A Security Protocol for Vehicle Platoon Verification Using Optical Camera Communications

Michael Plattner, Erik Sonnleitner, and Gerald Ostermayer, *Member, IEEE*

***Abstract*— In autonomous vehicle platooning, members of the platoon not only use their own sensor data for making driving decisions. They also rely on data shared by other members of the platoon. This article proposes a security protocol to verify the established communication link between two vehicles driving in succession. Optical camera communications (OCC) via modulated taillights of the leading vehicle and a front-facing camera of the follower is utilized to transmit a verification key. In the footage of the receiving camera, both the transmitted verification key and the transmitting vehicle are visible and can be associated. If the car in front is able to transmit a valid verification key, the platoon can be built. In this article, a comprehensive evaluation of vehicular OCC is presented. The system is tested in different configurations on public roads with various environmental conditions. This platoon verification mechanism takes less than 10 seconds, even in challenging conditions, e.g., in rain, darkness, or low sun. The experiments demonstrate that modern vehicles are equipped with all hardware components required to implement this OCC system by using the built-in front camera of a Tesla Model 3 as receiver without any modifications.**

***Index Terms*— Security protocol, vehicle-to-vehicle (V2V), optical camera communications (OCC), platooning.**

I. Introduction

AUTONOMOUS vehicle platooning requires the member vehicles of the platoon to communicate with each other to exchange time-sensitive and safety-critical data [1]. The individual driving behavior of the platoon members is replaced by cooperative behavior and driving decisions of the entire platoon. Platoon members can decelerate and accelerate simultaneously. This allows to reduce the safety distance between the platoon members. Energy efficiency is increased by driving in the slipstream of the platoon leader, by making the traffic flow transient, and by optimizing the use of the road capacity [2].

It is crucial to verify the used vehicle-to-vehicle (V2V) communication link before building or joining a platoon. Otherwise, it might happen, unintentionally or by manipulation of a malicious third party, that two vehicles are communicating with each other that are not actually driving in direct succession. This can lead to hazardous situations. The security protocol presented in this article allows to verify that two communicating vehicles are driving behind each other by utilizing OCC. The taillights of the leading car are modulated to transmit a signal, the follower uses a front-facing camera installed behind the windshield to receive the data. This V2V-OCC channel acts as an out-of-band channel for the main radio frequency (RF) communication link. By transmitting a verification key via V2V-OCC, the identity of the leading car can be verified. The camera footage shows the transmitted data as well as its origin. This allows to associate the verification key and the transmitting vehicle even if multiple cars are visible in the camera footage. The security protocol presented in this article shows how this attribute can be utilized to protect the platoon communication from attackers outside the platoon. V2V-OCC is only used to verify the V2V-RF communication link; the security protocol and the exchange of actual payload data still relies on RF communications.

A. Contributions

The key contributions of this article are the following:

- A security protocol is developed to establish and verify a fast and secure communication link between members of a vehicle platoon without the need of a trusted certificate authority (CA).
- A V2V-OCC system is proposed and evaluated in public road scenarios in various environmental conditions and configurations.
- It is demonstrated that modern vehicles are already equipped with all the required hardware components for V2V-OCC.

B. Outline

This article is organized as follows: Section II gives an overview of the state-of-the-art by summarizing related work. Section III describes the methodology of the proposed V2V-OCC system in detail. In section IV, a security protocol is defined to use V2V-OCC for vehicle platoon verification. The experimental setup is explained in section V. Section VI evaluates the results of test drives on public roads. The article is concluded in section VII.

II. Related Work

This section summarizes related concepts briefly. The proposed system realizes an application of OCC for vehicle platoon verification.

Manuscript received 5 October 2023; revised 1 February 2024 and 3 April 2024; accepted 10 April 2024. The Associate Editor for this article was S. Kumari. *(Corresponding author: Michael Plattner.)*

Michael Plattner and Erik Sonnleitner are with the Department of Smart and Interconnected Living, University of Applied Sciences Upper Austria, 4232 Hagenberg, Austria (e-mail: michael.plattner@fh-hagenberg.at; erik.sonnleitner@fh-hagenberg.at).

