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

Seyhan Ucar*, Sinem Coleri Ergen† and Oznur Ozkasap*
*Department of Computer Engineering, †Department of Electrical and Electronics Engineering
Koc University, Turkey
{sucar, sergen, oozkasap}@ku.edu.tr

***Abstract*—Autonomous vehicle platoon is an enhancement of autonomous behavior, where vehicles are organized into groups of close proximity through wireless communication. Platoon members mostly communicate with each other via the current dominant vehicular radio frequency (RF) technology, IEEE 802.11p. However, this technology leads security vulnerabilities under various attacks from adversaries. Visible Light Communication (VLC) has the potential to alleviate these vulnerabilities by exploiting the directivity and impermeability of light. Utilizing only VLC in vehicle platoon, on the other hand, may degrade platoon stability since VLC is sensitive to environmental effects. In this paper, 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 securing platoon maneuvers under data packet injection, channel overhearing, jamming and platoon maneuver attacks. We define platoon maneuver attack based on the identification of various scenarios where a fake maneuver packet is transmitted by a malicious actor. SP-VLC includes mechanisms for the secret key establishment, message authentication, data transmission over both IEEE 802.11p and VLC, jamming detection and reaction to switch to VLC only communication and secure platoon maneuvering based on the joint usage of IEEE 802.11p and VLC. We develop a simulation platform combining realistic vehicle mobility model, realistic VLC and IEEE 802.11p channel models, and vehicle platoon management. We show the functionality of the SP-VLC protocol under all possible security attacks by performing extensive simulations. Our findings demonstrate that SP-VLC protocol generates less than 0.1% difference in the speed of and distance between platoon members during security attacks in comparison to 25% and 10% in that of previously proposed IEEE 802.11p and IEEE 802.11p-VLC hybrid protocols, respectively.**

***Index Terms*—autonomous platoon, vehicular communication, security, visible light communication, IEEE 802.11p**

I. 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, Global Positioning System (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 [3]. Autonomous vehicle platoon is a group of cooperative adaptive cruise control (CACC) vehicles kept in close proximity through wireless communication [4], [5]. 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 [6]. 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 [6]–[10]. 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. Recent studies demonstrate that the lack of security protocol causes platoon instability under message falsification and RF jamming attacks [11], [12]. Platoon systems usually adopt the current dominant vehicular RF technology, IEEE 802.11p, which forms the standard for Wireless Access for Vehicular Environments. Although the high transmission range of IEEE 802.11p provides access to a large number of vehicles at once, this wide coverage makes this communication technology vulnerable to adversaries blocking and interrupting the communication among the vehicles.

*A preliminary version of this work appeared in IEEE Vehicular Networking Conference, Columbus, Ohio, USA, Dec. 2016 [1]

Existing security solutions proposed for inter-vehicular communication mostly address general vehicular ad hoc networks (VANETs). In solutions for VANETs, the infrastructure support is an essential part of the security architectures. Security architecture not only defines the security policies but also specifies when and where to apply security controls. Security standard, on the other hand, provides detailed requirements on how these security policies must be implemented. For VANETs, the security architectures and infrastructures have been investigated in [13]–[17] and security standard protocols are presented in [18]–[20]. In the following, the details of the most popular security infrastructures, the recent security architectures and well-known security standards for VANET are described.

Public Key Infrastructure (PKI) is the most used VANET security infrastructure that supports the distribution and identification of public encryption keys which enable vehicles to securely exchange data and verify the identity of the other vehicles. Security architectures for Intelligent Transportation System (ITS) that are based on PKI are proposed by ETSI and National Highway Traffic Safety Administration (NHTSA) in [21] and [13], respectively. PKI guarantees the integrity of the packet, eliminating the interruption by non-authorized vehicles. However, authorized vehicles may still perform attacks, which need to be detected and included in the certificate revocation list (CRL) [22]. 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 roadside units are used [23]–[25]. This delay cannot be tolerated in vehicle platoon settings. Moreover, the CRL transmissions are prone to security attacks. On the other hand, the usage of centralized ETSI and NHTSA architectures in vehicle platoons has the following drawbacks [26]. First, the communication with the centralized entities can create a single point of failure, making it vulnerable to several attacks. Second, the large communication overhead and delay associated with the verification is not tolerable in time-critical vehicle platoons.

The security standard to enable secure V2V and V2I wireless communications is published under the IEEE 1609 Family of Standards for Wireless Access in Vehicular Environments (WAVE) protocol [16]. The IEEE 1609.2 protocol presents methods to secure the messages that are used by WAVE. Security is provided based on key and certificate management that is derived from PKI. The encryption and digital signature are used for secure key distributions. In the key distribution/management, vehicles use secret keys to secure the communication based on either asymmetric cryptography [27] or symmetric cryptography [28]. In asymmetric cryptography, sender and receiver establish a secret key by using pairs of keys: the public key that may be disseminated publicly, and the private key that is known only to the owner. Sender and receiver agree on a secret key using a key establishment protocol. On the other hand, in symmetric cryptography, a shared key is used 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. Moreover, in IEEE 1609.2 despite the security requirements such as confidentiality, authenticity and integrity are ensured, the anonymity is limited and no mechanism is defined for multi-hop V2V communication.

