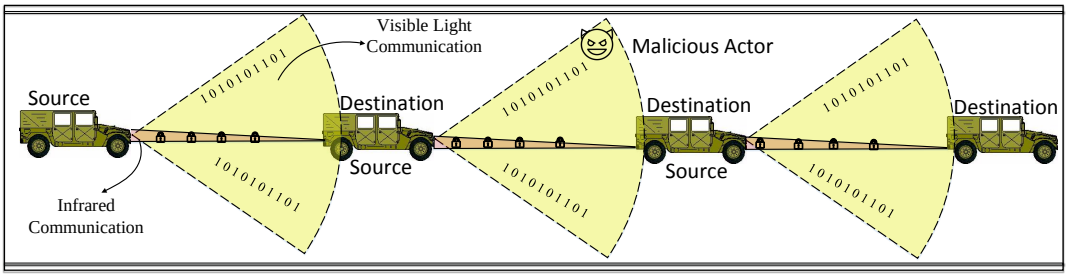


Figure 4.2: System Model for Military Visible Light Communication

The system consists of vehicles moving on the highway or urban roadways as a convoy, as depicted in Fig. 4.2. In the vehicular convoy, vehicles are

organized into groups of closely following vehicles and obey the traffic rules such as speed limit and usage of headlights. The speed variation of the vehicles in the convoy is very small. Each vehicle maintains a proper following distance by either slowing down when it gets too close or speeding up to preserve the convoy distance that is minimum 2 meters [61]. Moreover, there may exist a malicious insider in the system that overhears the communication channel and tries to extract the data content. The malicious insider can be a roadside unit or a vehicle that is not part of military ad hoc network.

The message is broadcast in the vehicle convoy in multiple hops. In other words, each vehicle can be both source and destination as shown in Fig. 4.2. In each hop, the communication of consecutive vehicles is provided via VLC, since further nodes cannot communicate with other vehicles in between. Each vehicle contains a transmitter unit connected to the LED headlights and IR receiver on the front bumper. The data is disseminated through these headlights from source to destination.

Vehicles are also equipped with the PD based receiver unit (Rx) and IR transmitter on the rear bumpers. Transmitted data packets are captured by Rx whereas the secret key is transmitted from destination to source by use of IR transmitter. Each vehicle uses IR as the outgoing link to share a secret key and VLC as the incoming link to receive encrypted data. To ensure shared secret key freshness, it is changed for each data transmission in order to prevent the system from a possible attack that can be triggered by the malicious insider. Due to LoS sensitivity of IR, it is only used for 4-bytes secret key dissemination.

4.5 Military Light Communication Confidentiality Service (SecVLC)

Features of the proposed secure light communication protocol SecVLC are as follows;

1. It uses the directionality property of VLC to ensure only target vehicles participate in the communication.

2. It utilizes the full-duplex communication where IR is the outgoing link to share a secret key and VLC is the incoming link to receive encrypted vehicle data.

3. It operates with keys generation and share mechanism that is used for the data encryption and decryption where data packets cannot be decrypted without generated keys.

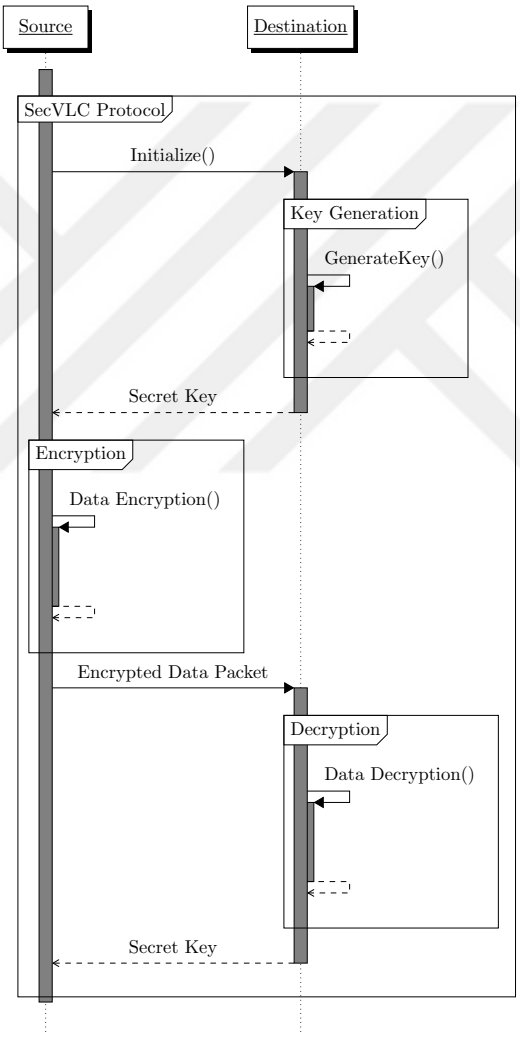


Figure 4.3: SecVLC Protocol steps

Fig. 4.3 demonstrates the steps of SecVLC protocol. SecVLC consists of five parts; initializing system, key generation, IR key transmission, data en-

cryption/decryption and VLC encrypted data dissemination. SecVLC starts by initializing the system. The system boots up its hardware components and informs the destination that it is waiting for the secret key. The destination is triggered via the incident light beam coming from the source. When the destination receives the light beams then it generates a secret key for data encryption.

Generated secret key is transmitted via IR transmitter. The narrow transmission angle property of IR enables only the following vehicle to receive the secret key, as opposed to all vehicles in the communication range in the case of DSRC. Secret keys are based on the Advanced Encryption Standard (AES) that is widely adopted due to features such as fast symmetric key generation and strength compared to other alternatives without any practical attacks against AES till to date.

After receiving the secret key from the destination, the source encrypts the data packet and transmits the encrypted packet via light beams in VLC. If any vehicle exists in the light coverage of the source, it cannot decode the data packet without the secret key. This actually solves the channel overhearing problem of DSRC based military communication.

Following the sharing of the secret key, the destination receives encrypted data packets from the source while concurrently sharing newly generated secret key via IR transmitter for the next round of data transmission. The full-duplex IR and VLC communication enable the data security without increasing delay. After receiving data packets, the destination decrypts them using the secret key. For each data message, the destination shares a secret key with the source for encryption.

4.6 Performance Evaluation

We implemented SecVLC protocol in Java on top of Li-1st transceiver software [32] that is integrated Keyczar [62] key generation toolkit. Li-1st is the first commercial product of VLC that is manufactured by pureLifi Ltd. It provides an opportunity to rapidly develop and test VLC applications that utilize commercial LED infrastructures. Li-1st consists of transmitter unit

Tx and PD based receiver unit Rx. The Tx unit is attached to two symmetrical LED fog lights [31] where automotive fog lights are preferred due to their wide and flat illumination pattern to minimize reflection by fog. On the other hand, Keyczar is an open source toolkit developed by Google for key generation.

Figure 4.4: VLC and SecVLC Experimental Setup

Two Vishay [63] high speed infra-red emitting diodes are utilized as IR transmitter and IR receiver for sharing the secret key between source and destination. Both Tx and Rx are connected to computers for evaluating communication performance. In order to compare the security vulnerabilities of communication medium, scenarios where vehicles use DSRC and visible light data transmission, namely VLC, are evaluated. The DSRC communication scenario is simulated with the convoy driving implemented simulator, VEhicular NeTwork Open Simulator (VENTOS) [64]. On the other hand, VLC and SecVLC experiments are performed in an outdoor environment as shown in Fig. 4.4 to take into account the reflections from vehicles and road. Night time outdoor measurements are executed to compensate shot noise, sourced by diurnal variations. Our experiment emulates the scenarios that are the front of following vehicle disseminating commands (i.e. mission orders, mission plan and etc.) with LED fog lights to the rear of leading vehicle proceeding on a curved path. Table 4.2 lists the experimental system parameters.

Performance evaluation of SecVLC is done in two parts. The first part focuses on the security analysis of SecVLC where the system with a malicious

Table 4.2: Experimental Setup Parameters

Parameters	Value
LED Fog Lights Ground Height	36 cm
LED Fog Lights Separation Distance	150 cm
Inter-Vehicular Distance	2 - 6 meters
Data Packet Size	100 bytes
Li-1st Modulation	Pulse Amplitude Modulation
Li-1st Error Correction	Reed-Solomon
Li-1st Data Rate	5 Mbps
Vishay IR Half Intensity	18°

insider is investigated. The malicious insider is a vehicle that is positioned on the road with constant mobility. For each experiment, 100 data packets are sent over the military ad hoc network and malicious insider tries to extract the data content. In the second part of the performance evaluation, network performance metrics are interpreted by comparing the data packet delivery ratio (DPDR) and the delay between vehicles. In each experiment, custom created 100-bytes data packet is sent. The effect of data size is considered for the different volume of data varying from 200 bytes to 500 bytes.

4.6.1 Security Analysis

In security analysis of SecVLC protocol, malicious vehicle's data decoding ratio is analyzed. Data decoding ratio is defined as the ratio of the number of successfully plain text converted data packets to the total number of transmitted data packets. In this scenario, the malicious vehicle receives the data packets and tries to decode the data for subsequent processes such as stealing the vehicle identity information.

Fig. 4.5 demonstrates that adversary vehicle can receive the data packet in both DSRC and VLC scenarios with minimum %70 data packet decoding ratio. In the DSRC, adversary vehicle overhears the channel if it is located in the transmission range (300 meters) of military vehicles. On the other hand, VLC limits the adversary data reception due to its directional transmission. However, adversary vehicle still receives the data if it is positioned in head-

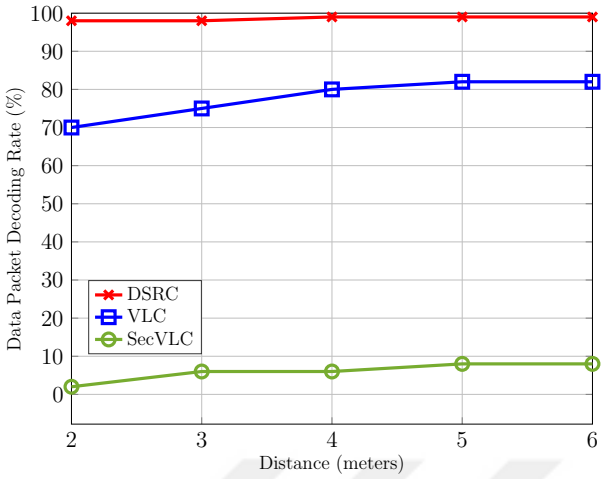


Figure 4.5: Data Packet Decoding Ratio Comparison

light coverage. Compared to DSRC and VLC, SecVLC encrypts the data packet and data content can only be decrypted with the secret key. Even if the adversary vehicle overhears the channel, it can only receive plain text control packets transmitted in the initialization phase of the protocol.

4.6.2 Network Performance Analysis

In this part of the performance evaluation, network performance of SecVLC protocol is investigated by analyzing the metrics including DPDR and the delay. DPDR is defined as the ratio of the number of successfully received data packets to the total number of transmitted data packets. The average delay metric is defined as the average latency of data packets that travel from the Source to the Destination that includes secret key IR transmission, data encryption/decryption and VLC dissemination.

Fig. 4.6 shows the DPDR comparison of SecVLC and VLC at different distances for varying data packet size. We observe that the DPDR value exhibits similar degradation patterns with the increasing distance. Moreover, as the distance gets larger, both SecVLC and VLC have difficulty in delivering data packets. This can be explained by the received signal strength (RSS), where as the distance gets larger the RSS sensed in receiver unit decreases. As a result of RSS decrease, data packets cannot be received successfully.

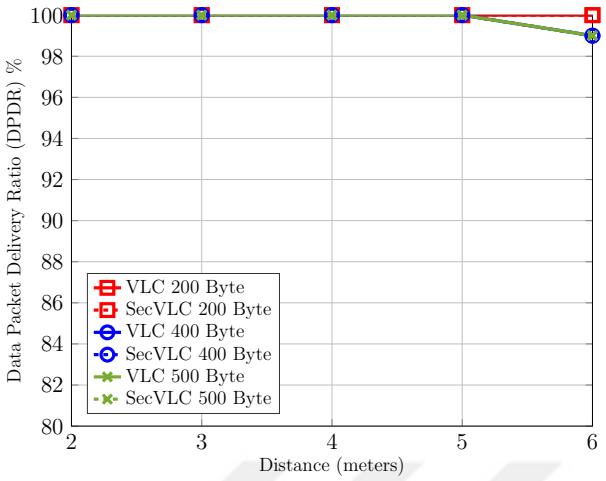


Figure 4.6: Data Packet Delivery Ratio Comparison

From this perspective, we can say that RSS decrease in the large distances is the major factor that affects the DPDR in SecVLC.

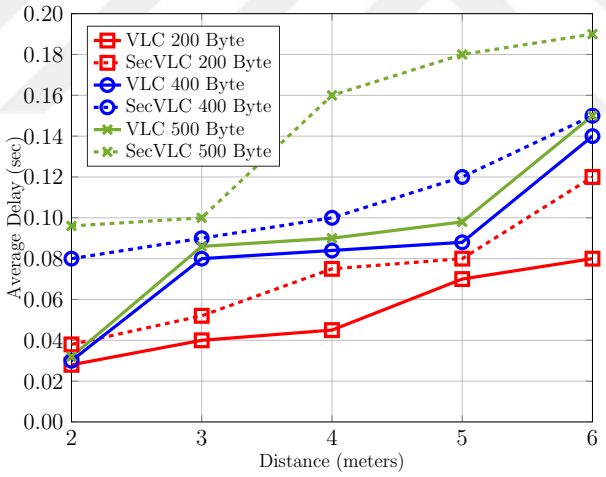


Figure 4.7: Average Delay Comparison

Fig. 4.7 shows the average delay performance of SecVLC protocol compared to VLC as a function of distance with varying data size. Compared to VLC, measured delay value for SecVLC contains key IR transmission, data encryption, data decryption and VLC data dissemination. Moreover, the effect of data size on average delay is analyzed by changing the data volume. As observed in Fig. 4.7, as the data size increases SecVLC necessitates lar-

ger time to encrypt and decrypt. Despite the average delay for SecVLC is higher than the VLC, it is acceptable provided that secure data transmission is enabled where only target vehicle can extract the data content. From this perspective, we can say that there is a trade-off between security and delay for VLC and SecVLC protocol: VLC provides lower delay than SecVLC whereas SecVLC achieves data security by encrypted communication.

4.7 Conclusion

In this study, we perform the first work to investigate data security in light based military ad hoc network and propose SecVLC protocol for securing communication. In SecVLC, we first use the VLC directionality property to ensure only target vehicles participate in the communication. Then, vehicles use full-duplex communication where IR is the outgoing link to share a secret key and VLC is an incoming link to receive encrypted vehicle data. We experimentally evaluate the suitability of SecVLC in outdoor scenarios by varying the inter-vehicular distance and data size with different metrics of interest including the security, data packet delivery ratio and delay.

Experimental evaluation of SecVLC protocol demonstrates its suitability for securing light based military communication. In the security analysis of SecVLC, we observe that despite VLC limits the data reception due to its directional transmission, it still possible to receive and decode the data packet if the adversary locates in light coverage. On the other hand, secret key enabled SecVLC prevents adversary vehicle decoding the data packet even it is received successfully. Moreover, the network performance analysis shows that DPDR value exhibits similar degradation patterns with the increasing distance for both SecVLC and VLC. RSS at large distance is not enough to successfully receive the data packet and it is the major factor that has an effect on the DPDR in SecVLC. On the other hand, delay value analysis shows that SecVLC requires extra time for data encryption and decryption. As the data packet size increases, delay value also increases.

In the future, we plan to extend SecVLC protocol by using VLC for both key and data transmission such that extra IR transceiver will not be required

by the protocol. We aim at determining the efficiency of SecVLC protocol in LoS scenarios and analyzing the performance of NLoS communication where the vehicle does not have a direct view of the rear vehicle bumper. We will also experimentally evaluate the SecVLC protocol at different light, temperature and humidity conditions for high-speed data communication with automotive LED lights.

Chapter 5

IEEE 802.11p and Visible Light Hybrid Communication based Secure Autonomous Platoon

5.1 Introduction

Autonomous vehicle platoons are expected to improve the safety, throughput, fuel economy and emission of transportation systems by combining the advantages of sensing the environment and making information available beyond driver's knowledge through communication. Autonomous vehicles have the capability of navigating without human input by identifying appropriate paths, obstacles and signage via a variety of sensor technologies such as radar, lidar, GPS. These vehicles have gained popularity since Google announced its self-driving car [2]. However, disconnected autonomous vehicles may not be fully reliable and effective in realistic environments with many dynamic variables. Therefore, autonomous vehicles need to incorporate vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication [1]. Autonomous vehicle platoon is a group of cooperative adaptive cruise control (CACC) vehicles kept in close proximity through wireless communication [3,4]. CACC is enhanced version of adaptive cruise control (ACC) system that not only maintains a proper following distance by slowing down once vehicles get too

close, but also allows vehicles to cooperate by communicating with each other and make a decision. Vehicle platoon improves traffic throughput since the cooperation among vehicles enhances their ability to plan ahead and drive closer than normal vehicles with small speed and distance variation [65]. Transportation safety is also enhanced through faster response to events than drivers. Furthermore, fuel consumption and emissions reduce by more stable movement on the road, decreasing unnecessary acceleration and deceleration.