Gerald Ostermayer is with the Research Group Networks and Mobility, University of Applied Sciences Upper Austria, 4232 Hagenberg, Austria (e-mail: gerald.ostermayer@fh-hagenberg.at).

Digital Object Identifier 10.1109/TITS.2024.3390393

A. Vehicle Platoon Verification

In autonomous vehicle platooning scenarios, driving decisions of members of the platoon are not only based on measurements of their own sensors. Additional data is gathered through V2V communication between the platoon members. This requires the autonomous vehicles to trust the data received from members in front. In literature, diverse concepts to verify the order of platoon members can be found.

Studer et al. [3] propose to measure the time-of-flight of broadcasting beacons transmitted via dedicated short range communication (DSRC). This enables them to verify the members of the convoy and their order.

Lai et al. [4] developed a security protocol for platoon-based vehicular cyber-physical systems using road-side units (RSUs) for performing access authentication with vehicles in the platoon.

Han et al. [5] use the unique attributes of road surfaces to verify that two cars are driving in succession. They utilize an accelerometer to measure and correlate vertical acceleration over time influenced by bumps and cracks.

The approach by Vaas et al. [6] compares past and intended trajectories of vehicles to match potential members of a platoon. Past trajectories are tracked using gyroscopes to identify turns.

Xu et al. [7] evaluate a proof-of-following scheme by recording the received signal strength of ambient mobile communication base stations. The large-scale fading effect is utilized as a common source of randomness to create unique but correlating fingerprints to verify the distance between candidate and verifier.

Wiggle by Dickey et al. [8] is a physical challenge-response verification mechanism for platoon verification. A candidate is following the verifier. The verifier transmits randomly-generated checkpoints, i.e., following distances, to the candidate. The candidate has to reach these following distances within a defined time frame. The verifier keeps track of the distance to the vehicle behind using radar.

Another approach in the literature for verifying the communication link with the vehicle in front involves the use of camera-based license plate recognition (LPR). In this scenario, the following vehicle F reads the rear license plate of the leading vehicle L, and a trusted CA verifies whether the public key $pubk_L$ used by the leading vehicle is associated with its license plate lp_L. F needs to be provided with $pubk_L$ and the associated certificate before a communication link can be established. Andreica and Groza [9] proposed the use of identity-based cryptography from LPR for secure V2V communication. Identity-based cryptography enables the generation of a public key from the identity of a participant, such as a phone number, email address, or license plate. To achieve this, an external trusted entity called private key generator (PKG) is necessary, which holds the master private key $privk_m$ and the master public key $pubk_m$. L requests its private key $privk_L$ from the PKG based on its identity, i.e., lp_L. The PKG generates $privk_L$ using $privk_m$ and lp_L. All potential communication participants need to know $pubk_m$. F uses its front camera to read lp_L and generate $pubk_L$ using lp_L and $pubk_m$. After all participants are provided with their private keys and know $pubk_m$, no additional communication with the PKG is needed.

Rowan et al. [10] proposed a session key establishment protocol for V2V communications utilizing a blockchain public key infrastructure alongside visual and acoustic side-channels.

B. Optical Camera Communications

OCC is a subset of visible light communications (VLC). VLC uses light sources as transmitters whose primary purpose is illumination or signaling. VLC in vehicular applications often uses headlights, taillights, street lamps or traffic lights for vehicle-to-everything (V2X) communication. On the receiving side, VLC systems often use photodiode-based receivers, e.g., [11], [12], and [13]. This kind of system allows high sampling rates resulting in high data throughput. However, the immense amount of noise, i.e., other uncontrolled light sources, might be challenging.