As an alternative, asymmetric cryptography has been recently proposed for the platoon where vehicles establish a shared group key based on the sharing of their public key between each pair of vehicles [29]. The system performance is evaluated based on the time duration needed for vehicles to exchange the public key and establish the group key. 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 radio 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 [30]–[33]. 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 distinguishing propagation characteristics [34]. VLC uses modulated optical radiation in the visible light spectrum to carry digital information wirelessly. A VLC system usually uses a light emitting diode (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 [35]. 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. The directivity of VLC is narrow and the attacker needs to point a strong light to the moving victim to saturate the VLC receivers. Such an attack on VLC can only be performed on a few VLC links, as opposed to all vehicles in the range of IEEE 802.11p for the case of RF. The

impermeability of the light, on the other hand, limits the data reception into specific area, typically within the light coverage, and makes the data difficult to intercept from outside. 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 [7]. On the other hand, VLC communication range has been demonstrated to be 100 m for headlights and 30 m for taillights [36]. Moreover, the attackers need to direct strong light to saturate the receiver, which may not be feasible without the vehicle noticing the attack.

Previous studies on the VLC based vehicular communication have focused on the derivation of channel characteristics [36]–[38], requirements [39]–[41], advanced modulation schemes [42]–[44] and feasibility in a hybrid architecture together with IEEE 802.11p [45]–[47]. 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) [48]. 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 [49], [50]. Physical layer security for indoor VLC is proposed by investigating the achievable secrecy rates of the Gaussian wiretap channel [49]. 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 [50]. 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 paper, 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 injection, channel overhearing, 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 paper 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 and larger transmission range of IEEE 802.11p. 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 in addition to commonly known attacks of data packet injection, channel overhearing and jamming, we define various forms of attacks specific to vehicular platoon management and maneuvers, including generation of fake entrance request, fake entrance response, fake leave request, fake leave response, fake merge request, fake merge response, fake split request and fake split response packets, for the first time in the literature. We demonsrate 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 [51].
- 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 paper is organized as follows. Section II describes the platoon management and communication. Section III describes the attack scenarios for malicious actors. Section IV demonstrates the platoon dynamicity, platoon information and platoon stability models. Section V presents the proposed SP-VLC protocol. Section VI 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 VII.

II. Platoon System 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 in the leftmost lane, as shown in Fig. 1.

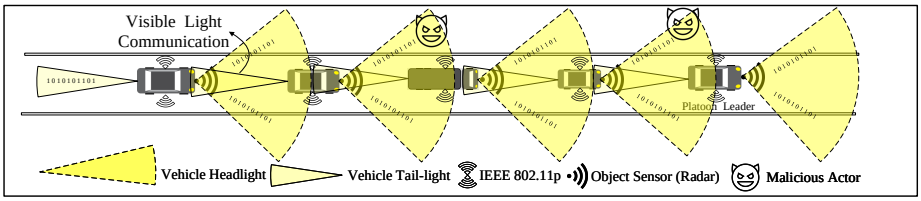


Fig. 1: Hybrid autonomous platoon communication architecture

In general, there exist 3 types of vehicles namely platoon-enabled, non-platooned and platooned vehicles. A platoon-enabled vehicle has all the required hardware and software and can be either a non-platooned or platooned vehicle. A non-platooned vehicle, on the other hand, is not part of any platoon and it travels under manual driving whereas platooned vehicle is a member of the platoon. The leftmost lane is reserved for the platoon to discriminate the non-platooned and platoon-enabled vehicles. Only the platoon-enabled vehicles are allowed to steer into the leftmost lane to be part of the vehicular platoon.

Each vehicle in the platoon contains an on-board unit (OBU) to implement platoon communication and management protocol, and keep the vehicle information base. OBU consists of a CPU, a volatile memory, a built-in clock and input/output interfaces. Moreover, OBU has a built-in battery to power the clock and detect the tamper in order to erase any vehicle private information, thus preventing the adversary compromise. The protocol relies on the data received from sensors, IEEE 802.11p and VLC receivers; and outputs data to IEEE 802.11p and VLC transmitters. VLC transmitters and receivers are placed on both the front and 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 an asymmetric communication link between consecutive vehicles. Sending messages from platoon leader to all members via VLC is not possible due to its directivity feature and obstacles caused by other vehicles. Thus, the data from the leader to the members are disseminated by headlights and tail-lights in a multi-hop manner. However, if the link speed is low, then the multi-hop transmission leads to long end-to-end delay. To reduce the delay, the platoon data is forwarded using both IEEE 802.11p and VLC.

Platoon communication should satisfy timeliness, security and reliability requirements 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 combining two platoons that are traveling in the same lane. Platoon splitting is defined as separating a platoon into two smaller size platoons. 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.

In autonomous vehicles, passengers indicate their destination as input through the user interface. It is assumed that autonomous vehicles try to find a target platoon to join based on their final destination. A list of target platoons, sorted by route, is broadcast by Road Side Units (RSUs). In route based platoon selection, autonomous vehicle joins a platoon that is traveling on the route that the passenger has selected for the trip. Joining a platoon that is traveling on the same route aims to fewer platoon maneuvers.