Up to now, most of the previous studies have focused on the design of platoon management protocols, with the assumption that secure communication exists among vehicles [61,65–68]. A vehicle platoon consists of a platoon leader that controls the platoon and platoon followers that follow the leader via adjusting the speed. Platoon management protocols are based on single hop V2V based messaging with the goal of keeping platoon stable and supporting platooning maneuvers such as merge, split, entrance and leave. Platoon stability refers to ensuring platoon followers follow the platoon leader with minimal speed variation. Platooning maneuvers, on the other hand, rely on controlled exchange of messages among relevant neighboring vehicles to make autonomous driving decisions. However, none of these protocols considers the effect of security attacks on platoon stability and membership. [69] investigates the security vulnerabilities of platoon under message falsification and RF jamming attacks. Platoon systems usually adopt the current dominant vehicular RF technology, IEEE 802.11p, which forms the standard for Wireless Access for Vehicular Environments. Although high transmission range of IEEE 802.11p provides access to a larger number of vehicles at once, this wide coverage makes this communication technology vulnerable to adversaries blocking and interrupting the communication among the vehicles, leading to platoon instability.

Existing security solutions proposed for inter-vehicular communication mostly address general vehicular ad hoc networks and can be classified into three categories: digital signature approach, certification based security and cryptographic key distribution/management [46,70]. In digital signature approach, the sender generates a code by processing the message content with a signing algorithm that uses a private key. This code acts as a signature

and is appended to the packet. Upon reception of the packet, receiver runs the signature verification algorithm that uses a public key and accepts the packet only if the generated signature matches received signature. Digital signature approach guarantees the integrity of the sent packet, eliminating the interruption by non-authorized vehicles that do not have access to the key pairs [71]. Authorized vehicles may still perform attacks, which need to be detected and included in the certificate revocation list (CRL). CRL is broadcast periodically, consisting of the certificate of the vehicles that have been revoked from the system. However, as the number of revoked vehicles increases, the CRL requires a larger amount of storage and causes higher transmission delays, even if compression capable tamper-proof base stations or road side units are used [72–74]. This delay cannot be tolerated in vehicle platoons. Moreover, the CRL transmissions are prone to security attacks.

In certification based security, sender either generates a certificate by using public/private key pair or receives a certificate from a trusted authority and appends it to the packet [75]. Receiver then checks the validity of the certificate by communicating with a centralized entity in the public-key infrastructure (PKI), which consists of the set of hardware, software, policies and procedures to store, distribute and revoke the digital certificates. The packet is accepted only if approved by certificate authority (CA) in PKI. The usage of this scheme in vehicle platoons has the following drawbacks [76]. First, the communication with the centralized entity can create a single point of failure, making it open to several attacks. Secondly, the large communication overhead and delay associated with the certificate verification is not tolerable in time-critical vehicle platoons.

In cryptographic key distribution/management, vehicles use secret keys to secure the communication based on either asymmetric cryptography [77] or symmetric cryptography [78]. In asymmetric cryptography, sender and receiver agree upon a secret key using a key establishment protocol periodically. On the other hand, in symmetric cryptography, the secret keys are shared among two or more vehicles. These secret or shared keys are then used in the encryption and decryption of the message at the sender and receiver, respectively. Allowing access to the secret key by two or more vehicles

makes symmetric key encryption vulnerable to security attacks. As an alternative, asymmetric cryptography based solution has been recently proposed for group of vehicles in a platoon where the idea is based on the sharing of common secret key between platoon members via RF communication. But, the solution does not consider the platoon stability and the security of the platoon maneuvers [79]. However, the platoon stability and security of the platoon maneuvers are not considered. Moreover, the key distribution/management heavily depends on the availability of RF communication through which vehicles share data and secret key among each other. Today, PC-based or FPGA-based software platforms such as GNU Radio/USRP are easy to obtain and an adversary with these devices can easily block the RF communication, preventing the functionality of the proposed solution. In addition, packet collisions due to the congestion on the channel can interrupt both key dissemination and data transmission on the platoon. The interruption on the timely and reliable data transmission in vehicle platoon may lead to pileup, which is one of the most severe forms of traffic accidents. Some pilot studies have already been conducted to demonstrate the possibility of taking over the total control of autonomous vehicles by falsifying sensor data [80–83]. Developing security protocols considering all possible security attacks is essential for the large-scale deployment of vehicle platoons.

VLC is a recently proposed alternative communication technology that might be used in achieving a secure communication protocol in vehicle platoons by exploiting its distinguished propagation characteristics [7]. VLC uses modulated optical radiation in the visible light spectrum to carry digital information wirelessly. A VLC system usually uses a LED as the transmitting component and a photodiode or CMOS camera as the receiving component. LED has become very common in automotive lighting due to its long service life, high resistance to vibration, and better safety performance. Similarly, CMOS camera is already available in many vehicles as the front or rear camera for lane tracking and parking purposes. IEEE 802.15.7 task group has been formed to standardize the PHY and MAC layers for VLC [36]. The light directivity and impermeability of the optical signal through vehicles and obstacles provide more secure data communication than IEEE 802.11p

by limiting the transmission area. This limited transmission area restricts the availability of the data to the attackers, while still allowing communication in the platoon setting. Inter-vehicular space gap in platoon is less than 15 m at vehicle speeds less than 100 km/h [61]. On the the other hand, VLC communication range has been demonstrated to be 100 m for headlights and 30 m for taillights [40]. Moreover, the attackers need to direct strong light to saturate the receiver, which may not be feasible without the vehicle noticing the attack. Furthermore, pointing strong light to the receiver can only be performed on a few VLC links, as opposed to all vehicles within the communication range of IEEE 802.11p.

Previous studies on the VLC based vehicular communication have focused on the derivation of channel characteristics [19,22,40], requirements [8,10,25], advanced modulation schemes [84–86] and feasibility in a hybrid architecture together with IEEE 802.11p [41, 87, 88]. None of these studies address the security of vehicular communication using VLC. Only recently, we demonstrated the first security protocol for military vehicle platoon utilizing both VLC and infra-red (IR) [11]. Platoon vehicles use IR for secure sharing of the secret key and VLC to disseminate the encrypted data. The narrow half intensity angle of IR provides secure secret key sharing by limiting the reception to the target vehicle only. However, very narrow transmission angle also makes the communication reliability sensitive to vehicle dynamics such as maneuvers. Moreover, this solution requires extra IR hardware.

Only few studies focus on the security of VLC, but for non-vehicular scenarios [48, 49]. Physical layer security for indoor VLC is proposed by investigating the achievable secrecy rates of the Gaussian wiretap channel [48] . The differences in channel characteristics to multiple receivers are exploited to hide information from unauthorized receivers in a closed area. However, the requirement of the complete channel information for the execution of the algorithm makes it impossible to use in highly dynamic vehicular scenarios. On the other hand, physical security enhancement mechanisms for barcode-based VLC in smartphones are introduced in [49]. The screen view angles are manipulated and user-induced motions are leveraged to securely transfer barcode information through optical machine-readable patterns. However, the

requirement of near-field communication that is less than a meter and usage of angle modification in visual blockage on smartphones makes it infeasible to use for vehicular communication.

In this chapter, we propose an IEEE 802.11p and VLC based hybrid security protocol for vehicular platoon communication, namely SP-VLC, with the goal of ensuring platoon stability and enabling platoon maneuvers under data packet forgery, data packet replay, jamming and platoon maneuver attacks. The protocol employs VLC for both secret key and data exchange by exploiting the directivity and impermeability of visible light to provide resilience to security attacks. Utilizing only VLC in vehicle platoon, however, may degrade platoon stability since VLC is sensitive to environmental effects, i.e. fog, and might have short-term unreachability due to the increase in the inter-vehicle distance and/or loss of line-of-sight on a curvy road. Thus, IEEE 802.11p is also used in the encrypted platoon data transmission to provide redundancy for better reliability. The original contributions of the chapter are listed as follows:

- We propose an IEEE 802.11p and VLC based security protocol for autonomous vehicle platoons. The proposed protocol, SP-VLC, includes mechanisms for secret key establishment and periodic update using VLC to ensure the participation of only the target vehicle in communication; authentication using message authentication code to ensure the integrity of the packets; data transmission over both IEEE 802.11p and VLC incorporating the encryption and decryption of the packets using the secret key generated between consecutive platoon members in the vehicle platoon to exploit the complementary propagation characteristics of data transmission over these protocols; jamming detection and reaction to switch to VLC only communication based on packet reception characteristics; and secure platoon maneuvering based on the joint usage of IEEE 802.11p and VLC while exploiting the directionality, limited range and impermeability properties of VLC. All of these mechanisms have been combined for secure vehicle platoon communication for the first time in the literature.

- We classify the attack scenarios for vehicle platoons and provide a detailed analysis of the proposed SP-VLC protocol under these scenarios. In addition to commonly known attacks of data packet forgery, data packet replay and jamming, we define various forms of attacks specific to vehicular platoon management and manevuers, including generation of fake entrance request, fake entrance response, fake merge request, fake merge response packets, fake platoon leave and splitting packets, for the first time in the literature. We demonstrate the proper functionality of SP-VLC protocol under all these possible attack scenarios.

- We develop a simulation platform combining realistic vehicle mobility model, realistic VLC and IEEE 802.11p channel models and vehicle platoon management for the first time in the literature. The software implementation is available in [89].

- We evaluate the performance of SP-VLC protocol in comparison to previously proposed IEEE 802.11p and IEEE 802.11p-VLC hybrid protocols, under all possible security attacks over a wide range of vehicle platooning metrics, including speed and distance variation within the platoon, via extensive simulations, for the first time in the literature.

The rest of the chapter is organized as follows. Section 5.2 describes the communication model and derives all possible security attacks for autonomous vehicle platoon. Section 5.3 describes the attack scenarios for malicious actors. Section 5.4 presents the proposed SP-VLC protocol. Section 5.5 provides the security analysis of the SP-VLC protocol and considers various forms of attack scenarios. Section 5.6 provides the performance evaluation of SP-VLC in comparison to IEEE 802.11p and IEEE 802.11p-VLC hybrid protocols via extensive simulations. Finally, concluding remarks are given in Section 5.7.

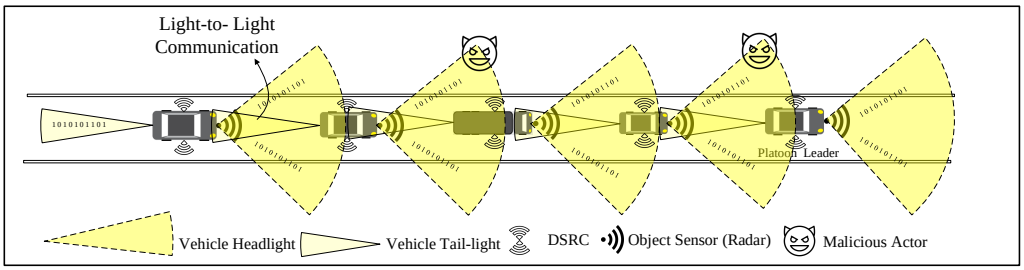


Figure 5.1: Hybrid autonomous platoon communication architecture.

5.2 System Model

5.2.1 Platoon Model

A vehicular platoon consists of a platoon leader that is the front vehicle in the platoon and one or more followers that follow the leader located on the leftmost lane, as shown in Fig. 5.1. Each vehicle in the platoon contains a specialized electronic controller unit (ECU) to implement platoon communication and management protocol and to keep the vehicle information base. ECU receives data from sensors, IEEE 802.11p and VLC receivers; and sends data to IEEE 802.11p and VLC transmitters. VLC transmitters and receivers are placed on both the front and the rear of the vehicle. VLC transmitters are connected to the headlights and taillights of the vehicle. The transmission characteristics of taillights and headlights are different, resulting in asymmetric communication link between consecutive vehicles. Multiple VLC receivers on the front and rear of the vehicle are assumed to enable the determination of the direction of transmission: The vehicle can determine whether the transmitting unit is on the road side, in the same lane or in the next lane by comparing the intensity of the received light at each receiver.

Platoon data communication should provide the features of timeliness, security and reliability in order to keep the platoon stable and support efficient platoon maneuver operations.Supported maneuver operations include entrance, leave, merge and split. The entrance and leave refer to joining to and exiting from the platoon, respectively. The merge operation stands for

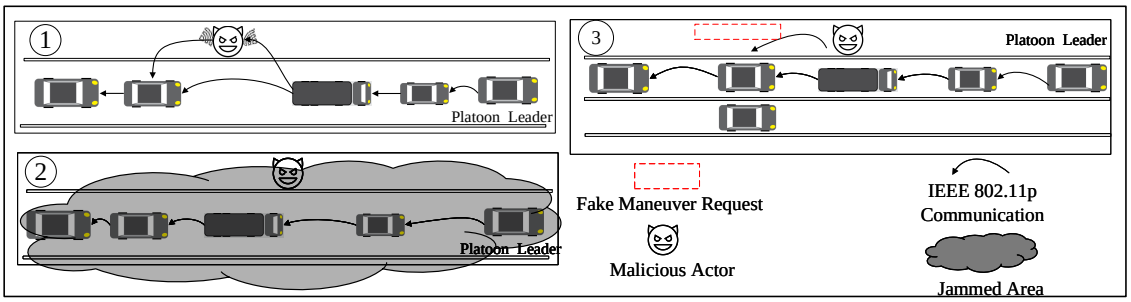


Figure 5.2: Illustration of platoon security attacks. 1) Data packet forgery and data packet replay attack 2) Jamming, 3) Platoon maneuver attack

combining two platoons that are traveling in the same lane. Separating a platoon into two smaller size platoons is defined as platoon splitting. Platoon members communicate with each other through periodic platoon data packets, maneuver request/response packets and membership view packets.

Platoon stability is achieved by the periodical exchange of platoon data packets. Platoon data packet is initiated by the platoon leader. The packet contains platoon identifier, platoon depth, lane identifier, sequence number, acceleration, speed, position, and sender address of the packet transmitter. Upon reception of the packet, platoon follower adjusts its own speed and distance to the preceding vehicle based on the speed and acceleration information of the vehicle itself and its preceding vehicle. The goal of this speed and distance adjustment is to keep a safe space gap to the vehicle in front. Vehicle then updates the sender address, speed and acceleration fields in the platoon data packet and sends it to the following vehicle.

Platoon leader coordinates all platoon maneuvers. Platoon maneuvers can happen at any point and only one maneuver is allowed at a time. Platoon followers need to inform platoon leader before performing any maneuver action. First, maneuver request packet is sent from the initiating to the destination vehicle, possibly in multiple hops. The initiating vehicle is the platoon member through which a new vehicle needs to enter the platoon in entrance maneuver, platoon member that needs to leave the platoon in leave maneuver, the platoon leader of the platoon that intends to merge with

another platoon in merging maneuver, and platoon leader in splitting maneuver. The destination vehicle is the platoon leader in entrance, leave and merging maneuvers, and the platoon member that needs to split the platoon in splitting maneuver. Maneuver request packet contains the maneuver identifier, the address of the initiating and destination vehicle. Upon reception of maneuver request packet, maneuver response packet is sent back to the initiating vehicle that contains the information for the suitability of the platoon maneuver. Following the completion of any maneuver and periodically, platoon members are updated with the membership view of the platoon by the dissemination of the membership view packet from platoon leader to all the platoon followers. Membership view packet contains the ordered sequence of vehicle identifiers in vehicle platoon.

A combination of sensors are used in conjunction with the communication among vehicles with the goal of determining the speed and distance to the preceding vehicle. Examples of sensors are speed sensor, radar and camera. Speed sensor measures the revolution per minute in the gearbox. Radar measures the distance to the preceding vehicle. Camera is used in line offsetting on lane tracking, and detection of objects and vehicles in front. Whenever the instantaneous space gap between vehicles is detected to be below the safe space threshold then platoon switches from CACC to ACC and actuates the brake and throttle to avoid the collision.

Vehicle information base (VIB) includes platoon depth; lane identifier; acceleration, speed and position of the vehicle itself and its preceding vehicle; membership view of the platoon; secret keys, sequence numbers and communication timing with the preceding and following vehicles; and maneuver requests. The platoon members update the VIB upon any change in the vehicle's own information or reception of a packet from any platoon member.

5.3 Vehicle Platoon Security Attack Categories

Malicious actors aim to destroy platoon stability and membership by replaying, modifying platoon packets and jamming platoon communication medium. Malicious actors are assumed to be roadside units or vehicles, not part of the platoon, which aim to destroy platoon stability without being affected from the consequences. They are equipped with both IEEE 802.11p and VLC devices. The behavior of the malicious actor is different for each type of platoon attack. The attack scenarios for malicious actors are illustrated in Fig. 5.2 and explained in detail next:

1. **Platoon Data Packet Forgery:** Malicious actor receives the platoon data packet, alters the content and rebroadcasts it as if the message comes from a platoon member. For instance, the malicious actor may modify the acceleration field in the platoon data packet from slowing down to speeding up. This might destroy platoon stability, possibly resulting in a collision.

2. **Platoon Data Packet Replay Attack:** Malicious actor overhears the packet transmitted over the platoon communication medium, stores and rebroadcasts it at a later time as if it is a new packet. Although the content of the platoon data packet is not modified, the outdated information may mislead the platoon members, possibly ruining the platoon stability.

3. **Platoon Jamming:** Malicious actor jams the platoon communication medium by using both IEEE 802.11p and VLC technologies. IEEE 802.11p and VLC jamming occur when adversary receives a platoon related information from vehicles via the IEEE 802.11p and VLC interfaces, respectively. During the jamming attack, the packets cannot be received successfully by the platoon members, endangering the stable operation of vehicle platoon.

4. **Platoon Maneuver Attack:** Malicious actor generates either a fake maneuver request packet or a fake maneuver response packet.

   (a) *Fake entrance request packet:* Malicious actor transmits a fake entrance request packet upon the detection of a vehicle in the lane next to the platoon, since platoon members do not process an entrance request unless they detect a vehicle that may request entrance to the platoon. Then the platoon leader sends a positive response, approving the entrance of the vehicle. Thus, two consecutive platoon members increase their inter-vehicular distance for the enabling entrance of the new vehicle. It takes some time until they realize that no vehicle actually intends to enter the platoon and close the gap again. However, this attack via fake entrance request packet decreases the efficiency of the platoon.