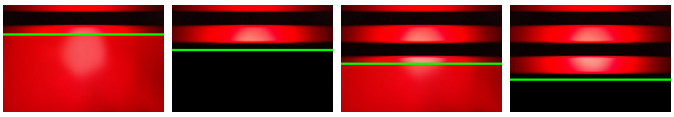
In contrast, OCC systems are using cameras as receivers for VLC. Cameras have a large field-of-view and are additionally capturing images. This makes it possible to filter most of the interfering noise by simply cropping the region of interest showing the modulated light source used to transmit the signal. OCC systems often have lower data rates because common complementary metal–oxide–semiconductor (CMOS) cameras usually use frame rates between 30 and 60 frames per second (FPS). To match the high data throughput of photodioide-based VLC, some papers propose to use high-speed cameras as receivers, e.g., [14] and [15]. Takai et al. [16] even developed a novel image sensor that combines the attributes of cameras and photodiodes for VLC.

Focusing on OCC systems using CMOS image sensors for V2X applications, it is usually possible to transmit one bit per captured frame and per individually modulated light source using on-off keying, e.g., demonstrated in [17] and [18]. Obviously, systems with such a low data rate cannot be used to transmit time-sensitive and safety-critical data in traffic. However, the receiving camera not only captures the data transmitted by the modulated light sources, but it also captures their position. In a V2V-OCC system, where the taillights of a car are used to transmit data, the camera is able to receive the message and associate it with the car that transmitted it [19].

There are papers proposing OCC systems that manage to transmit multiple bits per captured frame and modulated light source by either using an LED array or by exploiting the rolling shutter effect of CMOS cameras. The latter rely on the modulated light source to cover large parts of the camera image. This means it is only feasible for close-up images or indoors with diffuse reflective surfaces. Ziehn et al. [20] proposed a V2V-OCC system that exploits the rolling shutter effect by putting an anisotropic low-pass filter onto the camera lens allowing to transmit multiple bits per frame in a vehicular OCC application at appropriate distances.

III. Methodology

This section introduces the methodology used for the proposed V2V-OCC system including the OCC concept, the modulation scheme, and how to resolve challenges.



(a) LED on. (b) LED off. (c) On again. (d) Off again.

Fig. 1. Stripe pattern occurs when capturing a flickering LED with a rolling shutter camera [22].

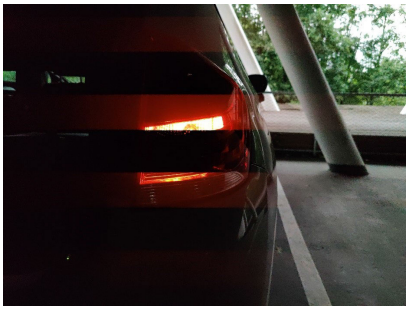


Fig. 2. Close-up photo of a modulated taillight [19].

This article proposes a security protocol for vehicle platoon verification that utilizes V2V-OCC as an out-of-band channel to transmit a verification key. The presented V2V-OCC system solely relies on hardware components that are already built into modern cars. LED taillights are used to transmit a signal, which can be received by front-facing cameras that are usually installed for advanced driver assistance systems (ADAS) like lane keeping assist systems or traffic sign recognition.

A. Taillight Modulation

Vehicle manufacturers often use pulse width modulation (PWM) to dim the perceived brightness of LED taillights. If the signal frequency of the modulation signal is above the flicker fusion threshold of 60 Hz [21], the intermittent light stimulus appears steady to the human eye. However, a camera recording the modulated light source using short exposure time is capable of capturing the distinct states. If the camera uses a rolling shutter, a stripe pattern appears in the image because the LED changes its state while being captured by the camera [22]. Fig. 1 shows close-up images of a flickering LED captured by a rolling shutter camera from top to bottom using short exposure time. The horizontal green line marks the row that is currently captured by the camera. The state of the LED changes during the process. In the final image, a horizontal stripe pattern emerges. The same effect can be observed in Fig. 2. It depicts an LED taillight modulated using a 120 Hz square wave signal that was captured using a smartphone camera with an exposure time of 1/8000 of a second.