Platoon leader coordinates all platoon maneuvers. Platoon maneuvers can happen any time 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, which contains the information for the suitability of the platoon maneuver, is sent back to the initiating vehicle. 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 systems is used in conjunction with the sensors and communication among vehicles with the goal of determining the speed and location of the vehicle, the distance to the preceding vehicle and having 360-degree of the field of view. Examples of the system are laser, vision, radar and audio. Laser system works day and night by beaming laser pulses and measuring how long it takes to reflect off a surface

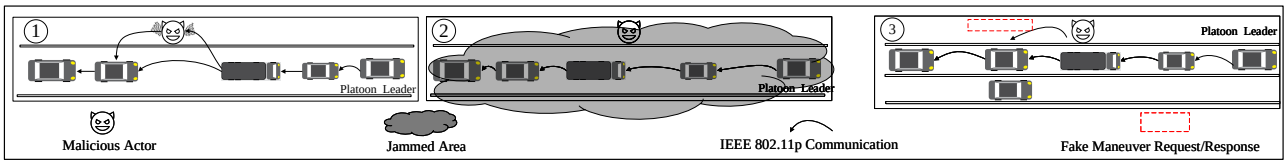


Fig. 2: 1) Platoon Data Packet Injection and Channel Overhearing 2) Platoon Jamming, 3) Platoon Maneuver Attack

to measure distance. Vision system includes cameras designed to see the world as a human would and showing dynamic and static objects such as pedestrians, cyclists, other vehicles and traffic lights. Radar system uses wavelength to perceive objects and movements. Audio system hears the police and emergency vehicle sirens. Whenever the instantaneous space gap between vehicles is detected to be below the safe space threshold, the vehicle control is relinquished to the human driver (if any) or vehicles switch from CACC to ACC and actuate the brake and throttle to avoid the collision.

The PKI in the system is responsible for the identity management of all vehicles registered in its region (e.g. national territory or district). Each vehicle keeps its unique identity, a pair of private and public cryptographic keys and a certificate issued by CA in the Hardware Security Module (HSM) of vehicle. HSM is physically separated from OBU. During proposed protocol execution, the HSM sensitive information are brought to volatile part of OBU, Vehicle Information Base (VIB), to establish separate secret keys for preceding and following vehicles. 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.

III. Vehicle Platoon Security Attack Categories

In this section, we present our attacker model by considering the currently used security infrastructure, security architecture and security standard protocols as discussed above. VANET security solutions generally include certificate and cryptographic keys in a HSM to provide privacy and confidentiality, respectively. It is assumed that the HSM is protected against the tampering. The core of our attacker model, on the other hand, is that an attacker may gain control over the security module by hacking the HSM. The hack of HSM can happen either through software compromise by physical manipulation of vehicle in manufacturing/maintenance phase or through reverse engineering from a captured old HSM [11], [12].

Malicious actors aim to destabilize the platoon and destroy membership by performing data packet injection, channel overhearing and jamming on platoon communication medium. Malicious actors are assumed to be roadside units or vehicles that are part of VANET, but not part of the platoon, which aim to destroy platoon stability without being affected by the consequences. They are equipped with both IEEE 802.11p and VLC devices. The case where the malicious actors are insider adversaries, which are trusted platoon members, on the other hand, necessitate misbehaviour/anomaly detection and trust management schemes [52], and are out of the scope of this paper.

The behavior of the malicious actor is different for each type of platoon attack. The attack scenarios for malicious actors are illustrated in Fig. 2 and explained in detail next.

1) **Platoon Data Packet Injection:** Data forgery and replay attacks are considered examples of this class. Data forgery is defined as altering the platoon data packet content and rebroadcasting it as if the message comes from platoon members. 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. In the 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 in the replay attack, the outdated information may mislead the platoon members, possibly ruining the platoon stability. Global Positioning System (GPS) synchronized clock or packet sequence numbers are used to prevent the data packet replay attacks, whereas the usage of cryptographic keys, digital certificates and signature eliminates data packet forgery attacks. However, the usage of replicated certificates or private keys concurrently, which is referred as Sybil attack [53], [54], may still make these attacks practically possible. Moreover, the dishonest vehicle might behave smartly by discarding any detected certificates or private keys in Sybil attack to avoid being traced/tracked by the authorities.

2) **Platoon Channel Overhearing:** Malicious actor overhears the platoon communication medium, collects vehicle private information and platoon operations, and impersonates the identity of platoon members. The information the malicious actor might get includes route and final destination of the autonomous vehicles, which exposes privacy at risk. For example, car rental or insurance companies may want to follow the vehicles in an illegitimate manner to track the passengers.

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. Malicious actor aims to violate the medium access control (MAC) protocol and cause delay in packet delivery, which endangers the stable operation of vehicle platoon. Moreover, it has been shown that jamming can be performed on network layer to disrupt the communication by overloading the HSM, which leads to cryptographic packet loss due to delay in packet

verification and authentication steps [11], [55].

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 enter the platoon. Then the platoon leader sends a positive response, approving the entrance of the vehicle. Two consecutive platoon members increase their inter-vehicular distance for the proper 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. This decreases the efficiency of the vehicle 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 increase 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 the proper leaving of the vehicle. The inter-vehicular distance stays larger than the safe distance of the platoon until the platoon members realize that no platoon member intends to leave. This decreases the efficiency of the vehicle 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 the platoon leader is performing another maneuver. 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 management.