   (b) *Fake entrance response packet:* Malicious actor sends a fake negative entrance response packet, rejecting the entrance of a vehicle, upon receiving the entrance request from a vehicle in the lane next to the platoon. Meanwhile, the platoon leader accepts the entrance request and sends a positive entrance response packet, approving the entrance of the vehicle. However, the new vehicle ignores the following responses. Consequently, the two consecutive platoon members increasing their inter-vehicular distance for entrance but no vehicle enters the platoon. This degrades the traffic throughput.

   (c) *Fake leave request packet:* Malicious actor transmits a fake leave request packet and platoon leader sends a positive response approving the vehicle leaving the platoon. As a result, the corresponding platoon members increase their inter-vehicular distance for enabling the leave operation. When it is realized that the platoon member did not perform the leave operation, the inter-vehicular distance would be decreased. However, this attack via fake leave request packet would degrade the proper behavior of the platoon.

(d) *Fake leave response packet:* Malicious actor sends a fake negative leave response packet, rejecting the leaving of the vehicle, upon reception of the leave request packet from a platoon member. Negative leave response is generated if and only if the platoon leader is performing another manuver. Even though the platoon leader accepts the leave request and sends a positive leave response, the platoon members ignore following responses. This destroys the proper functioning of the leave operations in the platoon.

(e) *Fake merge request packet:* Upon the detection of two platoons, malicious actor transmits a fake merge request to the preceding platoon. The platoon leader of the preceding platoon sends a positive response and updates the membership view of its platoon by including the members of the following fake platoon. This will cause the platoon leader to make wrong decisions about the following platoon maneuvers. For instance, the platoon leader may reject the entrance request from new vehicles due to optimal platoon size limitation. This destroys the proper operation of the platoon.

(f) *Fake merge response packet:* Malicious actor may send a fake negative or positive merge response packet, upon reception of the merge request packet from a platoon. If malicious actor sends a fake negative merge response, the following platoon does not perform the merging operation while ignoring all the following responses. Meanwhile, the leader of the preceding platoon approves the merge operation, sends a positive response and updates the membership view of its platoon by including the members of the following platoon although the merging did not happen. On the other hand, if malicious actor sends a fake positive merge response while the leader of the preceding platoon sends a negative merge response afterwards, the following platoon decreases its distance to the preceding platoon without being part of the preceding platoon. These contradicting decisions and behaviours destroy the

proper operation of the platoon.

(g) *Fake split request packet:* Malicious actor sends a fake split request and the platoon member that needs to split the platoon sends a positive response, approving the split operation. The corresponding platoon member then increases the inter-vehicular distance to the preceding platoon member and becomes a platoon leader. It takes some time until the rear platoon leader realizes that two platoons can merge and decreases the inter-vehicular distance back to the safe gap value between platoon members. This degrades the platoon efficiency.

(h) *Fake split response packet:* Malicious actor sends a fake negative split response packet, rejecting the split operation, upon reception of the split request packet from the platoon leader. The following positive split response packet generated by the corresponding platoon member is ignored at the platoon leader. Consequently, although the split operation has actually happened, the platoon leader does not update the membership view of its platoon based on the negative response. These contradicting decisions and behaviours again degrades the proper operation of the platoon.

5.4 Secure Hybrid Platoon Communication and Platoon Management Protocol (SP-VLC)

The design goal of the secure platoon communication and management protocol is to keep the platoon stability and perform maneuver operations considering various attack types. SP-VLC is based on the usage of asymmetric cryptography for key establishment and symmetric cryptography for confidential communication between consecutive vehicles in the platoon and smart exchange of secret keys and data packets by combining the complementary propagation characteristics of VLC and IEEE 802.11p. The features of the

proposed secure hybrid communication protocol are as follows:

1. It provides a secret key establishment mechanism via VLC to construct the initial secret key securely. The initial secret key is needed for the communication between a vehicle that intends to enter the platoon and one of the platoon members, or a vehicle that has just entered the platoon and its preceding and succeeding vehicles. The usage of VLC in the secret key establishment provides resilience to jamming, fake entrance request and response attacks.

2. It provides a secret key update mechanism executed periodically using VLC to prevent attackers from decoding the secret key. Small distance between consecutive platoon members ensures VLC availability at all times. In the case of short term unreachability due to the increase in the inter-vehicle distance and loss of line-of-sight on a curvy road, the previous key is used without any update. The usage of VLC in the secret key update provides resilience to jamming attacks.

3. It provides an authentication mechanism using message authentication code (MAC). The authentication mechanism generates a code by encrypting the unique identifiers of vehicle and platoon, and packet sequence number with the secret key. The message authenticity ensures that the message has been sent by a platoon member and has been recently generated, preventing replay attacks.

4. It provides a data transmission mechanism over both IEEE 802.11p and VLC, incorporating the encryption and decryption of the packets using the secret key generated between each pair of consecutive platoon members in the vehicle platoon. This confidential transmission mechanism prevents the decryption of the packets by the attackers, avoiding data packet forgery. IEEE 802.11p is used to provide sufficient transmission coverage during the short-term unavailability of VLC, whereas VLC is used to provide successful data transmission even during jamming attacks.

5. It provides a jamming detection and reaction mechanism by interpreting packet reception statistics, and in case of jamming detection, switches to VLC-only communication for secure packet reception.

6. It provides secure platoon maneuver operations based on the joint usage of IEEE 802.11p and VLC while exploiting the directionality, limited range and impermeability properties of VLC and larger transmission range of IEEE 802.11p.

7. It provides confidential data transmission combining the light directional transmission and the mechanisms for secure secret key establishment and update to ensure that the data disseminated via VLC cannot be decoded by malicious actors even if they eavesdrop packets within the headlight or taillight coverage.

Next, we describe the detailed description of the mechanisms for secret key establishment, secret key update, data transmission, jamming detection and reaction, and platoon maneuver operations. The notation used in algorithms is given in Table 5.1.

5.4.1 Secret Key Establishment and Update Mechanism

Unified Diffie-Hellman (DH) is adopted in the secret key establishment and update mechanism. The initial secret key is needed for the communication between a vehicle that intends to enter the platoon and one of the platoon members, or a vehicle that has just entered the platoon and the preceding and following vehicles. DH secret keys have the potential to be recovered by the use of supercomputers within a limited amount of time [90, 91]. This necessitates the periodical update of the secret key between consecutive vehicle pairs in the platoon to prevent attackers from decoding the secret key, thus, packets [92]. Platoon members keep separate Key_{secret} for the following and preceding vehicle. This secret key is used in the encoding of the remaining packets. The secret key initiator and responder can be any platoon member. However, to prevent the contention in the secret key establishment, the rear

Table 5.1: Notation

Notation	Description
$Platoon_{id}$	Platoon Unique Identifier
Veh_{id}	Vehicle Unique Identifier
VIB	Vehicle Information Base
$Platoon_{data}$	Platoon Disseminated Data
Seq_{id}	Platoon Data Sequence Identifier
$Platoon_{size}$	Platoon Participated Vehicle Size
$Optimal_{size}$	Optimal Size of Platoon
$Membership_{view}$	Platoon Membership View Message
$Entrance_{req}$	Vehicle Entrance Request
$Entrance_{resp}$	Vehicle Entrance Response
$Merge_{req}$	Merge Request Message
$Merge_{resp}$	Merge Response Message
$Leave_{req}$	Leave Request Message
$Leave_{resp}$	Leave Response Message
$Split_{req}$	Split Request Message
$Split_{resp}$	Split Response Message
T_{key}	Key Usage Timer
$T_{session}$	Key Session Timer
Key_{secret}	Consecutive Platoon Member's Shared Key
$Session_{ack}$	Key Session Acknowledgement Packet

platoon member in a pair of consecutive vehicles is selected as the secret key initiator.

A pair of consecutive platoon members establishes a common Key_{secret} value without any explicit announcement to each other. The initiator and responder vehicles first choose the secret values a and b, respectively, that are both less than $p-1$, where p is a large prime number. The initiator and responder then compute $X = g^a mod(p)$ and $Y = g^b mod(p)$ by using secret a and b and common g and p values, respectively, where g is a primitive root modulo p, and send these values to each other. The same Key_{secret} is then computed by calculating $Y^a mod(p)$ and $X^b mod(p)$ at the initiator and responder, respectively, and stored in their VIB for future packet exchange. Since there may be packet losses over the wireless channel, session acknowledgement packet is transmitted following secret key initiation and response packets. Moreover, a mechanism for multiple transmissions of these packets are included to deal with packet losses.

The initiator vehicle executes Algorithm 1. This vehicle triggers the secret

Algorithm 1: Initiator Algorithm

```
1 Compute X = g^a mod(p);
2 Send X via VLC;
3 while Y is not received within T_session do
4 |   Send X via VLC;
5 while Y is received within T_session do
6 |   Compute Key_secret as Y^a mod(p);
7 |   Send Session_ack via VLC;
8 if Y is received then
9 |   Update Key_secret in VIB;
```

key establishment by sending secret key initiation packet. The value of X is computed and shared with the responder via VLC (Lines $1-2$). The initiator then waits for the secret key response packet, including the value of Y, from the responder. While Y value is not received within $T_{session}$, the initiator resends the secret key initiation packet to the responder (Lines $3-4$). If Y value is received from the responder then the initiator computes the Key_{secret} and sends $Session_{ack}$ packet to the responder via VLC. $Session_{ack}$ consists of the unique sequence identifier of the secret key session and is used to validate that both initiator and responder agree on the same Key_{secret}. It is possible that secret key response packet, thus Y, is received multiple times at the initiator. This happens when $Session_{ack}$ packet is not received by the responder successfully. Thus, the initiator vehicle is ready to receive multiple secret key response packets, in which case it retransmits $Session_{ack}$ (Lines $5-7$). Once the initiator makes sure that session acknowledgement packet is received successfully, it updates the VIB and uses the new Key_{secret} in the encoding of the following packets (Lines $8-9$).

The responder vehicle runs Algorithm 2. This vehicle triggers the secret key establishment upon reception of secret key initiation packet from the initiator (Line 1). The responder then computes the Key_{secret} and sends secret key response packet, including Y, to the initiator via VLC (Lines $2-4$). While the initiator's $Session_{ack}$ is not received within $T_{session}$, the responder resends the secret key response packet to the initiator (Lines $5-6$).

Algorithm 2: Responder Algorithm

```
1 if X is received then
2     Compute Key_secret as X^b mod(p);
3     Compute Y = g^b mod(p);
4     Send Y via VLC;
5     while Session_ack not received within T_session do
6         Send Y via VLC;
7     if Session_ack is received then
8         Update Key_secret in VIB;
```

If $Session_{ack}$ from the initiator is received then responder updates the VIB and uses new Key_{secret} in the encoding of the following packets (Lines $7-8$).

Key_{secret} is used for T_{key} time duration and regenerated in each period. If the vehicles cannot communicate via VLC then vehicles use the most recent Key_{secret} in VIB to encrypt and decrypt the data and maneuver packets. Whenever VLC is available between vehicles, the Key_{secret} update mechanism is triggered. During the Key_{secret} update, both initiator and responder use the same base g and p but renew the secret values a and b to ensure a new Key_{secret} is generated.

5.4.2 Message Authentication Mechanism

The authentication of the message is achieved via Cipher-based Message Authentication Code (CMAC). CMAC is a block cipher-based authentication algorithm, where both the integrity and authenticity of a message are verified. CMAC consists of three parts: identical key generation, signing and verification. In the key generation, CMAC adopts the secret key that is established with DH. In signing, a tag is generated by using the secret key, vehicle identifier, platoon identifier and packet sequence number, denoted by Veh_{id}, $Platoon_{id}$ and Seq_{id}, respectively. The tag is then appended to the packet. In verification step, the receiver verifies the authenticity of the packet in three steps:

1. The packet is given to decryption function with Key_{secret}. Decryption

function decodes the packet and returns the packet content if and only if the packet is encrypted with the current Key_{secret}. If Key_{secret} cannot decrypt the packet then the packet is rejected.

2. If the packet is decrypted, the receiver reproduces the tag by using the content of the received packet and current Key_{secret}. If reproduced and piggybacked tags are not identical then the packet is rejected.

3. The receiver compares the expected and received packet sequence numbers. If sequence numbers do not match, packet is rejected.

5.4.3 Data Transmission Mechanism

The exchange of vehicle platoon data packets between consecutive vehicle pairs in the platoon requires the insertion of CMAC and encryption by using Key_{secret} at the sender and decryption by using the same Key_{secret} and verification of CMAC at the receiver. Vehicle platoon data packet is generated by the platoon leader periodically and forwarded by all the platoon members to the following vehicle, resulting in multiple hop data dissemination.

Algorithm 3: Secure Data Transmission Mechanism

```
1  foreach received Platoon_data^encrypted do
2      Retrieve Key_secret from VIB;
3      Platoon_data=Decrypt(Platoon_data^encrypted, Key_secret);
4      if verify(Platoon_data, Key_secret) then
5          Update VIB based on Platoon_data;
6          Generate new Platoon_data based on VIB;
7          Retrieve Key_secret from VIB;
8          tag=sign(Platoon_data, Key_secret);
9          Platoon_data^encrypted=Encrypt(Platoon_data, tag, Key_secret);
10         Send Platoon_data^encrypted with VLC;
11         Send Platoon_data^encrypted via IEEE 802.11p;
```

Algorithm 3 is executed at each platoon member upon reception of an encrypted data packet from the preceding vehicle. The secure hybrid platoon communication is triggered upon reception of an encrypted $Platoon_{data}$,

denoted by $Platoon_{data}^{encrypted}$ (Line 1). The platoon member retrieves the Key_{secret} corresponding to the source of the received packet from VIB and decrypts the packet with this Key_{secret} (Line $2-3$). $Platoon_{data}$ is then authenticated by using the content of $Platoon_{data}$, including $Platoon_{id}$, Veh_{id} and Seq_{id}, and Key_{secret} through the verification step described in detail in Section 5.4.2 (Line 4). If the packet is authenticated then the vehicle updates its VIB based on the received $Platoon_{data}$ and generate new $Platoon_{data}$ for transmission to the following vehicle (Lines $5-6$). The new $Platoon_{data}$ is then signed and encrypted for transmission over both VLC and IEEE 802.11p (Lines $7-11$).

5.4.4 Jamming Detection and Reaction Mechanism

Platoon jamming attack is detected by a periodic check of the received messages from the preceding and following vehicles in the platoon. If no message is received by IEEE 802.11p for a certain amount of time then the vehicle decides that there is an RF jamming attack. The platoon then switches to the transmission of the packets by using VLC only. This continues until the vehicle senses the IEEE 802.11p channel idle again. In VLC jamming, on the other hand, attackers need to receive platoon related messages from vehicles to point a strong light towards the VLC receiver. Attackers do not turn the light source on until the platoon is ensured to be within the light coverage and consist of platoon followers rather than the single platoon leader. Secure platoon communication encrypts the message content and ensures confidential data transmission, which prevents platoon from such VLC jamming.

5.4.5 Platoon Maneuver Operations

5.4.5.1 Platoon Entrance

The secure entrance of a new vehicle into the platoon requires the establishment of an initial secret key of the new vehicle with the platoon members via VLC, encrypted forwarding of the entrance request packet to the platoon leader over multiple hops, and multi-hop transmission of encrypted entrance

response packet from platoon leader to the initiating vehicle by using both VLC and IEEE 802.11p. When a new vehicle intends to enter the platoon, the following steps are executed:

- A secret key initiation packet is sent to the platoon members via VLC. This enables the reception of the packet by the neighboring vehicles within VLC range only, while avoiding the reception by the malicious actors on the side of the road.

- The platoon members that receive the secret key initiation packet prior to entrance request over VLC check whether the source of the packet is a roadside unit or a vehicle traveling on the next lane. If the source is a vehicle on the next lane, these platoon members send a secret response packet. Otherwise, they ignore the packet.

- The vehicle waits until the reception of the first secret key response from a platoon member. Entrance request packet is then encrypted by the use of the key and sent to the corresponding platoon member via VLC.

- The platoon member that receives encrypted entrance request packet decrypts the packet and encrypts it with the secret key of the preceding vehicle in the platoon and sends it to that vehicle over both VLC and IEEE 802.11p.

- Upon reception of the encrypted entrance request packet, each platoon member decrypts the packet with the secret key of the following vehicle, encrypts the packet with the secret key of the preceding vehicle in the platoon and sends it over both VLC and IEEE 802.11p. This continues until the request reaches platoon leader.

- Upon reception of entrance request packet, the platoon leader generates and sends the entrance response packet by using encryption/decryption mechanism over both VLC and IEEE 802.11p in multiple hops.

- If entrance response is positive, entrance operation starts. The platoon members increases their inter-vehicular distance so that the new vehicle can steer to the platoon lane.

5.4.5.2 Platoon Leave

When a platoon member wants to leave the platoon, it sends leave request packet to the platoon leader. Upon reception of a platoon leave request, the platoon leader generates and sends platoon response packet to the initiating vehicle. If leave response is positive, the driver takes control of the corresponding vehicle in order to exit from platoon lane. Leave request and response packets are transmitted over multiple hops by using encryption/decryption mechanism over both VLC and IEEE 802.11p between consecutive vehicles in the platoon.