On-off keying allows to use this attribute of cameras using short exposure to transmit data without noticeable flickering for the human eye. The modulation method used for the proposed system is undersampled differential phase shift on-off keying (UDPSOOK) [23]. Here, a square wave signal is used with a carrier frequency f_c that is a multiple of the sampling rate f_s of the receiving camera. For a pure square wave signal, the resulting stripe pattern caused by the rolling shutter acts like a standing wave and is identical in every frame. As this stripe pattern is only visible in regions of the image covered by the modulated light source, the LED taillights of a car always show the same state depending on the position inside the image.

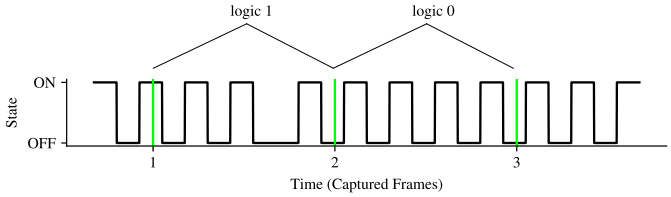


Fig. 3. UDPSOOK modulation signal in original mode [23].

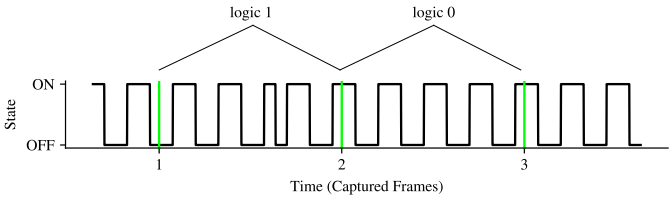


Fig. 4. UDPSOOK modulation signal in $\pi/2$ mode [22].

If a phase shift is applied to the signal, i.e., the signal is inverted, also the stripe pattern is inverted and the state of the taillight changes. The receiving camera is detecting the applied phase shift by analyzing the state of the modulated taillight in every image. If the state changes from one frame to the next, the transmitted bit is a 1, otherwise a 0 is received. Fig. 3 shows the UDPSOOK modulation signal as proposed by Liu et al. [23] with $f_c = 4 \cdot f_s$.

1) Flicker Mitigation: Even if a modulated LED with a frequency of 120 Hz or more appears uniform, the inversion of the signal causes a significant, albeit brief, change in the pulse width ratio (PWR). This results in slight brightness differences that might be perceived as flickering. To mitigate this effect, the phase shifts are applied in the middle of a pulse as shown in Fig. 4 resulting in a steady transition for the human eye [22].

2) Pulse Width Ratio: During communication it might happen that the receiving camera captures the modulated taillight while a transition from ON to OFF or vice versa happens. This results in ambiguous states of the modulated taillight causing bit errors. If the modulation signal uses a PWR of 50%, bright phases of the LED taillight are dominant because of blooming and exposure effects. Ambiguous states of the taillight cannot be prevented using UDPSOOK modulation but using a PWR of less than 50% reduces bit errors significantly [22]. The proposed V2V-OCC system yields the best results using a PWR of 49%.

3) Synchronization: The carrier frequency f_c must be a multiple of the receiving cameras sampling rate f_s. Not all cameras are recording with the same f_s. This means the transmitter needs to be provided with f_s of the intended receiving camera to adjust the modulation signal accordingly. However, such an OCC system is non-synchronized. This means, the modulation signal and the relative sampling position might drift. In a theoretical scenario, where f_c exactly matches $4 \cdot f_s$, it might happen that in every captured frame, the edge of the modulation signal, i.e., a state transition of the taillight, is sampled. This results in a very high error rate because every frame would show ambiguous taillight states. This is why signal drifting, which is inevitable in such a system, is not that bad. Nevertheless, the better the synchronization of transmitter and receiver, the lower the BER, but there is some tolerance [24].