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.

IV. Stability Analysis of Information Flow on Vehicular Platoon

In this section, we provide the mathematical model for the platoon stability incorporating vehicle longitudinal dynamics, information flow topology and decentralized feedback control law.

A. 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

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

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 [56], [57]

$$x_i'(t) = Ax_i(t) + Bu_i(t) \tag{2}$$

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.

B. 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 [58]–[60]. 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

$$u_i(t) = -k^T \epsilon_i(t) \tag{3}$$

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,

$$\epsilon_i(t) = \sum_{j=0}^{N} m_{ji}(\widetilde{x}_i(t) - \widetilde{x}_j(t)), \tag{4}$$

$\widetilde{x}_i(t) = [\widetilde{p}_i(t), \widetilde{v}_i(t), \widetilde{a}_i(t)]$, $\widetilde{p}_i(t)$, $\widetilde{v}_i(t)$ 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

$$\widetilde{x}_i'(t) = A\widetilde{x}_i(t) - Bk^T \sum_{j=0}^{N} m_{ji}(\widetilde{x}_i(t) - \widetilde{x}_j(t)) \tag{5}$$

C. Platoon Stability Model

A platoon is stable if

$$\lim_{t\to\infty} \widetilde{x}_i(t) \leq C_0 \tag{6}$$

is satisfied for all $i \in [1, N]$, where C_0 is a constant bounded value [61], [62]. Equation (6) demonstrates that the platoon stability is a function of vehicle longitudinal dynamics and information flow among platoon members. The security attacks prevent the information flow, thus destroying platoon stability. Next, we propose a novel hybrid platoon communication and management protocol and analyze its effect on the information flow under security attacks.

V. Secure Hybrid Platoon Communication and 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 under various types of security attacks. SP-VLC is based on secret key establishment using asymmetric cryptography and usage of established secret key for the exchange of packets between consecutive vehicles in the platoon while exploiting 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 VLC based generated secret keys 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 injection. 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 based on the interpretation of packet reception statistics,

and switching to VLC-only communication for secure packet reception in case of jamming detection.

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.
8) It provides a decision mechanism for the verification of the maneuver request based on the determination of the vehicle existence in the next lane by using the vision system of the vehicle.

Next, we provide 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 I.

TABLE I: 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 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 Members' Secret Key
$Session_{ack}$	Key Session Acknowledgement Packet

A. Secret Key Establishment and Update Mechanism

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 [63], [64]. This necessitates the periodical update of the secret key between consecutive vehicle pairs in the platoon, which is referred as key freshness [65]. Key freshness is essential to prevent the adversaries from obtaining and decoding the secret keys [66].

A pair of consecutive platoon members establishes a common Key_{secret} without any explicit announcement to each other. The secret key initiator and responder can be any platoon member. However, to prevent the contention in the secret key establishment, the rear platoon member in a pair of consecutive vehicles is selected as the secret key initiator. The initiator and responder vehicles first agree on two prime numbers g and p, where p is a large prime number and g is a primitive root modulo p. Then, vehicles run different algorithms to establish the same Key_{secret} at the initiator and responder, respectively.

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 Update Key_secret in VIB;
```

The initiator vehicle executes Algorithm 1. This vehicle computes the secret key initiation packet and shares X with 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 (Line 8).

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     Update Key_secret in VIB;
```

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 $5-6$). 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 (Line 7).

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.

B. Data Transmission Mechanism

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. The exchange of vehicle platoon data packets between consecutive vehicle pairs in the platoon requires message authentication code insertion, encryption by using Key_{secret} at the sender and decryption by using the same Key_{secret} and authentication of the message at the receiver. 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.

Algorithm 3: Secure Data Transmission Mechanism

1 **foreach** *received* $Platoon_{data}^{encrypted}$ **do**
2 Retrieve Key_{secret} from VIB;
3 ($Platoon_{data}$, tag)=Decrypt($Platoon_{data}^{encrypted}$, Key_{secret});
4 **if** *verify(tag,*$Platoon_{data}$*,* 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 steps of CMAC (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 $7-11$).

C. 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 initiate the VLC jamming and 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. By receiving the platoon data or membership view packets, malicious actors figure out that the platoon is in the light transmission range and consists of members where the VLC jamming can be initiated. Secure platoon communication, on the other hand, encrypts the platoon data and membership view packets content and ensures confidential data transmission, which prevents platoon from such VLC jamming. In case that the attackers detect the existence of the vehicle platoon via other techniques, such as camera, VLC and RF communication can be jammed simultaneously. Then the solution is to either relinquish the vehicle control to the human driver (if any) or switch from CACC to ACC to prevent the collision. The transition to a driver or ACC switch to take over the vehicle control are still required by CACC technologies when an event is detected and not resolved by the autonomous vehicle's software [67].