5.4.5.3 Platoon Merge

Merge operation is performed if the total size of two consecutive platoons traveling on the same lane is less than or equal to optimal platoon size. As long as the number of vehicles in a platoon is less than the optimal size, the platoon leader initiates a merge request to the preceding platoon periodically. In case of a positive merge response, the platoon leader of the following platoon decreases the space to the preceding platoon, becoming a member of the preceding platoon. Since the distance between these two platoons may be larger than VLC transmission range, it is possible that the merge request packet may only reach the preceding platoon members over IEEE 802.11p. Therefore, an additional merge justification stage following the merge process is included to ensure the secure communication over VLC. The following message exchanges are performed during the merging of two platoons:

- The platoon leader of the rear platoon sends a secret key initiation packet to the last vehicle of the preceding platoon over both VLC and IEEE 802.11p, since the range of VLC may not be large enough to reach any member of the preceding platoon.

- The vehicle waits for a certain time duration for the reception of secret key response packet from the last vehicle of the preceding platoon. If multiple secret key response packets are received, the platoon leader ignores them all. If there exists only one secret key response packet received over VLC, merge request packet is sent to the corresponding platoon member by using encryption mechanism via both VLC and IEEE 802.11p. Otherwise, merge request packet is sent to the source of secret key response packet over IEEE 802.11p only.

- The merge request packet is transmitted to the platoon leader of the preceding platoon over multiple hops by using encryption/decryption mechanism over both VLC and IEEE 802.11p.

- Upon reception of merge request packet, the platoon leader generates a merge response packet. The merge response is positive if the total number of vehicles in both platoons is less than or equal to optimal size, and negative otherwise. However, the platoon leader does not update platoon membership until it receives merge justification message.

- Merge response packet is transmitted to the platoon leader of the following platoon over multiple hops by using encryption/decryption mechanism over both VLC and IEEE 802.11p again.

- If merge response is positive, the platoon leader of the following platoon decreases the space to the preceding platoon, and sends a secret key update packet to the last vehicle of the preceding platoon via VLC. If the last vehicle of the preceding platoon determines that the source of the secret initiation packet travels on the same lane, it responds with a secret key response packet.

- If the secret key response packet is received from a vehicle traveling on the same lane, the platoon leader of the rear platoon sends merge verification message encrypted using the corresponding secret key to the last vehicle of the preceding platoon. This merge verification request is then transmitted to the platoon leader over multiple hops by using encryption/decryption mechanism over both VLC and IEEE 802.11p.

- The platoon leader updates the membership view of the platoon only after receiving merge verification request message and sends merge verification response packet in response. Merge verification response message is sent back over multiple hops by using encryption/decryption mechanism over both VLC and IEEE 802.11p.

- Upon reception of merge verification response packet, the platoon leader of the following platoon becomes a member of the preceding platoon together with all its members.

5.4.5.4 Platoon Split

Split operation refers to separating the platoon at a specific position to form two smaller platoons in the case when the platoon size is larger than optimal size and the leaving of a platoon member. The optimal platoon size depends on the road status. Thus, the leader may decide to split the platoon if the road allowed optimal size is less than the current platoon size. Moreover, when a platoon member is approaching its destination, it initiates a leave request. The leave maneuver is performed by a sequence of split and merge maneuvers. Similar to merge, the split operation is coordinated by platoon leader. The platoon leader sends a split request packet to the platoon member from which the split is initiated. The corresponding vehicle acknowledges the receipt of the split request packet by transmitting split response packet. The splitting platoon member then increases the distance to the preceding vehicle, forming a new platoon together with the following vehicles. These request and response packets are transmitted over multiple hops by using encryption/decryption mechanism over both VLC and IEEE 802.11p between consecutive vehicles in the platoon.

5.5 Security Analysis of SP-VLC

We now provide the mathematical model for the platoon stability incorporating vehicle longitudinal dynamics, information flow topology and decentralized feedback control law. We then prove the theorems on maintaining

the platoon stability under platoon data packet forgery, data packet replay, jamming and platoon maneuver attacks.

5.5.1 Theoretical Analysis of Platoon Stability

Platoon Dynamicity Model

The platoon is assumed to be homogeneous containing the same-type vehicles, e.g. only trucks or only passenger cars, with vehicle dynamics close to each other. The platoon leader is considered to have a constant speed $v_0(t) = v_0$. The platoon followers adjust their speed with the goal of tracking the speed of the leader vehicle and keeping a constant inter-vehicular space gap between any consecutive vehicles, such that

$$\begin{cases} p_{i-1}(t) - p_i(t) & = d_{i-1,i} \\ v_i(t) & = v_0(t) \end{cases} \tag{5.1}$$

for $i \in [1, N]$, where $i \in [1, N]$ refers to the i-th following vehicle and 0 refers to the platoon leader; $p_i(t)$ and $v_i(t)$ are the position and speed of vehicle i, respectively; $d_{i-1,i}$ is the desired space gap between vehicle $i-1$ and i. For platoon control, a 3rd-order state space model for vehicle i is given by [93,94]

$$x_i'(t) = Ax_i(t) + Bu_i(t) \tag{5.2}$$

where $x_i'(t)$ is the derivative of $x_i(t)$,

$$x_i(t) = \begin{bmatrix} p_i(t) \\ v_i(t) \\ a_i(t) \end{bmatrix}, A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -\frac{1}{\tau} \end{bmatrix}, \ B = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{\tau} \end{bmatrix},$$

$a_i(t)$ is the acceleration of vehicle i, $u_i(t)$ is the input signal, τ is the inertial delay of vehicle longitudinal dynamics. The input signal is determined via information flow among platoon members.

Platoon Information Flow Model

The information flow among platoon members determines the vehicle behaviour by providing the position, speed and acceleration of the neighboring vehicles as an input to the vehicle dynamics model [95–97]. The information flow among the platoon members is modelled by the use of a directed graph $G = (V, E)$, where $V = \{0, 1, ..., N\}$ and $(i, j) \in E$ if vehicle j has access to the platoon data of vehicle i. Adjacency matrix associated with graph G is defined as $M = [m_{ij}] \in \mathbb{R}^{(N+1)\times(N+1)}$ such that m_{ij} takes value 1 if $(i, j) \in E$ and 0 otherwise.

The feedback controller uses the neighborhood information specified by matrix M in a distributed way in each vehicle. The linear controller in the vehicle specifies input signal as

$$u_i(t) = -k^T \epsilon_i(t) \tag{5.3}$$

where $k = [k_1, k_2, k_3]$, k_i is the i-th control gain of the linear controller, T denotes the transpose of a vector,

$$\epsilon_i(t) = \sum_{j=0}^{N} m_{ji}(\widetilde{x}_i(t) - \widetilde{x}_j(t)), \tag{5.4}$$

$\widetilde{x}_i(t) = [\widetilde{p}_i(t), \widetilde{v}_i(t), \widetilde{a}_i(t)]$, $\widetilde{p}_i(t)$, $\widetilde{v}_i(t)$ and $\widetilde{a}_i(t)$ are the tracking errors in position, speed and acceleration, equal to $p_i(t) - p_0(t) + \sum_{j=0}^{i-1} d_{j,j+1}$, $v_i(t) - v_0$ and $a_i(t)$, respectively.

The closed loop dynamics of vehicle i is then given by

$$\widetilde{x}_i{}'(t) = A\widetilde{x}_i(t) - Bk^T \sum_{j=0}^{N} m_{ji}(\widetilde{x}_i(t) - \widetilde{x}_j(t)) \tag{5.5}$$

Platoon Stability Model

A platoon is stable if

$$\lim_{t\to\infty} \widetilde{x}_i(t) \leq C_0 \tag{5.6}$$

is satisfied for all $i \in [1, N]$, where C_0 is a constant bounded value [98, 99].

5.5.2 Analysis of SP-VLC

Theorem 1. *The stability of the platoon managed by the SP-VLC protocol is maintained under platoon data packet forgery, platoon data packet replay attack and platoon jamming.*

Proof. Eqn. 5.5 shows that the vehicle stability depends on two factors; vehicle dynamics (denoted by A and B) and the information flow among platoon members (denoted by matrix M). We prove the maintainability of the stability of the platoon managed by SP-VLC under security attacks by demonstrating that the malicious actor cannot destroy the information flow among the platoon members, i.e., matrix M.

- *Platoon Data Packet Forgery:* Malicious actor can only alter the content by decrypting the packet with the corresponding secret key. Secret key is established between consecutive vehicle pairs using DH mechanism. Even if malicious actor hears both secret key initiation and response packets over VLC, it cannot identify the secret key. Malicious actor may only decode the secret key based on a certain number of received data packets. This is avoided by ensuring key freshness through periodic update of the secret keys.

- *Platoon Data Packet Replay Attack:* Although the malicious actor cannot decrypt the packet, it can still store received packet and retransmit it at a later time. The signing of each packet with a tag by using secret key, vehicle identifier, platoon identifier and packet sequence number in CMAC allows the identification of replay attacks. The receiver does not authenticate the replayed packets due to either the update of secret key or unmatched sequence number. If the secret key is updated while the malicious actor is waiting to retransmit the packet, the tag reproduced by using the content of the received packet and current secret key does not match the piggybacked tag. If the secret key is not updated, the tags match. However, in that case, the sequence number of the received packet is outdated.

- *Platoon Jamming:* In the case of the detection of RF jamming attack through the disruption of received messages over IEEE 802.11p, the vehicle switches to the transmission of packets over VLC only. Since the secret key exchange is already performed over VLC, the operation of the platoon continues as usual. In the case of VLC jamming attack, malicious actor is assumed to point a strong light to the platoon member only when it receives a platoon data packet. However, due to encryption/decryption mechanism with periodically updated secret keys over VLC, the VLC attacker cannot decode platoon data packets.

□

Theorem 2. *The stability of the platoon managed by the SP-VLC protocol is maintained under platoon maneuver attacks.*

Proof. We prove the maintainability of the stability of the platoon managed by SP-VLC by demonstrating that the fake maneuver request and response packets injected by the malicious actor cannot deceive the receiving vehicles.

- *Fake platoon leave and splitting packets:* These packets are handled by the usage of already established secret keys between consecutive vehicle pairs. Malicious actor does not have access to the secret key since it is established by DH and kept fresh by periodic update.

- *Fake entrance request packet:* If a fake secret key establishment request packet prior to entrance request is generated via VLC, this can be detected by the receiving platoon member using the directionality of VLC. Malicious actor is assumed to be a transmitting unit on the side of the road, in contrast to the road where an entering vehicle would normally be traveling. The usage of multiple VLC receivers in the front and rear of the vehicle enables determining the direction of the transmitting unit. If the transmitting unit is located on the roadside, the secret key establishment is ignored, eliminating fake entrance request packet.

- *Fake entrance response packet:* When a vehicle sends secret key initiation request packet prior to entrance request via VLC, this cannot be

received by a roadside unit. This eliminates the generation of a fake secret key response prior to entrance request.

- *Fake merge request packet:* Upon reception of a fake merge request packet following secret key initiation and response packets transmitted by a malicious actor via IEEE 802.11p, the last vehicle of the platoon forwards it to the platoon leader. The platoon leader merge response is then sent back to the malicious actor. If the response is positive, the protocol requires the transmission of merge verification message encrypted using the secret key established between the malicious actor and the last vehicle in the platoon via VLC. However, malicious actor may not be in the VLC range of the last vehicle of the platoon. Even if the VLC communication is possible, the last vehicle can determine whether the malicious actor is on the roadside by detecting the direction of the transmitting unit. If the transmitting unit is located on the roadside, the secret key establishment prior to merge verification packet is ignored. Since merge verification packet is not received by the platoon leader, the platoon leader does not update the membership view of the platoon.

- *Fake merge response packet:* When the leader of the following platoon sends a secret initiation packet prior to merge request to the last vehicle of the preceding platoon via both IEEE 802.11p and VLC, malicious actor may respond in addition to that last vehicle. If multiple responses are received within a certain duration, the platoon leader ignores the response and tries again later.

□

5.6 Performance Evaluation

The goal of the simulations is to compare the performance of the proposed SP-VLC protocol to the previously proposed IEEE 802.11p based platoon management protocol [61], denoted by *IEEE 802.11p protocol*, and VLC

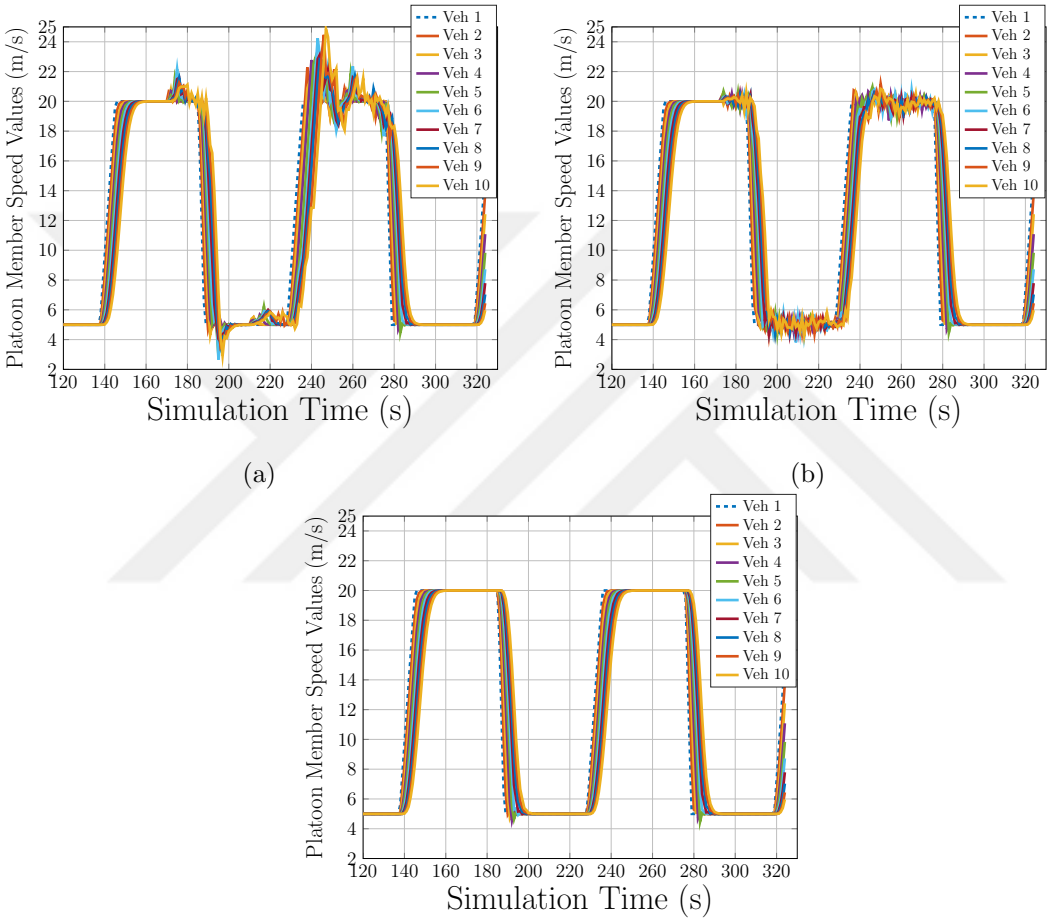


Figure 5.3: Data Forgery Attack on Platoon (a) IEEE 802.11p protocol (b) VLC-IEEE 802.11p protocol (c) SP-VLC

and IEEE 802.11p based hybrid platooning control, denoted by *VLC-IEEE 802.11p protocol* [87], in terms of platoon stability under data packet forgery, data packet replay, jamming and fake maneuver packet attacks. In IEEE 802.11p protocol, only IEEE 802.11p is used for the communication among vehicles. In VLC-IEEE 802.11p protocol, platoon members exchange messages with their preceding and following vehicles via sending the same packet synchronously over both IEEE 802.11p and VLC. No security protocol is used based on the assumption that malicious actors only use IEEE 802.11p protocol and frequency in their attacks. Platoon stability is quantified by the variation of speed and inter-vehicular distance over time.

The simulations are performed in VEhicular NeTwork Open Simulator (VENTOS) [64]. VENTOS is a simulator integrating realistic mobility generator, Simulation of Urban Mobility (SUMO) [100]; discrete packet-level simulator, OMNET++ [101]; and V2V communication platform, Vehicles in Network Simulation (Veins) [102]. SUMO is an open-source, space-continuous, and discrete-time traffic simulator that is capable of modeling the behavior of individual drivers. OMNET++ is component based library and framework and used for building the platoon data and platoon maneuvers that are simulated in VENTOS. The communication based on IEEE 802.11p protocol is adopted from the Veins, which is an open source framework to make vehicular network simulations. We have extended VENTOS by including VLC channel model, encryption/decryption and authentication mechanisms. VLC channel model adopts the received signal strength measurement results as a function of distance and bearing angle between two VLC capable vehicles in [40]. Encryption/decryption and authentication mechanism of SP-VLC adopts DH, which is provided from an open access cryptography library, Crypto++ [103]. Vehicles use secret 1024 bit values, a and b, in key agreement, having the form of safe primes specified in More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange [104] and periodically updated. Crypto++ is a library for cryptographic schemes including message authentication and key agreement.