(a) Frame N. (b) Frame N+1. (c) Frame N+2.

Fig. 5. Decoding example for V2V-OCC.

For optimal results, the transmitting system should not just be provided with the nominal sampling rate of the receiving camera but rather an accurately measured value for f_s.

Additionally, in the proposed system, the modulation signal of the left and right taillight is slightly shifted. This helps to reduce the probability of an error burst caused by ambiguous states occurring on both taillights at the same time [25].

B. Vehicle Tracking

The following car uses a front-facing camera to receive the data transmitted by the modulated LED taillights of the leading car. The leading car and its taillights need to be detected and tracked in the recorded camera footage. In bright scenarios, the proposed V2V-OCC system relies on the MobileNet single shot multibox detector (SSD) [26] to detect vehicles in the footage. Detected cars are then tracked using a MOSSE tracker [27]. After every 20th frame, the MobileNet SSD is run again to detect cars. The newly detected cars are associated with the previously tracked cars considering the intersection-over-union (IOU) ratio of the respective bounding boxes. Based on the bounding box of the detected car in front, a region of interest (ROI) is cropped for the left and the right taillight to decode the signal.

In dark scenarios, e.g., at night or in a tunnel, the footage might be too dark for the MobileNet SSD to detect vehicles. In this case, a fallback algorithm is used to track the transmitting vehicle. In the dark, only the taillights of the car in front are visible when using short exposure time. If a car is transmitting data using UDPSOOK modulation, the states of the modulated LED taillights change many times when looking at multiple consecutively captures frames. The positions of the taillights in the frame hardly change when following each other. By calculating the cumulative difference of multiple frames, modulated taillights can be detected. If two areas with big cumulative difference at the same vertical position with reasonable distance between them are present in the footage, the transmitting vehicle can be detected. This approach would even work in bright environments, but it is more error prone than using MobileNet SSD.

There are far more sophisticated approaches to object tracking. However, the simple task of tracking the vehicle in front while driving on a highway can be solved sufficiently using the described algorithms. The tracking algorithm can be exchanged in future versions of this V2V-OCC system, many modern vehicles are already capable of detecting other vehicles nearby.

C. Decoding

Phase shifts applied during the modulation process induce changes in the taillight states captured in camera footage. As illustrated in Fig. 5, three consecutive images recorded by a receiving camera demonstrate these changes. The states of the left and right taillights transition from Fig. 5a to Fig. 5b, resulting in the reception of two logic 1's. Subsequently, from Fig. 5b to Fig. 5c, the state of the left taillight remains unchanged while the right taillight state alters. Consequently, a logic 0 and a logic 1 are received, resulting in the bit string "1101".

TABLE I
DECODING MODEL

Layer	Kernel	Stride	Activation	Output Size
Input	–	–	–	$28 \times 28 \times (3 \text{ or } 9)$
Conv.	5×5	1	ReLU	$28 \times 28 \times 6$
Conv.	5×5	2	ReLU	$14 \times 14 \times 12$
Conv.	4×4	2	ReLU	$7 \times 7 \times 24$
Flatten	–	–	–	1176
Dense	–	–	ReLU	200
Dense	–	–	Softmax	2

To decode the signal, every recorded camera frame needs to be analyzed to see if the state of the modulated LED taillight has changed. This is done using a convolutional neural network (CNN) model. Two versions of this model are trained using 60,000 labelled images of taillights.

One version is trained to classify the state of the currently shown taillight. The input layer of this version of the CNN expects a 28×28 image with three color channels. To decode the transmitted data, the state of the taillight in two consecutively captured frames needs to be classified. If the states are different, a 1 is decoded, otherwise a 0.