D. Platoon Maneuver Operations

1) Platoon Entrance: When a new vehicle intends to enter the platoon, the following steps are executed:

- The new vehicle sends a secret key initiation packet 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 by using their vision system. If the source is a vehicle on the next lane then these platoon members send a secret key response packet. Otherwise, they ignore the packet.
- The vehicle waits until the reception of the first secret key response from a platoon member. Then $Session_{ack}$ packet and subsequently entrance request packet en-

crypted by the use of the Key_{secret} are sent to the corresponding platoon member via VLC.
- The platoon member that receives encrypted entrance request packet decrypts/authenticates the packet and performs secure data transmission mechanism (Algorithm 3) with the secret key of the preceding vehicle in the platoon and sends the packet to that vehicle over both VLC and IEEE 802.11p.
- Upon reception of the encrypted entrance request packet, each platoon member decrypts/authenticates 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 increase their inter-vehicular distance so that the new vehicle can steer to the platoon lane.

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 leave 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.

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 platoon member, which receives the secret key initiation packet via VLC, first checks whether the source of the packet is a roadside unit or a vehicle traveling in the same lane prior to secret key response packet. The vision system controls the vehicle and if the source of secret key initiation packet is not a vehicle, the packet is ignored.
- 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, $Session_{ack}$ packet is sent over VLC and merge request packet is sent via both VLC and IEEE 802.11p by using encryption mechanism to the corresponding platoon member. Otherwise, $Session_{ack}$ packet and merge request packet are 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 distance 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 key 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 $Session_{ack}$ packet and 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.

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. 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. Similar to merge, the split operation is coordinated by the platoon leader. The platoon leader sends a split request packet to the platoon member from which the split needs to be 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.

VI. 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 [7], denoted by *IEEE 802.11p protocol*, and VLC and IEEE 802.11p based hybrid platooning control, denoted by *VLC-IEEE 802.11p protocol* [46], in terms of platoon stability under data packet injection, 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) [68]. VENTOS is a simulator integrating an open source microscopic road traffic simulator, Simulation of Urban Mobility (SUMO) [69]; a discrete packet-level simulator, OMNET++ [70]; and V2V communication platform, Vehicles in Network Simulation (Veins) [71]. SUMO is an open-source, space-continuous, and discrete-time traffic simulator that is developed by Institute of Transportation System at the German Aerospace Center and capable of simulating the micro-behavior of individual vehicles. OMNET++ is a component-based simulation package and used for capturing the wireless communication simulation in VENTOS. Veins is based on these two well-established simulators SUMO and OMNET++, and extends them with comprehensive channel models and communication protocols for vehicular networks. VENTOS further includes platoon management protocols supporting different maneuvers. 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 [36]. The DH, encryption/decryption and authentication mechanism of SP-VLC are developed using the open-access cryptography library, Crypto++ [72]. Crypto++ is a library for cryptographic schemes including message authentication and key agreement. Vehicles utilize the Crypto++ functionalities and use secret 1024 bit values, a and b, in key agreement, having the form of safe primes specified in More Modular Exponential (MODP) DH groups for Internet Key Exchange [73] and periodically updated.

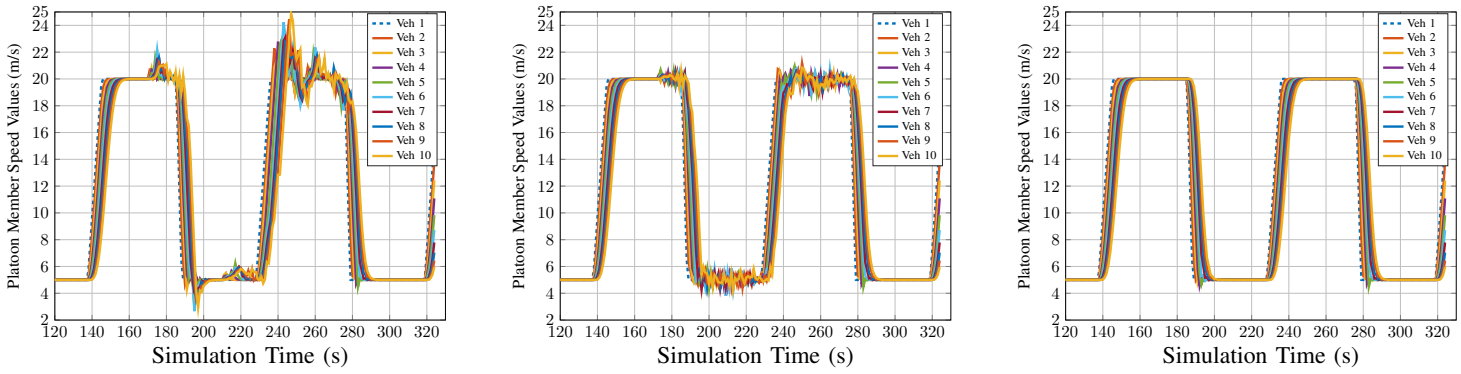
The road topology consists of a two-lane road of length 90 km with the leftmost lane reserved for platooned vehicles. We assume vehicles are homogeneous and all are platoon-enabled. At some point, vehicles perform entrance maneuver to be part of platoon. The vehicles are injected into the road from the right lane according to Poisson process at 0.5 vehicles per second rate. 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 II lists simulation parameters.