The road topology consists of a two-lane road of length 90 km with the leftmost lane reserved for platooned vehicles. The vehicles are injected into

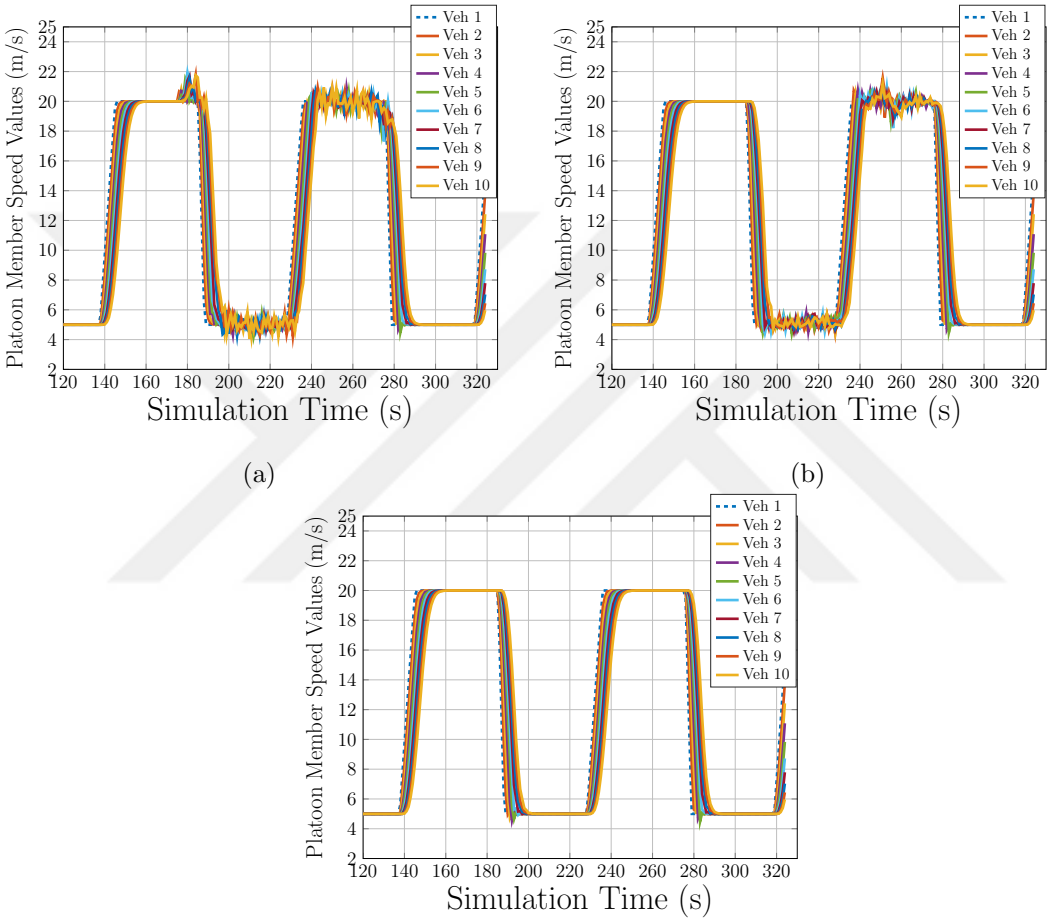


Figure 5.4: Data Replay Attack on Platoon (a) IEEE 802.11p protocol (b) VLC-IEEE 802.11p protocol (c) SP-VLC

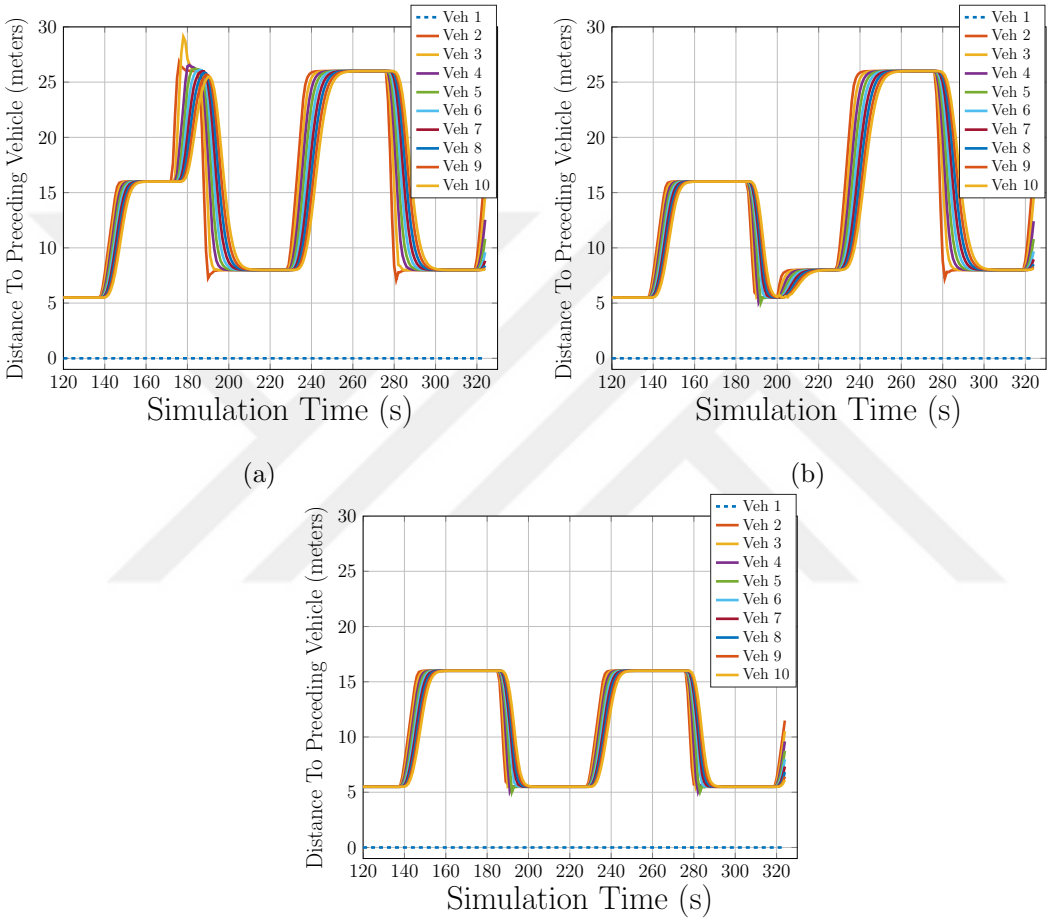


Figure 5.5: Jamming Attack on Platoon (a) IEEE 802.11p protocol (b) VLC-IEEE 802.11p protocol (c) SP-VLC

the road from the right lane according to Poisson process at 0.5 vehicles per second rate. CACC enabled vehicles move to the leftmost lane to form a platoon. A platoon consists of 10 autonomous vehicles. $Vehi$ refers to the i-th vehicle in the platoon, with $Veh1$ as the platoon leader. The mobility of the platoon leader depends on the road speed limit, that varies between 5 and 20 m/s. Platoon followers adjust their speed based on the platoon data exchanged via wireless communication with the goal of tracking the speed of the leader vehicle and keeping a constant inter-vehicular space gap. Two malicious actors are located on the road side with IEEE 802.11p transmission range of 1000 meters and VLC coverage of 100 meters. In the simulations, the platoon enters and leaves the IEEE 802.11p coverage of adversaries at $t = 172$ s and $t = 280$ s, respectively. Platoon is in both IEEE 802.11p and VLC coverage of malicious actors between $t = 200$ s and $t = 220$ s. Malicious actors attack the platoon by using both IEEE 802.11p and VLC. Table 5.2 lists simulation parameters.

Table 5.2: Simulation Parameters

	Parameter	Value
Simulation	Simulation Time	325 s
	Vehicle Length	5 m
	Number of Vehicles	20
	CACC Capable Vehicles	10
	IEEE 802.11p Range	300 m
	Communication Frequency	10 Hz
	$Platoon_{data}$ size	100 bytes
	$Membership_{view}$ size	100 bytes
	$Tkey$	5 s
	$Tsession$	2 s
VLC	Headlight Range	100 m
	Angular Headlight Range	-45° $\sim$ 45°
	Tail-light Range	30 m
	Angular Tail-light Range	-60° $\sim$ 60°
	Transmit Power	-60 dB
	Packet Sensitivity	-114 dB
CACC	Min Speed	5m/s
	Min Space Gap	2 m
	Max Speed	20 m/s
	Max Acceleration	3 m/s^2
	Max Deceleration	5 m/s^2
	$Optimal_{size}$	12

5.6.1 Platoon Data Packet Forgery Attack

Fig. 5.3 presents the speed profile of the platoon for IEEE 802.11p, VLC-IEEE 802.11p and SP-VLC protocols under data forgery attack. Malicious actors modify the acceleration field such that acceleration is converted to deceleration and vice versa. In IEEE 802.11p protocol, the speed value of platoon followers fluctuates around that of platoon leader by $[0, 5]$ m/s. VLC-IEEE 802.11p decreases this fluctuation to $[0, 2]$ m/s range for a much shorter time duration by exploiting the backup transmission over VLC. When the platoon is under IEEE 802.11p data forgery attack, VLC still allows to forward unmodified packets. However, when the platoon is within both IEEE 802.11p and VLC coverage of malicious actors (between $t = 200$ s and $t =220$ s), these actors can still receive and modify packets due to the lack of security protocol. The platoon members then use these forged packets in their CACC decision, resulting in speed fluctuations. The magnitude of the speed fluctuation in VLC-IEEE 802.11p protocol is less than that of the IEEE 802.11p protocol due to light directivity. The malicious actors can only attack a subset of the platoon members as opposed to all vehicles within the coverage of IEEE 802.11p. On the other hand, SP-VLC is robust to data replay attack without any fluctuation in platoon member speed values. As explained in detail in Section 5.5.2, malicious actors cannot modify the content of received platoon data packets since the secret keys used for the encryption of these packets are generated over VLC by using DH mechanism and kept fresh through a periodic update.

5.6.2 Platoon Data Packet Replay Attack

Fig. 5.4 shows the speed profile of the platoon for IEEE 802.11p, VLC-IEEE 802.11p and SP-VLC protocols under data replay attack. In data replay attack, malicious actors are assumed to eavesdrop the transmission of platoon data packets and replay them five seconds later as if newly generated, without the knowledge of any encryption mechanism. In IEEE 802.11p protocol, platoon stability is ruined with speed fluctuations within $[0, 2]$ m/s of that of platoon leader within the IEEE 802.11p coverage of the malicious

actor. Vehicles receive outdated packets from malicious actors and use for CACC decision, which degrades the platoon stability. In IEEE 802.11p-VLC protocol, the magnitude of fluctuations decreases to $[0, 1]$ m/s range for a shorter time duration within the VLC coverage. The data replay packets are resolved within IEEE 802.11p range due to the simultaneous transmission of the same data packets over VLC. The time duration of speed fluctuations under data replay attack is much shorter than that under data forgery attack, mainly because the vehicles that are close to leaving the VLC range of malicious actor do not receive the replayed data packet after five seconds. Finally, as explained in detail in Section 5.5.2, in SP-VLC, the authentication of the packets with secret key, vehicle identifier, platoon identifier and packet sequence number allows the identification of data replay attacks. Therefore, stability of vehicle platoon is kept in SP-VLC protocol.

5.6.3 Jamming Attack

Fig. 5.5 shows the space gap between consecutive platoon members for IEEE 802.11p, VLC-IEEE 802.11p and SP-VLC protocols under jamming attack. In IEEE 802.11p protocol, we observe that before the platoon enters the IEEE 802.11p transmission coverage of malicious actor, the space gap between consecutive platoon members is 16 meters when the platoon is traveling with 20 m/s. Since the platoon members cannot receive any packet during IEEE 802.11p jamming, at $t = 172$ s, CACC vehicles downgrade to ACC mode with larger space gap set to 26 meters. The platoon members then adjust their following distance according to the mobility of the platoon leader $Veh1$, with larger space gap than CACC vehicles. Furthermore, since ACC vehicles are controlled by on-board sensors, reactions to distance variation is slower than CACC vehicles. In IEEE 802.11p-VLC protocol, when the platoon is under IEEE 802.11p jamming attack, the platoon stability is maintained since VLC is used to forward platoon data without any interference. However, when vehicles enter the IEEE 802.11p and VLC coverage of malicious actors, all communication is blocked and vehicles downgrade to ACC mode decreasing their inter-vehicle distance. On the other hand, SP-VLC solves both IEEE

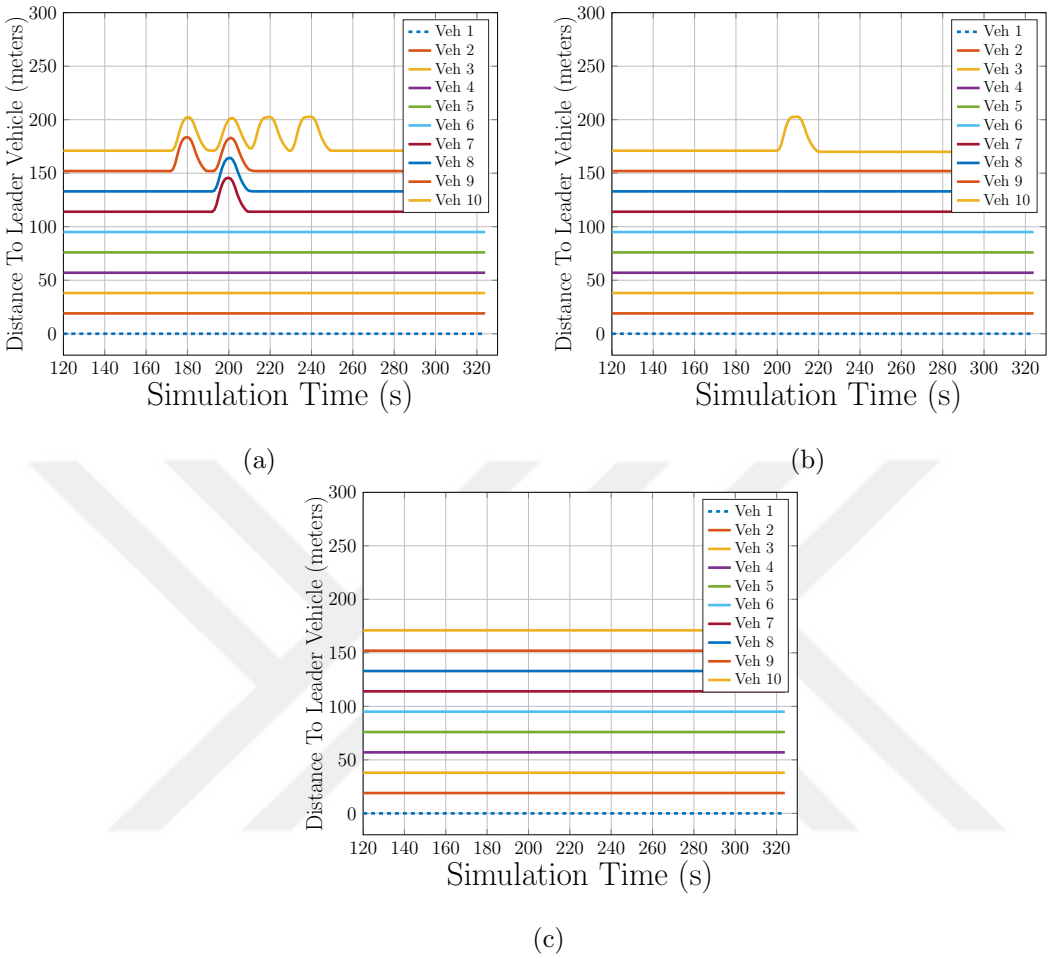


Figure 5.6: Fake Entrance Request Attack on Platoon (a) IEEE 802.11p protocol (b) VLC-IEEE 802.11p protocol (c) SP-VLC

802.11p and VLC jamming attacks. Since platoon data packets cannot be decrypted by the malicious actor, VLC communication cannot be jammed. The periodic secret key exchange and data exchange is performed securely over VLC.

5.6.4 Platoon Maneuver Attack

We have chosen the fake entrance request and fake split request as examples of platoon maneuver attacks, since they are representative of other maneuver attacks and their effect on the platoon efficiency is easier to visualize.