TABLE II: Simulation Parameters

	Parameter	Value
Simulation	Simulation time	325 s
	Number of vehicles	15
	Vehicular IEEE 802.11p range	300 m
	Platoon data transmission frequency	10 Hz
	$Platoon_{data}$, $Membership_{view}$ size	100 bytes
	$Tkey$ / $Tsession$	5 s / 2 s
VLC	Transmit Power	-60 dBm
	Packet Sensitivity	-114 dBm
	Path Loss Exponent	2
	Height of Front Receiver	0.9 m
	Height of Back Receiver	0.55m
	Headlight / Tail-light Range	100 m / 30 m
	Angular Headlight Range	-45° $\sim$ 45°
	Angular Tail-light Range	-60° $\sim$ 60°
C(ACC)	Min / Max Speed	5 m/s / 20 m/s
	Min Space Gap	2 m
	Max Acceleration / Deceleration	3 m/s^2 / 5 m/s^2
	$Optimal_{size}$	10

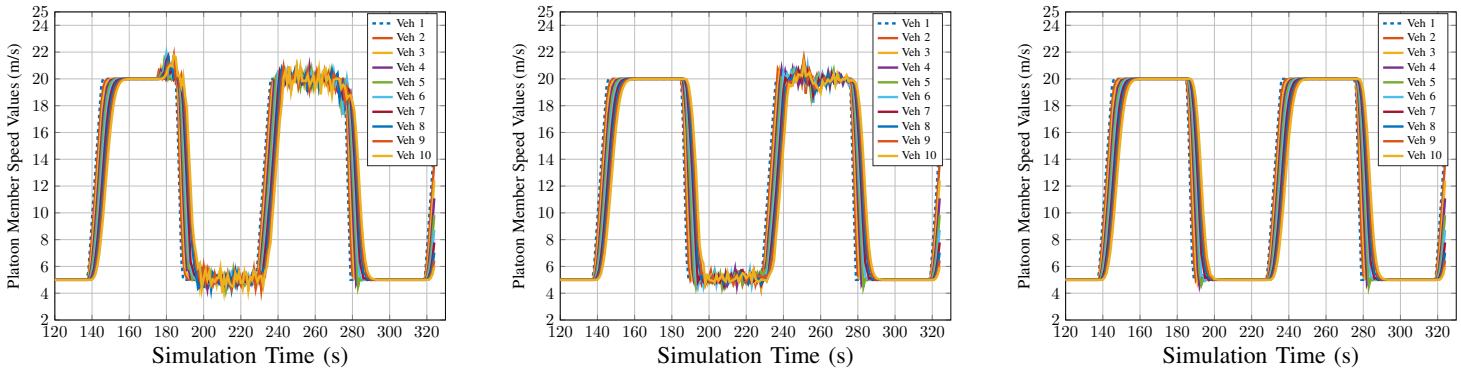
A. Platoon Data Packet Injection

1) Platoon Data Packet Forgery Attack: Fig. 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



(a) (b) (c)

Fig. 3: Data Forgery Attack on Platoon (a) IEEE 802.11p protocol (b) VLC-IEEE 802.11p protocol (c) SP-VLC



(a) (b) (c)

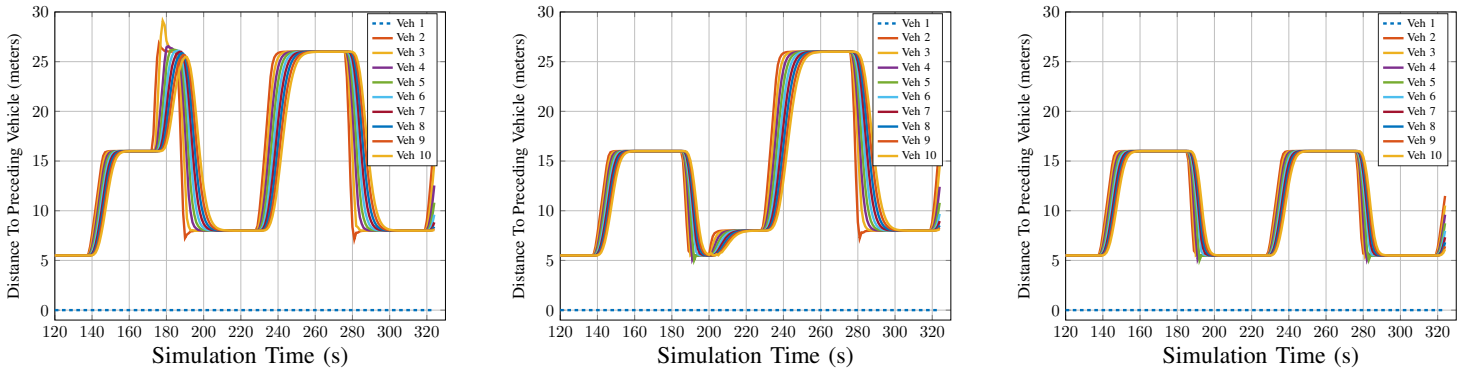
Fig. 4: Data Replay Attack on Platoon (a) IEEE 802.11p protocol (b) VLC-IEEE 802.11p protocol (c) SP-VLC

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 forgery attack without any fluctuation in platoon member speed values. 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.

2) Platoon Data Packet Replay Attack: Fig. 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, 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.

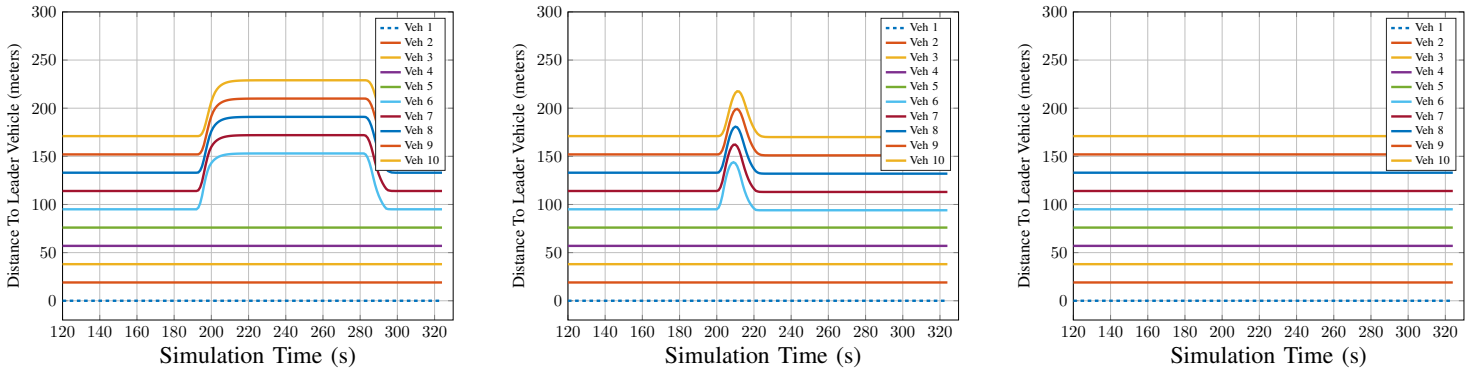
B. Jamming Attack

Fig. 5 shows the space gap between consecutive platoon members for IEEE 802.11p, VLC-IEEE 802.11p and SP-VLC



(a) (b) (c)

Fig. 5: Jamming Attack on Platoon (a) IEEE 802.11p protocol (b) VLC-IEEE 802.11p protocol (c) SP-VLC



(a) (b) (c)

Fig. 6: Fake Split Request Attack on Platoon (a) IEEE 802.11p protocol (b) VLC-IEEE 802.11p protocol (c) 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 increasing their inter-vehicle distance. On the other hand, SP-VLC solves both IEEE 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.

C. Platoon Maneuver Attack

We have chosen the fake split request as example of platoon maneuver attack, since it is representative of other maneuver attacks and its effect on the platoon efficiency is easier to visualize.

Fig. 6 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 this 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. 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.

VII. Conclusion

In this paper, 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 injection, channel overhearing, 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 demonstrate the proper functioning of the proposed SP-VLC protocol under all possible security attacks by performing extensive simulations. 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 show that IEEE 802.11p protocol based platoon management is highly vulnerable to data packet injection, 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 duration and amount of speed fluctuations due to the light directivity by 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 of the platoon members and performs any maneuvers without interference from attackers.

References

[1] 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.

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

[3] 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*, April 2016.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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 Conference on Security & Privacy in Wireless and Mobile Networks*, ser. WiSec. ACM, 2015.

[10] 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.

[11] 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.

[12] R. W. van der Heijden, T. Lukaseder, and F. Kargl, "Analyzing Attacks on Cooperative Adaptive Cruise Control (CACC)," in *IEEE Vehicular Networking Conference (VNC)*, Nov 2017.

[13] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, "A security credential management system for V2V communications," in *IEEE Vehicular Networking Conference*, Dec 2013.

[14] K. Pll and H. Federrath, "A privacy aware and efficient security infrastructure for vehicular ad hoc networks," *Computer Standards and Interfaces*, 2008.

[15] M. Abuelela, S. Olariu, and K. Ibrahim, "A Secure and Privacy Aware Data Dissemination For The Notification of Traffic Incidents," in *IEEE 69th Vehicular Technology Conference*, April 2009.

[16] H. Hasrouny, C. Bassil, A. E. Samhat, and A. Laouiti, "Group-based authentication in V2V communications," in *Fifth International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*, April 2015.

[17] "SCOOP@F, Cooperative Intelligent Transport Systems Pilot Deployment Project," https://goo.gl/xqA1jF.

[18] "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation," *IEEE Std 1609.4-2006 -Test*, Nov 2006.

[19] "ETSI TS 102 940, Intelligent Transport Systems Security," https://goo.gl/gy4VHS.

[20] "ETSI TS 102 941 Intelligent Transport Systems Security, Trust and Privacy Management," https://goo.gl/UGoy5z.

[21] "ETSI TS 102 867 V1.1.1 - Security-Mapping for IEEE 1609.2," https://goo.gl/4FWCMe.

[22] 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.

[23] 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.