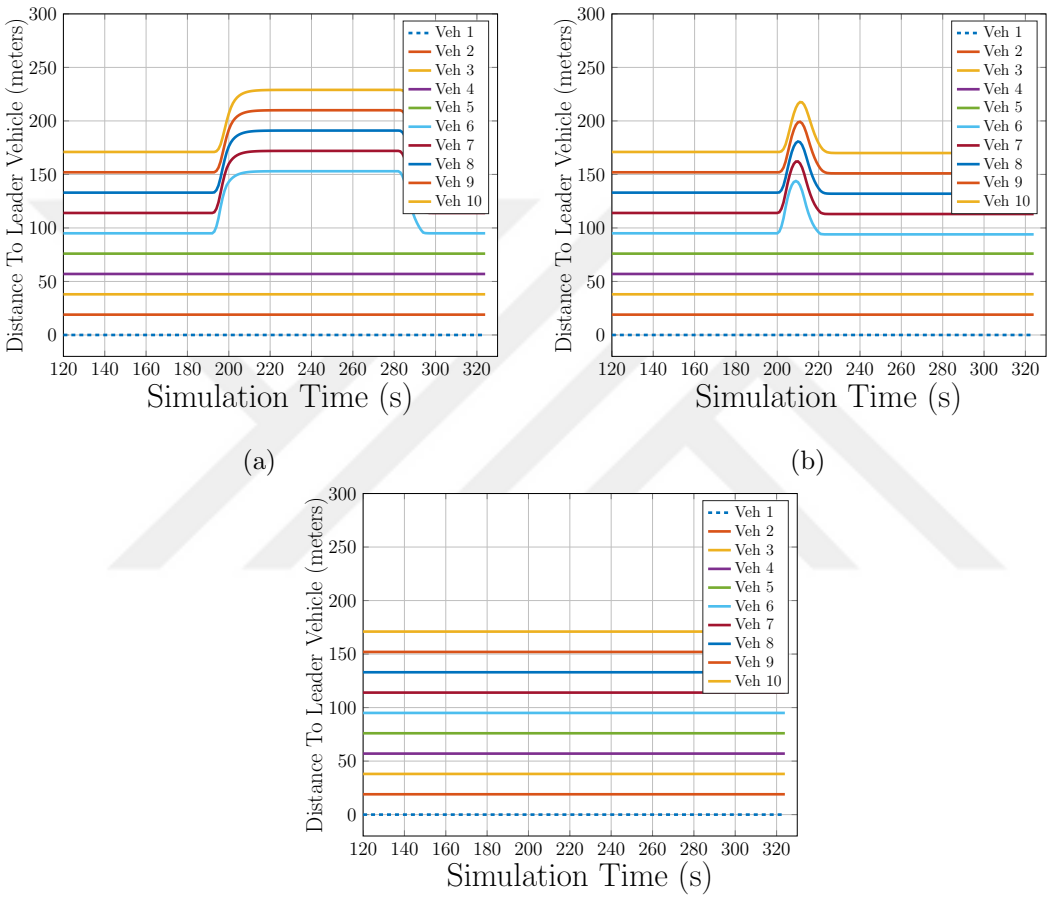


Figure 5.7: Fake Split Request Attack on Platoon (a) IEEE 802.11p protocol (b) VLC-IEEE 802.11p protocol (c) SP-VLC

5.6.4.1 Fake entrance request packet

Fig. 5.6 shows the distance to the platoon leader for IEEE 802.11p, VLC-IEEE 802.11p and SP-VLC under fake entrance request attack. Fake entrance request is generated by the malicious actor when there exists a vehicle in the right lane that may enter the platoon. In IEEE 802.11p, adversaries generate four fake entrance requests and platoon leader accepts these requests. Two consecutive platoon members then increase their inter-vehicular distance for the proper entrance of the new vehicle. It will take some time until they realize that no vehicle actually intends to enter the platoon and close the gap again. In IEEE 802.11p-VLC protocol, the number of fake entrance requests is less than that of the IEEE 802.11p. This is mainly because the malicious actors have limited VLC coverage and the entrance request is processed only if it is received by both IEEE 802.11p and VLC interfaces. On the other hand, the efficiency of the platoon managed by SP-VLC protocol is not affected by these fake entrance request attacks. As explained in detail in Section 5.5.2, the platoon member that receives the secret key establishment request prior entrance request determines the location of the transmitting unit on the roadside via the usage of the directionality of VLC. The secret key establishment is then ignored, eliminating the transmission of the following fake entrance request packet.

5.6.4.2 Fake split request packet

Fig. 5.7 shows the distance to the platoon leader for IEEE 802.11p, VLC-IEEE 802.11p and SP-VLC under fake split request attack. In IEEE 802.11p protocol, malicious actor generates a fake split request for $Veh6$ and platoon is split into two. Afterwards, the rear platoon leader periodically sends a merge request packet to the leader of the preceding platoon. However, as long as the second platoon is within the IEEE 802.11p coverage of the malicious actors, the merging does not happen since these actors send fake negative merge response each time. Only when the vehicles exit the IEEE 802.11p coverage of adversaries, two platoons are merged. In IEEE 802.11p-VLC protocol, the duration of the fake split request attack is shorter than that

of the IEEE 802.11p protocol, since the platoon member does not process the request unless it is received via both IEEE 802.11p and VLC interfaces. On the other hand, the stability of the platoon managed by the SP-VLC protocol is maintained under both IEEE 802.11p and VLC fake split request attacks. As explained in detail in Section 5.5.2, the split request packets are not processed at the platoon members unless they are encrypted by the use of the secret keys established and periodically updated by DH.

5.7 Conclusion

In this chapter, we propose an IEEE 802.11p and VLC based hybrid security protocol for platoon communication, namely SP-VLC, with the goal of ensuring platoon stability and enabling platoon maneuvers under data packet forgery, data packet replay, jamming and platoon maneuver attacks. We define various types of fake maneuver packet attack scenarios where a fake maneuver request packet or a fake maneuver response packet is transmitted by a malicious user on the side of the road.

We develop a simulation platform combining realistic vehicle mobility model, realistic VLC and IEEE 802.11p channel models, and vehicle platoon management. Extensive simulations demonstrate the superior performance of SP-VLC over previously proposed IEEE 802.11p and VLC-IEEE 802.11p hybrid protocols. We demonstrate the proper functioning of the proposed SP-VLC protocol under all possible security attacks by both providing a detailed analysis and performing extensive simulations. We show that IEEE 802.11p protocol based platoon management is highly vulnerable to data packet forgery, data packet replay, jamming attack and platoon maneuver attack. The speed value of the platoon followers fluctuates around that of platoon leader by $[0, 5]$ and $[0, 2]$m/s in data forgery and data replay attacks, respectively. All communication is blocked in jamming and vehicles downgrade to ACC with larger inter-vehicular space gap settings. Fake maneuver attacks degrade the platoon stability and decrease the platoon efficiency. VLC-IEEE 802.11p protocol based platoon, on the other hand, reduces the effect of adversaries due to the light directivity decreasing the coverage of

adversaries. However, adversaries can still ruin the platoon stability and degrade the traffic throughput when vehicles are in both IEEE 802.11p and VLC transmission range of malicious actors. In SP-VLC, vehicles are capable of communicating with each other via both VLC and IEEE 802.11p by exploiting the mechanisms for secret key establishment and periodic update via the usage of VLC to ensure the participation of only the target vehicle in communication; authentication with the usage of message authentication code to ensure the integrity of the packets; data transmission over both IEEE 802.11p and VLC incorporating the encryption and decryption of the packets using the secret key generated between consecutive platoon members in the vehicle platoon to exploit the complementary propagation characteristics of data transmission over these protocols; jamming detection and reaction to switch to VLC only communication based on packet reception characteristics; and secure platoon maneuvering based on the joint usage of IEEE 802.11p and VLC while exploiting the directionality, limited range and impermeability properties of VLC. SP-VLC achieves less than 0.1% difference in the speed and performs any maneuvers without interference from attackers.

Chapter 6

Visible Light Communication Assisted Safety Message Dissemination in Multiplatoon

6.1 Introduction

Advances in automobile industry bring the autonomous vehicle into the reality where vehicles cruise themselves via cooperative adaptive cruise control (CACC) system. CACC enables autonomous vehicles to access each others information based on vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication and groups them within close proximity called platoons [3]. The chain of platoons that follow one-another instead of organizing vehicles as one big platoon, on the other hand, refers to multiplatoon [5]. Multiplatoon is a promising vehicle formation technique with the potential of offering benefits in terms of traffic safety, throughput and homogeneity [6].

A primary objective for the multiplatoon system is to support data dissemination for different information types. Table 6.1 demonstrates the information dissemination applications discussed in [105]: update rate refers to the packet generation rate of vehicles, latency is the maximum tolerable end-to-end delay for the dissemination, distance is defined as the scope within which the information needs to be disseminated, dissemination refers to in-

Table 6.1: Requirements for Information Dissemination Applications in Multiplatoon

Type	Update Rate	Use Case	Latency	Distance	Dissemination
Status Monitoring	1 Hz	Road Condition, Vehicle Diagnostic	1 s	1000 m	Periodic, Broadcast
Vehicle Control	10 Hz	CACC	100 ms	-	Periodic, Multicast
Infotainment	0.01 Hz	News, Media, Advertisement	-	1000 m	Event-Based, Unicast
Safety / Warning	10 Hz	PCN, Emergency Brake / Lane Change	100 ms	1000 m	Event-Based, Broadcast

formation distribution characteristics that is either event based or periodic with communication modes: broadcast/multicast/unicast. Multiplatoon systems usually adopt the current dominant vehicular RF technology IEEE 802.11p for packet dissemination. However, IEEE 802.11p has many problems that may degrade the delay and delivery ratio of safety message applications [1]. First, IEEE 802.11p suffers from the scarcity of RF. The increasing wireless data traffic volume of rapidly growing wireless mobile devices causes pressure on RF spectrum. Second, congestion on the IEEE 802.11p channel may cause broadcast storm [106] which ruins the system performance. With the co-existence of different applications, vehicles attempt to transmit simultaneously. The contention based carrier sense multiple access scheme of IEEE 802.11p causes packet collisions at the medium access control layer that increase dramatically as the number of vehicles transmitting simultaneously increases. Third, IEEE 802.11p high transmission range makes this technology vulnerable to adversaries. Today, PC-based or FPGA-based software platforms such as GNU Radio/USRP are easy to obtain and an adversary with these devices can easily jam the IEEE 802.11p communication, preventing the proper functionality of safety message dissemination.

Up to now, most of the multiplatoon studies have focused on multiplatoon management based on the assumption that vehicles do not generate application level data traffic [61, 65, 67, 68, 107]. However, none of these works perform neither safety message dissemination scheme nor feasibility analysis of message delivery in the multiplatoon under the assumption of application level traffic with the goal of satisfying the safety application requirements.

Only one study [107] investigates the performance analysis of multiplatoon communication with the assumption of connected platoons and single information dissemination application. However, delivering safety information over a multiplatoon under application level traffic requires a protocol handling the safety application requirements in terms of latency and packet delivery ratio.

VLC is a relatively new communication technology that uses modulated optical radiation in the visible light spectrum to carry digital information. VLC brings several advantages of not causing any health concern nor any electromagnetic interference, being license-free and easy integration with the existing light emitting diode (LED) equipped vehicles with low cost additional onboard units. VLC is a promising complementary technology with the potential to address IEEE 802.11p problems [7]. First, VLC uses unlicensed and uncongested frequency band, which facilitate high throughput and low latency communication in a short range. VLC offers better scalability compared to RF based vehicular network, which experiences longer delay and lower packet rate due to congestion on the channel. Secondly, the directivity of the VLC limits the contention domain typically within the line-of-sight (LoS) vehicles, which lowers the packet collision and improves scalability in dense scenarios. Third, the directivity of the VLC transceivers facilitates secure communication where attackers need to direct strong light to jam the receiver which can only be performed on a single VLC link, as opposed to all vehicles in the communication range in the case of IEEE 802.11p.

Recently, many researchers investigate vehicular VLC for different purposes such as channel characteristics [19, 40], requirements [8, 10, 25] and security [11, 16]. Moreover, it has been demonstrated that inter-vehicular space gap in the platoon is less than 15 m at vehicle speeds less than 100 km/h [61] and VLC can achieve data transmission up to 100 m for headlights and 30 m for taillights [40]. Expanding on this vision, hybrid platooning architectures together with IEEE 802.11p and VLC are proposed [41, 87]. The large coverage of IEEE 802.11p and secure, high rate and low latency data transmission of VLC complement each other. Although message dissemination schemes for the vehicular network are viable, timely and reliable delivery

of safety messages in multiplatooned network is still challenging [108]. On the other hand, VLC has the potential to achieve the low latency and high packet delivery ratio in the platoon. Thus, we address the design of an IEEE 802.11p and VLC hybrid safety message dissemination protocol that ensures the requirements of safety applications.

The original contributions of this chapter is threefold. First, we propose an IEEE 802.11p and VLC hybrid safety message dissemination protocol. We develop a simulation platform supporting both IEEE 802.11p and VLC for the hybrid communication in the multiplatoon. Second, we perform an extensive analysis of the IEEE 802.11p and hybrid IEEE 802.11p-VLC based safety message dissemination in multiplatoon in the presence of application-level traffic, with different vehicle densities over a wide range of performance metrics including packet delivery ratio, delay and packet loss ratio. Third, we discuss the alternative ways to achieve the requirements of the safety application in multiplatoon.

The organization of the chapter is as follows. Section 6.2 shows the multiplatoon and safety application model. The details of IEEE 802.11p-VLC hybrid safety dissemination protocol are presented in Section 6.3, followed by the performance evaluation in Section 6.4. Finally, conclusions and future work are given in Section 6.5.

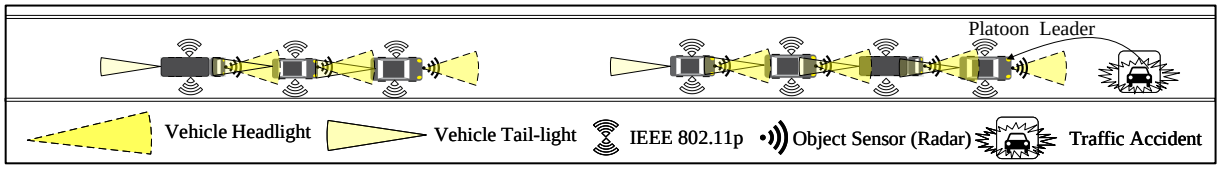


Figure 6.1: Hybrid multiplatoon communication architecture

6.2 System Model

A multiplatoon consists of a number of platoons where each consists of a platoon leader that is the front vehicle and one or more members that follow the leader, as shown in Fig. 6.1. Each vehicle in the platoon receives data from

sensors, IEEE 802.11p and VLC receivers; and sends data to IEEE 802.11p and VLC transmitters. VLC transmitters and receivers are placed on both the front and the rear of each vehicle. VLC transmitters are connected to the headlights and taillights of the vehicle. The transmission characteristics of taillights and headlights are different, resulting in an asymmetric communication link between consecutive vehicles.

Each platoon is controlled by a platoon management protocol that supports platoon maneuvers of entrance, leave, merge and split. Platoon members communicate with each other through periodic packets and event based maneuver request/response packets. Apart from platoon management protocol, vehicles run multiple applications such as status monitoring, vehicle control and warning. Platoon members use VLC and IEEE 802.11p for message dissemination. Sending messages to all members in a platoon via VLC is not possible due to directivity and other vehicles as obstacles. Thus, the data from leader to platoon is disseminated by the headlight and taillight in a multi-hop manner through VLC. Vehicle keeps information of its neighboring vehicles in Vehicle Information Base (VIB), which includes maneuver requests/responses, application messages and last communication time.

As an example of safety message dissemination, Post-Crash Notification (PCN) application is utilized. PCN is a safety application where vehicles in an accident area send out PCN alert. The PCN alert contains the position of the crashed vehicle, heading, speed limit, vehicle status and it requires high packet delivery ratio with the short amount of delay in order to prevent the possible pileup in a platoon. The platoon, which receives the PCN alert, informs the other platoons by periodically broadcasting the alert until it exits from the range of accident location.

6.3 VLC-Assisted Safety Message Forwarding

To achieve hard delay and a high packet delivery ratio constraints, we consider the hybrid usage of VLC and IEE 802.11p. The unique features of

VLC assisted safety message forwarding are; it utilizes full duplex light-to-light communication for intra-platoon V2V communication to improve the delay and reliability performance of transmission, it performs smart forwarding where vehicles adaptively decide to forward the received message via the IEEE 802.11p or VLC.

Algorithm 4 is executed by each vehicle in multiplatoon for safety message dissemination, where the aim is to reduce the delay and increase the packet delivery ratio of the safety messages from the leader to the other vehicles by using both IEEE 802.11p and VLC.

Algorithm 4: Hybrid Dissemination Protocol

```
1  foreach received PCN packet do
2      Check the VIB;
3      if PCN not received before then
4          if packet is received by VLC then
5              Send PCN only via VLC;
6          else
7              Send PCN via IEEE 802.11p/VLC;
8          Update VIB;
9          if tail vehicle of a platoon then
10             Broadcast PCN;
```

When a vehicle receives a PCN packet, it checks the VIB to control if PCN was received before (Line 2). If not, then the vehicle checks if PCN is received the by VLC (Line 4). If the vehicle receives the PCN via VLC earlier than IEEE 802.11p, it sends the PCN only via the VLC to the following vehicle(Line 5). The case of a PCN packet received via VLC earlier than IEEE 802.11p implies that the channel is congested and vehicles have failed to receive the PCN via RF. Thus, the PCN is forwarded only via the VLC for the purpose not to further congest the radio link. On the other hand, if PCN is received via IEEE 802.11p first, the assumption is that RF channel is not severely congested, then the vehicle sends the PCN via both IEEE 802.11p and VLC (Line 7). After forwarding the PCN, the VIB is updated (Line 8). When the PCN reaches to the tail vehicle in each platoon,

the last vehicle of each platoon broadcast the PCN for following platoons (Line $9-10$).

6.4 Performance Evaluation

For the performance evaluation of safety message dissemination in multiplatoon, we compare the proposed VLC-IEEE 802.11p hybrid safety message dissemination scheme denoted by *VLC-IEEE 802.11p Hybrid* to the IEEE 802.11p based flooding, denoted by *IEEE 802.11p Flooding* and previously proposed multi-hop IEEE 802.11p based multiplatoon communication, denoted by *IEEE 802.11p Backbone* [107], in terms of packet delivery ratio, delay and packet loss ratio. In *IEEE 802.11p Backbone*, safety message is broadcast by only the leader and the tail vehicles in each platoon. Vehicles in multiplatoon are controlled via IEEE 802.11p based platoon management protocol [61]. Apart from platoon management, vehicles generate application level data traffic via services such as cooperative awareness, status monitoring, vehicle control and vehicle warning with broadcast communication mode and period of 0.1 seconds.

We use VEhicular NETwork Open Simulator (VENTOS) [64] for performance evaluation of various multiplatoon scenarios. VENTOS is an integrated simulator containing the; the realistic mobility generator, Simulation of Urban Mobility (SUMO) [100], discrete packet-level simulator, OMNET++ [101] and vehicular communication platform Vehicles in Network Simulation (Veins) [102]. VENTOS provides a platform to perform multiplatoon simulation under different vehicle mobility where platoons utilize the CACC. We have extended the VENTOS by including the previously developed VLC channel model [40], where the VLC channel model adopts the received signal strength that is a function of distance and bearing angle between vehicles. The end-to-end transmission delay is computed as the sum of the ratio of packet size to VLC achievable data rate at each hop of VLC transmission [7].