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

[25] J. L. Huang, L. Y. Yeh, and H. Y. Chien, "ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Ser-

vices in Vehicular Ad Hoc Networks," *IEEE Transactions on Vehicular Technology*, Jan. 2011.
[26] S. Biswas and J. Mii, "A Cross-Layer Approach to Privacy-Preserving Authentication in WAVE-Enabled VANETs," *IEEE Transactions on Vehicular Technology*, Jun 2013.
[27] 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.
[28] Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhang, "Enforcing Privacy Using Symmetric Random Key-Set in Vehicular Networks," in *IEEE Eighth International Symposium on Autonomous Decentralized Systems (ISADS)*, March 2007.
[29] 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.
[30] 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.
[31] C. Miller and C. Valasek, "Demo: Adventures im automotive networks and control units," in *Proceedings of the DEFCON*, 2013.
[32] C. Miller and C. Valasek, "A survey of remote automotive attack surfaces," in *Proceedings of the Blackhat*, 2014.
[33] C. Miller and C. Valasek, "Remote exploitation of an unaltered passanger vehicle," in *Proceedings of the Blackhat*, 2015.
[34] 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.
[35] S. Rajagopal, R. D. Roberts, and S. K. Lim, "IEEE 802.15.7 Visible Light Communication: Modulation Schemes and Dimming Support," *IEEE Communications Magazine*, March 2012.
[36] 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.
[37] W. Viriyasitavat, S.-H. Yu, and H.-M. Tsai, "Short paper: Channel model for visible light communications using off-the-shelf scooter taillight," in *IEEE Vehicular Networking Conference (VNC)*, Dec 2013.
[38] 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.*, March 2015.
[39] 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/IFIP Network Operations and Management Symposium (NOMS)*, 2016.
[40] B. Turan, S. Ucar, S. Coleri Ergen, and O. Ozkasap, "Dual Channel Visible Light Communications for Enhanced Vehicular Connectivity," *Vehicular Networking Conference (VNC), IEEE*, 2015.
[41] 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.
[42] L. Wu, Z. Zhang, J. Dang, and H. Liu, "Adaptive Modulation Schemes for Visible Light Communications," *Journal of Lightwave Technology*, Jan. 2015.
[43] 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.
[44] S. H. Lee, S. Y. Jung, and J. K. Kwon, "Modulation and coding for dimmable visible light communication," *IEEE Communications Magazine*, Feb. 2015.
[45] S. Ishihara, R. V. Rabsatt, and M. Gerla, "Improving reliability of platooning control messages using radio and visible light hybrid communication," in *Vehicular Networking Conference (VNC), IEEE*, Dec 2015.
[46] 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 *IEEE 12th Annual Conference on Wireless On-demand Network Systems and Services (WONS)*, Jan. 2016.
[47] 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.
[48] 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.
[49] A. Mostafa and L. Lampe, "Physical-layer security for indoor visible light communications," in *Communications (ICC), IEEE International Conference on*, June 2014.
[50] 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.
[51] "IEEE 802.11p-VLC Simulation Platform," https://goo.gl/VCHzRo.
[52] S. Ucar, S. C. Ergen, and O. Ozkasap, "Data-driven abnormal behavior detection for autonomous platoon," in *IEEE Vehicular Networking Conference (VNC)*, Nov 2017.
[53] J. R. Douceur, *The Sybil Attack*. Springer Berlin Heidelberg, 2002.
[54] C. A. Kerrache, C. T. Calafate, J. C. Cano, N. Lagraa, and P. Manzoni, "Trust Management for Vehicular Networks: An Adversary-Oriented Overview," *IEEE Access*, 2016.
[55] M. Feiri, J. Petit, and F. Kargl, "Evaluation of congestion-based certificate omission in VANETs," in *IEEE Vehicular Networking Conference (VNC)*, Nov 2012.
[56] L. Xiao and F. Gao, "Practical String Stability of Platoon of Adaptive Cruise Control Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, Dec 2011.
[57] 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.
[58] P. Seiler, A. Pant, and K. Hedrick, "Disturbance propagation in vehicle strings," *IEEE Transactions on Automatic Control*, Oct. 2004.
[59] 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.
[60] M. R. Jovanovic and B. Bamieh, "On the ill-posedness of certain vehicular platoon control problems," *IEEE Transactions on Automatic Control*, Sept 2005.
[61] D. Jia and D. Ngoduy, "Platoon based cooperative driving model with consideration of realistic inter-vehicle communication," *Transportation Research Part C: Emerging Technologies*, 2016.
[62] 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.
[63] D. R. Stinson, "Cryptography: Theory and Practice," *CRC Press*, 2006.
[64] U. M. Maurer and S. Wolf, "The relationship between breaking the diffie–hellman protocol and computing discrete logarithms," *SIAM Journal on Computing*, 1999.
[65] P. Trimintzios and G. Georgiou, "WiFi and WiMAX Secure Deployments," *Journal of Computer Systems, Networks, and Communications*, 2010.
[66] S. Woo, H. J. Jo, I. S. Kim, and D. H. Lee, "A Practical Security Architecture for In-Vehicle CAN-FD," *IEEE Transactions on Intelligent Transportation Systems*, Aug 2016.
[67] "SAE J3016. Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles," http://standards.sae.org/j3016_201609/.
[68] "VEhicular NeTwork Open Simulator (VENTOS)," http://goo.gl/OueFkO.
[69] "Simulation of Urban MObility (SUMO)," http://sumo.sourceforge.net/.
[70] "OMNET++ Networ Simulator," https://omnetpp.org/.
[71] "Vehicles in Network Simulation (Veins)," http://veins.car2x.org/.
[72] "Crypto++ Library," http://www.cryptopp.com/wiki/Main_Page.
[73] "More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange," https://tools.ietf.org/html/rfc3526.