The simulation scenario consists of a two-lane road with the leftmost lane reserved for multiplatoon. Vehicles enter the road from the right lane

with Poisson distribution and an average of one vehicle every two seconds rate. After vehicle injection, vehicles change lane to the leftmost to be part of the multiplatoon network. The leader vehicles in multiplatoon have the mobility that speeds up and slows down based on the road conditions where the minimum and maximum speed values are 5 and 20 m/s, respectively. For each scenario, three accident events are simulated in the right lane. When multiplatoon enters the coverage of PCN, it is delivered to multiplatoon based on the proposed safety message dissemination scheme. Table 6.2 lists simulation parameters.

Table 6.2: Parameters

	Parameter	Value
Simulation	Simulation Time	250 s
	Vehicle Length	5 m
	PCN size	100 bytes
	Number of Vehicles	50
	IEEE 802.11p Range	300 m
VLC	Headlight / Tail-light Range	100 m / 30 m
	Angular Headlight Range	-45° $\sim$ 45°
	Angular Tail-light Range	-60° $\sim$ 60°
	Transmit Power	-60 dB
	Packet Sensitivity	-114 dB
CACC	Min./Max. Speed	5 m/s / 20 m/s
	Max. Acceleration / Deceleration	3 m/s^2 / 5 m/s^2
	Min. Space Gap	2 m
	Platoon Size (numbers of vehicle)	5, 8, 10, 15, 20

6.4.1 Packet Delivery Ratio

Packet delivery ratio (PDR) is defined as the ratio of the number of vehicles successfully receiving PCN packet to the total number of vehicles within the target geographical area for dissemination of PCN.

Fig. 6.2 shows the PDR performance of different PCN dissemination schemes on multiplatoon as a function of platoon size. PDR has a tendency to decrease as the platoon size increases. Application level traffic causes medium contention on IEEE 802.11p and it increases the packet collision probability in *IEEE 802.11p Flooding* and *IEEE 802.11p Backbone*.

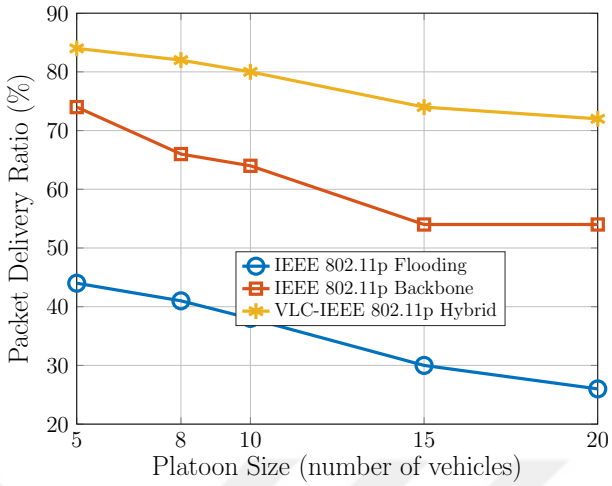


Figure 6.2: PDR of different data dissemination schemes

The PDR of *VLC-IEEE 802.11p Hybrid*, on the other hand, outperforms all the other dissemination schemes in all cases. The reason for the superior performance of VLC and IEEE 802.11p hybrid dissemination over the other schemes is the usage of VLC in intra-platoon data dissemination. VLC links cause limited or no inter-network interference and do not get affected by the channel congestion caused by application level traffic on IEEE 802.11p. However, as the platoon size increases, multiplatoon gets disconnected. Although the set of tail vehicles broadcast the PCN, it is not delivered to following platoons due to the limited transmission range of IEEE 802.11p.

6.4.2 Packet Loss Ratio

Packet loss ratio (PLR) refers to the ratio of the number of lost safety messages to the total number of safety messages subject to different volumes of background application data traffic. Application level data traffic is generated by each vehicle within the target geographical area for dissemination of PCN.

Fig. 6.3 shows the average PLR of the vehicles selected randomly within the target geographical area of PCN. As the application level traffic increases, PLR has a tendency to increase. Broadcast nature of *IEEE 802.11p Flooding* causes high PLR compared to *IEEE 802.11p Backbone* and *VLC-IEEE*

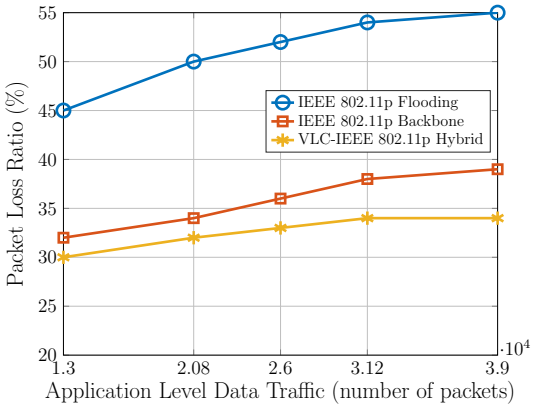


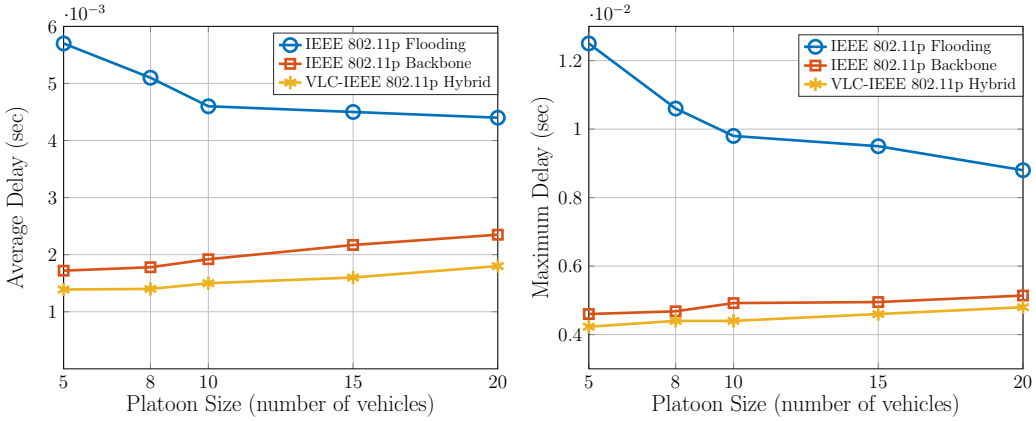
Figure 6.3: PLR of different data dissemination schemes

802.11p Hybrid schemes. Less number of PCN broadcasting in *IEEE 802.11p Backbone* decreases the PLR. PLR of *VLC-IEEE 802.11p Hybrid*, on the other hand, is below all the other dissemination schemes in all cases. Likewise, the main reason behind this is the utilization of VLC for safety message dissemination in multiplatoon. The directionality of light is beneficial in the vehicular VLC since the only small number of vehicles that are in direct LoS are in the same contention domain. When we consider this result together with Fig. 6.2, we observe that usage of VLC significantly increases the PDR and decreases the PLR compared to pure IEEE 802.11p based schemes.

6.4.3 Delay

The delay metric is defined as the time duration that the PCN travels from the source to the vehicles within the target geographical area of dissemination. The average is taken over all vehicles that successfully receive the PCN. The maximum delay, on the other hand, refers to the maximum latency of each PCN packet transmitted from the source to the vehicles within the target geographical area of PCN.

Fig. 6.4 shows the average and maximum delay of different PCN dissemination schemes as a function of platoon size. When these results are considered together with the PDR results of Fig. 6.2, we observe that there exists a trade-off between PDR and delay in terms of platoon size for *IEEE*



(a) (b)

Figure 6.4: PCN Delay Comparison (a) Average Delay (b) Maximum Delay

802.11p Flooding. As the platoon size increases the latency for PCN dissemination decreases whereas the *IEEE 802.11p Flooding* results in lower PDR.

In *IEEE 802.11p Backbone* and *VLC-IEEE 802.11p Hybrid*, on the other hand, as the platoon size increases, the delay has tendency to increase. As platoon size increases, the number of PCN transmission also increases in both *IEEE 802.11p Backbone* and *VLC-IEEE 802.11p Hybrid* to reach the set of tail vehicles. The delay of *VLC-IEEE 802.11p Hybrid*, on the other hand, is lower than the delay measured for all the other dissemination schemes in all cases. When we consider these results together with PLR results reported in Fig. 6.3, we can conclude that usage of VLC results in improved scalability in scenarios with high vehicle density where the IEEE 802.11p suffers from longer delays and higher PLR.

6.5 Conclusion and Future Work

In this chapter we proposed a VLC-IEEE 802.11p based safety message dissemination scheme and investigated the safety message dissemination schemes of pure IEEE 802.11p and hybrid VLC-IEEE 802.11p based multiplatoon for varying platoon sizes. We developed a simulation platform to model and

evaluate the hybrid communication in multiplatoon. We show that IEEE 802.11p based multiplatoon safety message dissemination suffers from less PDR, longer delay and high PLR. Usage of VLC, on the other hand, significantly improves the performance that lowers the PLR and increases the scalability of safety message dissemination.

Future work would concentrate on designing a VLC-IEEE 802.11p hybrid safety message dissemination protocol for multiplatoon robust to the disconnected network. Such a protocol requires VLC communication for V2V to improve delay and reliability of safety message dissemination in high vehicle density, utilizing multi-metric mobile gateway selection for V2I communication when IEEE 802.11p gets disconnected and adopting a service migration scheme between gateways when the serving gateway loses its efficiency.

Chapter 7

Conclusion

In this thesis, we investigate the hybrid usage of DSRC and VLC in autonomous platoon/multiplatoon with the goal of achieving secure and efficient communication architecture. We first experimentally analyze the VLC usage in different vehicular scenarios including single and dual channel data transmission considering various light dimming level and the bearing angle of values with the goal of determining the usage limitation of VLC in vehicular environment. We demonstrate that state of the art Lambertian radiation pattern does not represent the automotive light emitting diode (LED) radiation pattern accurately. Dual channel usage increases the angular limitation by up to 10° compared to the single channel VLC. We show that dimming is a key parameter in VLC, which affects data dissemination and received power signal strength. Second, we propose a light communication protocol, namely SecVLC to secure vehicular military visible light communication where directionality of light is used with a key exchange mechanism to ensure only the participating vehicles understand the contents of the messages. We experimentally evaluate the performance of SecVLC in the vehicular environment with a malicious insider to ensure fully reliable communication. We demonstrate that despite VLC limits the data reception due to its directional transmission, it still possible to receive and decode the data packet if the adversary locates in light coverage. On the other hand, secret key enabled SecVLC prevents adversary packet reception and achieves confidential data transmission

with short delay and high rate of packet delivery. Third, we propose a DSRC and VLC based hybrid security protocol for platoon communication, namely SP-VLC with the goal of ensuring platoon stability and enabling platoon maneuvers under different attacks from adversaries. We develop a simulation platform combining realistic vehicle mobility model, realistic VLC and DSRC channel models and vehicle platoon management for the first time in the literature. We show that DSRC based platoon management is highly vulnerable to attacks from adversaries. VLC reduces the effect of adversaries due to the light directivity decreasing the coverage of adversaries. However, adversaries can still ruin the platoon stability degrade the traffic throughput when vehicles are in both DSRC and VLC transmission range of malicious actors. SP-VLC, on the other hand, includes mechanisms for secret key initiation and periodic update via the usage of VLC to ensure the participation of only the target vehicle in communication; authentication with the usage of message authentication code to ensure the integrity of the packets; data transmission over both DSRC and VLC incorporating the encryption and decryption of the packets using the secret key generated between consecutive platoon members in the vehicle platoon to exploit the complementary propagation characteristics of data transmission over these protocols; jamming detection and reaction to switch to VLC only communication based on packet reception characteristics; and secure platoon maneuvering based on the joint usage of DSRC and VLC while exploiting the directionality, limited range and impermeability properties of VLC and achieves less than 0.1% difference in the speed and performs any maneuvers without interference from attackers. Fourth, we propose a DSRC and VLC based safety message dissemination protocol to satisfy the hard delay and high packet delivery ratio constraints of the safety application under application level data traffic. Vehicles utilize VLC for safety message dissemination within the platoon when the multiplatoon has high vehicle density leading to high medium contention. DSRC is adopted for platoon based data dissemination when VLC is disconnected within the dissemination distance. We demonstrate that the proposed hybrid protocol improves both packet delivery ratio and delay by limiting the contention to the line-of-sight vehicles.

We believe that our studies on autonomous platoon/multiplatoon are very promising for the next generation automotive revolution, autonomous vehicular system. In this thesis, we have provided detailed research findings from the emerging problems that are security and efficiency in autonomous vehicular platoon/multiplatoon communication. We believe that there are still open issues that need to be addressed before the practical usage of the platoon.

First, the realistic modeling of vehicular VLC can still be improved. In this thesis, we have developed a VLC channel model that adopts the received signal strength measurement results as a function of distance and bearing angle between two VLC capable vehicles where headlight and taillight are used. The channel model can be further enhanced by including the environmental effects, i.e. fog, the impact of the reflection from road, vehicles and other obstacles and the effect of curvy road, which may cause loss of line-of-sight during light communication. The realistic VLC channel model would improve the simulation realism and would give us an idea of the limitation of VLC in the vehicular environment.

Second, the platoon security can still be enhanced. We model the adversary as the road side units or vehicles, not part of the platoon, which aims to destroy the platoon stability without being affected from the consequences. We propose a cryptographic solution to ensure secure communication. However, the cryptographic security does not work in the case where the adversary is an insider, it is a trusted platoon member. The case where the adversary is a platoon member, on the other hand, necessitates misbehavior/anomaly detection schemes which require multiple sources of data and a voting procedure among platoon members. Misbehavior/anomaly detection schemes would further improve the platoon security.

Third, hybrid DSRC and VLC based safety message dissemination can still be further investigated over a scalable multiplatoon scenarios. We demonstrate that VLC significantly improves the performance and scalability of safety message dissemination. However, hybrid DSRC and VLC based dissemination scheme still suffers from the disconnected network. Disconnected autonomous platoon, on the other hand, may not be fully reliable and ef-

fective in realistic environments with many dynamic variables. From this perspective, a safety message dissemination protocol needs to utilize a multi-metric mobile gateway selection for vehicle-to-infrastructure communication when DSRC gets disconnected and it needs to adopt a service migration scheme between gateways when the serving gateway loses its optimality. Such an improved safety dissemination protocol would increase the scalability of safety message dissemination over the multiplatoon.

In the future, we plan to concentrate on the open problems and incorporate our findings and solution approaches in practical deployment of autonomous platoon/multiplatoon communication to be part of the effort on achieving secure and efficient communication architecture for the autonomous system.

References

[1] S. Ucar, S. C. Ergen, and O. Ozkasap, "Multihop-Cluster-Based IEEE 802.11p and LTE Hybrid Architecture for VANET Safety Message Dissemination," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 4, pp. 2621–2636, April 2016.

[2] Google Blog, @ONLINE. [Online]. Available: https://goo.gl/hWU0V0

[3] J. Ploeg, E. Semsar-Kazerooni, G. Lijster, N. van de Wouw, and H. Nijmeijer, "Graceful Degradation of Cooperative Adaptive Cruise Control," *IEEE Transactions on Intelligent Transportation Systems*, Feb 2015.

[4] X.-Y. L. Steven Shladover, Dongyan Su, "Impacts of cooperative adaptive cruise control on freeway traffic flow," *Transportation Research Record: Journal of the Transportation Research Board*, 2013.

[5] P. Fernandes and U. Nunes, "Multiplatooning Leaders Positioning and Cooperative Behavior Algorithms of Communicant Automated Vehicles for High Traffic Capacity," *IEEE Transactions on Intelligent Transportation Systems*, June 2015.

[6] D. Jia, K. Lu, and J. Wang, "A disturbance-adaptive design for vanet-enabled vehicle platoon," *IEEE Transactions on Vehicular Technology*, 2014.

[7] 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*, Dec 2015.

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

[9] S. Ucar, S. C. Ergen, and O. Ozkasap, "Visible light communication in vehicular ad-hoc networks," in *24th Signal Processing and Communication Application Conference (SIU)*, May 2016, pp. 881–884.

[10] S. Ucar, B. Turan, S. Coleri Ergen, O. Ozkasap, and M. Ergen, "Dimming Support For Visible Light Communication in Intelligient Transportation and Traffic System," in *Urban Mobility and Intelligient Transportation System (UMITS), IEEE*, 2016.

[11] S. Ucar, S. C. Ergen, O. Ozkasap, D. Tsonev, and H. Burchardt, "SecVLC: Secure Visible Light Communication for Military Vehicular Networks," in *Proceedings of the 14th International Symposium on Mobility Management and Wireless Access (MobiWac)*. ACM, 2016.

[12] S. Ucar, S. C. Ergen, O. Ozkasap, and M. Ergen, "Askeri Araçlar Arası Güvenilir Görünür Işık ile İletişim Protokolü (SV^{2}LC)," in *8. Savunma Teknolojileri (SAVTEK)*, 2016.

[13] S. Ucar, S. C. Ergen, and O. Ozkasap, "Visible Light Communication Assisted Secure Autonomous Platoon," *pending Patent Application*, 2017.

[14] S. Ucar, S. C. Ergen, and O. Ozkasap, "IEEE 802.11p and Visible Light Hybrid Communication based Secure Autonomous Platoon," *under review IEEE Transactions on Vehicular Technology*, February 2017.

[15] S. Ucar, S. C. Ergen, and O. Ozkasap, "Security Vulnerabilities of Autonomous Platoon," *under review 25th Signal Processing and Communication Application Conference (SIU)*, February 2017.

[16] S. Ucar, S. C. Ergen, and O. Ozkasap, "Security vulnerabilities of IEEE 802.11p and visible light communication based platoon," in *IEEE Vehicular Networking Conference (VNC)*, Dec 2016.

[17] S. Ucar, S. C. Ergen, and O. Ozkasap, "Safety Message Dissemination in IEEE 802.11p and Visible Light Hybrid Communication Based Multiplatoon," *to be submitted IEEE Transactions on Vehicular Technology*, February 2017.

[18] S. Ucar, S. C. Ergen, and O. Ozkasap, "Visible Light Communication Assisted Safety Message Dissemination in Multiplatoon," *under review International Black Sea Conference on Communications and Networking*, February 2017.

[19] W. Viriyasitavat, S.-H. Yu, and H.-M. Tsai, "Short paper: Channel model for visible light communications using off-the-shelf scooter taillight," in *Vehicular Networking Conference (VNC), IEEE*, Dec 2013, pp. 170–173.

[20] 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 *Communications and Electronics (ICCE), Fourth International Conference on*, Aug 2012, pp. 31–34.

[21] A.-M. Cailean, B. Cagneau, L. Chassagne, S. Topsu, Y. Alayli, and M. Dimian, "Visible light communications cooperative architecture for the intelligent transportation system," in *Communications and Vehicular Technology in the Benelux (SCVT), IEEE 20th Symposium on*, Nov 2013, pp. 1–5.

[22] P. Luo, Z. Ghassemlooy, H. L. Minh, E. Bentley, A. Burton, and X. Tang, "Performance analysis of a car-to-car visible light communication system," *Appl. Opt.*, vol. 54, no. 7, pp. 1696–1706, Mar 2015.

[23] N. Zhu, Z. Xu, Y. Wang, H. Zhuge, and J. Li, "Handover method in visible light communication between the moving vehicle and multiple LED streetlights," *Optik - International Journal for Light and Electron Optics*, vol. 125, no. 14, pp. 3540 – 3544, 2014.

[24] C. B. Liu, B. Sadeghi, and E. W. Knightly, "Enabling Vehicular Visible Light Communication (V2LC) Networks," in *Proceedings of the Eighth ACM International Workshop on Vehicular Inter-networking*, ser. VANET. ACM, 2011, pp. 41–50.

[25] M. Abualhoul, M. Marouf, O. Shagdar, and F. Nashashibi, "Platooning control using visible light communications: A feasibility study," in *Intelligent Transportation Systems - (ITSC), 16th International IEEE Conference on*, Oct 2013, pp. 1535–1540.

[26] J.-H. Yoo, R. Lee, J.-K. Oh, H.-W. Seo, J.-Y. Kim, H.-C. Kim, and S.-Y. Jung, "Demonstration of vehicular visible light communication based on LED headlamp," in *Ubiquitous and Future Networks (ICUFN), Fifth International Conference on*, July 2013, pp. 465–467.

[27] M. Abualhoul, M. Marouf, O. Shag, and F. Nashashibi, "Enhancing the field of view limitation of Visible Light Communication-based platoon," in *Wireless Vehicular Communications (WiVeC), IEEE 6th International Symposium on*, Sept 2014, pp. 1–5.

[28] J. Liu, P. Chan, D. Ng, E. Lo, and S. Shimamoto, "Hybrid visible light communications in Intelligent Transportation Systems with position based services," in *Globecom Workshops (GC Wkshps), IEEE*, Dec 2012, pp. 1254–1259.

[29] A.-M. Cailean, B. Cagneau, L. Chassagne, V. Popa, and M. Dimian, "A survey on the usage of DSRC and VLC in communication-based vehicle safety applications," in *Communications and Vehicular Technology in the Benelux (SCVT), IEEE 21st Symposium on*, Nov 2014, pp. 69–74.

[30] B. V. Arem, C. J. G. V. Driel, and R. Visser, "The impacts of cooperative adaptive cruise control on traffic-flow characteristics," *IEEE Transactions on Intelligent Transportation Systems*, 2006.

[31] LEDFog101 OSRAM, @ONLINE. [Online]. Available: http://goo.gl/ty5zEC

[32] Li-1st, @ONLINE. [Online]. Available: http://purelifi.com/li-fire/li-1st/

[33] J. R. Barry, "Wireless infrared communications," in *Kluwer Academic Press*, 1994.

[34] Uniform provisions concerning the approval of power driven vehicle front fog lamps, United Nations Economic Commission for Europe, Vehicle Regulations - 1958 Agreement Regulation No. 19 @ONLINE. [Online]. Available: http://goo.gl/sdpQPb

[35] Transport Topic, @ONLINE. [Online]. Available: http://goo.gl/DslUJO

[36] S. Rajagopal, R. Roberts, and S.-K. Lim, "IEEE 802.15.7 visible light communication: modulation schemes and dimming support," *Communications Magazine, IEEE*, March 2012.

[37] E. Pisek, S. Rajagopal, and S. Abu-Surra, "Gigabit rate mobile connectivity through visible light communication," in *Communications (ICC), IEEE International Conference on*, June 2012.

[38] S.-H. Yu, O. Shih, H.-M. Tsai, N. Wisitpongphan, and R. Roberts, "Smart automotive lighting for vehicle safety," *Communications Magazine, IEEE*, December 2013.

[39] T. Yamazato, I. Takai, H. Okada, T. Fujii, T. Yendo, S. Arai, M. Andoh, T. Harada, K. Yasutomi, K. Kagawa, and S. Kawahito, "Image-sensor-based visible light communication for automotive applications," *Communications Magazine, IEEE*, July 2014.

[40] H.-Y. Tseng, Y.-L. Wei, A.-L. Chen, H.-P. Wu, H. Hsu, and H.-M. Tsai, "Characterizing link asymmetry in vehicle-to-vehicle Visible Light Communications," in *Vehicular Networking Conference (VNC), IEEE*, Dec 2015.

[41] S. Ishihara, R. V. Rabsatt, and M. Gerla, "Improving Reliability of Platooning Control Messages Using Radio and Visible Light Hybrid Communication," *Vehicular Networking Conference (VNC), IEEE*, 2015.

[42] Mercedes-Benz Multibeam Headlight, @ONLINE. [Online]. Available: https://goo.gl/Sn5LgI

[43] OSRAM Self-Dimming Headlights, @ONLINE. [Online]. Available: http://goo.gl/G30wmo

[44] F. Zafar, D. Karunatilaka, and R. Parthiban, "Dimming schemes for visible light communication: the state of research," *Wireless Communications, IEEE*, April 2015.

[45] I. Rubin, A. Baiocchi, F. Cuomo, and P. Salvo, "Vehicular Backbone Network Approach to Vehicular Military Ad Hoc Networks," in *Military Communications Conference, MILCOM IEEE*, Nov 2013.

[46] R. G. Engoulou, M. Bellaiche, S. Pierre, and A. Quintero, "VANET security surveys," *Computer Communications*, 2014.

[47] "Hacking The Vehicles By Listening Medium," http://goo.gl/3aGHwr.

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

[49] B. Zhang, K. Ren, G. Xing, X. Fu, and C. Wang, "SBVLC: Secure barcode-based visible light communication for smartphones," in *INFOCOM, Proceedings IEEE*, April 2014.

[50] A. M. Khalid, G. Cossu, R. Corsini, P. Choudhury, and E. Ciaramella, "1-Gb/s Transmission Over a Phosphorescent White LED by Using Rate-Adaptive Discrete Multitone Modulation," *IEEE Photonics Journal*, Oct 2012.

[51] G. Cossu, A. M. Khalid, P. Choudhury, R. Corsini, and E. Ciaramella, "2.1 Gbit/s visible optical wireless transmission," in *Optical Communications (ECOC), 38th European Conference and Exhibition on*, Sept 2012.

[52] D. Tsonev, S. Videv, and H. Haas, "Towards a 100 Gb/s visible light wireless access network," *Opt. Express*, 2015.

[53] A. Gomez, K. Shi, C. Quintana, M. Sato, G. Faulkner, B. C. Thomsen, and D. OBrien, "Beyond 100-Gb/s Indoor Wide Field-of-View Optical Wireless Communications," *IEEE Photonics Technology Letters*, Feb 2015.

[54] Y. Wang, X. Huang, L. Tao, and N. Chi, "1.8-Gb/s WDM visible light communication over 50-meter outdoor free space transmission employing CAP modulation and receiver diversity technology," in *Optical Fiber Communications Conference and Exhibition (OFC)*, March 2015.

[55] O. Almer, D. Tsonev, N. A. W. Dutton, T. A. Abbas, S. Videv, S. Gnecchi, H. Haas, and R. K. Henderson, "A SPAD-Based Visible Light Communications Receiver Employing Higher Order Modulation," in *IEEE Global Communications Conference (GLOBECOM)*, Dec 2015.

[56] Z. Wang, D. Tsonev, S. Videv, and H. Haas, "On the Design of a Solar-Panel Receiver for Optical Wireless Communications With Simultaneous Energy Harvesting," *IEEE Journal on Selected Areas in Communications*, Aug 2015.

[57] S. Zhang, D. Tsonev, S. Videv, S. Ghosh, G. A. Turnbull, I. D. W. Samuel, and H. Haas, "Organic solar cells as high-speed data detectors for visible light communication," *Optical*, Jul 2015.

[58] LiFiX, @ONLINE. [Online]. Available: http://purelifi.com/lifi-products/lifi-x/

[59] T. Komine and M. Nakagawa, "Fundamental analysis for visible-light communication system using LED lights," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, Feb 2004.

[60] Z. Cui, C. Wang, and H. M. Tsai, "Characterizing channel fading in vehicular visible light communications with video data," in *Vehicular Networking Conference (VNC), IEEE*, Dec 2014.

[61] M. Amoozadeh, H. Deng, C.-N. Chuah, H. M. Zhang, and D. Ghosal, "Platoon management with cooperative adaptive cruise control enabled by VANET," *Vehicular Communications*, 2015.

[62] Google Keyczar Tool, @ONLINE. [Online]. Available: https://goo.gl/LMuY1l

[63] Vishay Infra-red (IR) Diodes, @ONLINE. [Online]. Available: http://goo.gl/2DIKcq

[64] "VEhicular NeTwork Open Simulator (VENTOS)," http://goo.gl/OueFkO.

[65] S. Santini, A. Salvi, A. S. Valente, A. Pescap, M. Segata, and R. L. Cigno, "A consensus-based approach for platooning with inter-vehicular communications," in *IEEE Conference on Computer Communications (INFOCOM)*, April 2015.

[66] R. Rajamani, H.-S. Tan, B. K. Law, and W.-B. Zhang, "Demonstration of integrated longitudinal and lateral control for the operation of automated vehicles in platoons," *IEEE Transactions on Control Systems Technology*, Jul 2000.

[67] B. DeBruhl, S. Weerakkody, B. Sinopoli, and P. Tague, "Is Your Commute Driving You Crazy?: A Study of Misbehavior in Vehicular Platoons," in *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, ser. WiSec. ACM, 2015.

[68] M. Segata, B. Bloessl, S. Joerer, C. Sommer, M. Gerla, R. L. Cigno, and F. Dressler, "Toward Communication Strategies for Platooning: Simulative and Experimental Evaluation," *IEEE Transactions on Vehicular Technology*, Dec 2015.

[69] M. Amoozadeh, A. Raghuramu, C.-N. Chuah, D. Ghosal, H. Zhang, J. Rowe, and K. Levitt, "Security Vulnerabilities of Connected Vehicle Streams and Their Impact on Cooperative Driving," *Communications Magazine, IEEE*, June 2015.

[70] F. Qu, Z. Wu, F. Y. Wang, and W. Cho, "A Security and Privacy Review of VANETs," *IEEE Transactions on Intelligent Transportation Systems*, Dec 2015.

[71] X. Lin, X. Sun, P. H. Ho, and X. Shen, "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications," *IEEE Transactions on Vehicular Technology*, Nov 2007.

[72] S. Jiang, X. Zhu, and L. Wang, "An Efficient Anonymous Batch Authentication Scheme Based on HMAC for VANETs," *IEEE Transactions on Intelligent Transportation Systems*, Aug 2016.

[73] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," *Selected Areas in Communications, IEEE Journal on*, Oct 2007.

[74] J. L. Huang, L. Y. Yeh, and H. Y. Chien, "ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks," *IEEE Transactions on Vehicular Technology*, Jan 2011.

[75] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An Efficient Pseudonymous Authentication Scheme With Strong Privacy Preservation for Vehicular Communications," *IEEE Transactions on Vehicular Technology*, Sept 2010.

[76] S. Biswas and J. Mii, "A Cross-Layer Approach to Privacy-Preserving Authentication in WAVE-Enabled VANETs," *IEEE Transactions on Vehicular Technology*, Jun 2013.

[77] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," *IEEE Transactions on Parallel and Distributed Systems*, Sept 2010.

[78] Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhang, "Enforcing Privacy Using Symmetric Random Key-Set in Vehicular Networks," in *Eighth International Symposium on Autonomous Decentralized Systems (ISADS)*, March 2007.

[79] M. N. Mejri, N. Achir, and M. Hamdi, "A new group Diffie-Hellman key generation proposal for secure VANET communications," in *13th IEEE Annual Consumer Communications Networking Conference (CCNC)*, Jan 2016.

[80] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces," in *Proceedings of the 20th USENIX Conference on Security*, ser. SEC, 2011.

[81] C. Miller and C. Valasek, "Demo: Adventures im automotive networks and control units," in *Proceedings of the DEFCON*, 2013.

[82] C. Miller and C. Valasek, "A survey of remote automotive attack surfaces," in *Proceedings of the Blackhat*, 2014.

[83] C. Miller and C. Valasek, "Remote exploitation of an unaltered passanger vehicle," in *Proceedings of the Blackhat*, 2015.

[84] L. Wu, Z. Zhang, J. Dang, and H. Liu, "Adaptive Modulation Schemes for Visible Light Communications," *Journal of Lightwave Technology*, Jan 2015.

[85] M. Wang, J. Wu, W. Yu, H. Wang, J. Li, J. Shi, and C. Luo, "Efficient coding modulation and seamless rate adaptation for visible light communications," *IEEE Wireless Communications*, April 2015.

[86] S. H. Lee, S. Y. Jung, and J. K. Kwon, "Modulation and coding for dimmable visible light communication," *IEEE Communications Magazine*, Feb 2015.

[87] M. Segata, R. L. Cigno, H. M. M. Tsai, and F. Dressler, "On platooning control using IEEE 802.11p in conjunction with visible light communications," in *12th Annual Conference on Wireless On-demand Network Systems and Services (WONS)*, Jan 2016.

[88] A. Bazzi, B. M. Masini, A. Zanella, and A. Calisti, "Visible light communications as a complementary technology for the internet of vehicles," *Computer Communications*, 2016.

[89] "IEEE 802.11p-VLC Simulation Platform," https://goo.gl/VCHzRo.

[90] D. R. Stinson, "Cryptography: Theory and Practice," *CRC Press*, 2006.

[91] U. M. Maurer and S. Wolf, "The relationship between breaking the diffie–hellman protocol and computing discrete logarithms," *SIAM Journal on Computing*, 1999.

[92] P. Trimintzios and G. Georgiou, "WiFi and WiMAX Secure Deployments," *Journal of Computer Systems, Networks, and Communications*, Jan. 2010.

[93] L. Xiao and F. Gao, "Practical String Stability of Platoon of Adaptive Cruise Control Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, Dec 2011.

[94] S. Li, K. Li, R. Rajamani, and J. Wang, "Model Predictive Multi-Objective Vehicular Adaptive Cruise Control," *IEEE Transactions on Control Systems Technology*, May 2011.

[95] P. Seiler, A. Pant, and K. Hedrick, "Disturbance propagation in vehicle strings," *IEEE Transactions on Automatic Control*, Oct 2004.

[96] R. Olfati-Saber and R. M. Murray, "Consensus problems in networks of agents with switching topology and time-delays," *IEEE Transactions on Automatic Control*, Sept 2004.

[97] M. R. Jovanovic and B. Bamieh, "On the ill-posedness of certain vehicular platoon control problems," *IEEE Transactions on Automatic Control*, Sept 2005.

[98] D. Jia and D. Ngoduy, "Platoon based cooperative driving model with consideration of realistic inter-vehicle communication," *Transportation Research Part C: Emerging Technologies*, 2016.

[99] Y. Li, K. Li, T. Zheng, X. Hu, H. Feng, and Y. Li, "Evaluating the performance of vehicular platoon control under different network topologies of initial states," *Physica A: Statistical Mechanics and its Applications*, 2016.

[100] "Simulation of Urban MObility (SUMO)," http://sumo.sourceforge.net/.

[101] "OMNET++ Networ Simulator," https://omnetpp.org/.

[102] "Vehicles in Network Simulation (Veins)," http://veins.car2x.org/.

[103] "Crypto++ Library," http://www.cryptopp.com/wiki/Main_Page.

[104] "More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange," https://tools.ietf.org/html/rfc3526.

[105] D. Jia, K. Lu, J. Wang, X. Zhang, and X. Shen, "A Survey on Platoon-Based Vehicular Cyber-Physical Systems," *IEEE Communications Surveys Tutorials*, 2016.

[106] N. Wisitpongphan, O. Tonguz, J. Parikh, P. Mudalige, F. Bai, and V. Sadekar, "Broadcast storm mitigation techniques in vehicular ad hoc networks," *Wireless Communications, IEEE*, December 2007.

[107] H. Peng, D. Li, K. Abboud, H. Zhou, H. Zhao, W. Zhuang, and X. Shen, "Performance Analysis of IEEE 802.11p DCF for Multiplatooning Communications with Autonomous Vehicles," *IEEE Transactions on Vehicular Technology*, 2016.

[108] S. Bitam, A. Mellouk, and S. Zeadally, "Bio-Inspired Routing Algorithms Survey for Vehicular Ad Hoc Networks," *IEEE Communications Surveys Tutorials*, 2015.