The second version of the CNN model takes two successively captured images as input and classifies whether the taillight states shown are the same or not. Again, the size of the input layer is 28×28, but with 9 channels—3 color channels for each of the two images and an additional 3 channels for the pre-processed pixel-based difference of the two images. In this case, the output of the model directly provides the probabilities that the decoded bit is a 1 or a 0.

Table I shows details about the CNN model. The model is identical for both versions, except for the number of channels of the input layer. Both versions are trained with the same images—version 1 with 60,000 single images, version 2 with 30,000 image pairs.

D. Channel Coding

In the proposed system, a verification key is periodically transmitted from the leading vehicle to the following vehicle. Both taillights of the leading vehicle are modulated. The most efficient way to encode a message in such a system is to alternate the bits of the transmitted code word between the left and right taillight. For example, the left taillight transmits odd bit indices, and the right taillight transmits even bit indices. After transmitting an entire code word, the bits are exchanged, with the left taillight transmitting the even bits and the right taillight transmitting the odd bits. In this way, the entire code word can be received within one transmission period by combining the data from both taillights. If the data from one of the taillights is incorrect, the entire code word can still be received within two consecutive periods by considering only the other taillight.

To detect and correct bit errors in the transmission, this V2V-OCC system uses Reed-Solomon (RS) error

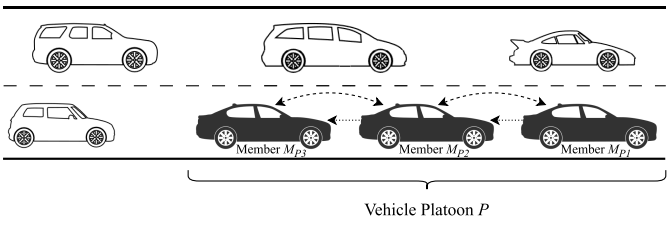


Fig. 6. A platoon of three vehicles in black with uninvolved other vehicles in white.

correction [28]. The optimal amount of redundancy to detect and correct errors depends on the raw bit error rate (BER) of the transmission. As shown in [25], the BER in a V2V-OCC system depends on various environmental conditions, e.g., distance, weather, road type, etc. To optimize such a system, the ideal code rate for the present environmental conditions could be estimated by the receiving vehicle using sensors, e.g., camera, rain sensor, radar. This estimation process is not in the scope of this article.

IV. Security Protocol

The general security protocol of the proposed vehicle platooning verification methodology is depicted in Fig. 8. The protocol focuses on a single platooning segment consisting of only two vehicles (the follower and the leader) but can be similarly applied to longer platoons if verification is done in a pairwise manner across the entire platoon. Fig. 6 depicts a platoon P of length 3, where the platoon member M_{P2} is the follower F of the platoon segment with M_{P1}, but the leader L in the platoon segment with M_{P3}. RF communication links are depicted with dashed arrows, V2V-OCC with dotted arrows.

Fig. 7 depicts a system module block diagram illustrating the setup for two vehicles forming a platoon segment. While the prerequisites for each participating vehicle may slightly differ, as V2V-OCC communication in this proposal is unidirectional, both vehicles should generally adhere to the displayed system component requirements. Components that are unused in a single platoon segment are depicted in gray. However, if not all of the following hardware requirements are met, a particular configuration would only allow a vehicle to either lead *or* follow, limiting the platoon size to only two vehicles:

- Platooning control unit,
- RF transceiver unit,
- V2V-OCC receiver unit (i.e., camera – required for follower), and
- V2V-OCC transmitter unit (i.e., modulated taillights – required for leader).

The security protocol is designed to use RF communication to establish a cryptographically secure channel, which then allows to distinctly verify the leading vehicle by transmitting a verification key via V2V-OCC. The general structure is divided into multiple phases:

1) *Initialization phase*, required for algorithmic setup (via RF): The platooning request is initiated by the follower F and sent to the leader L. In order to establish a cryptographic channel, the channel initiator (follower) includes a list of possible asymmetric encryption as well as hashing

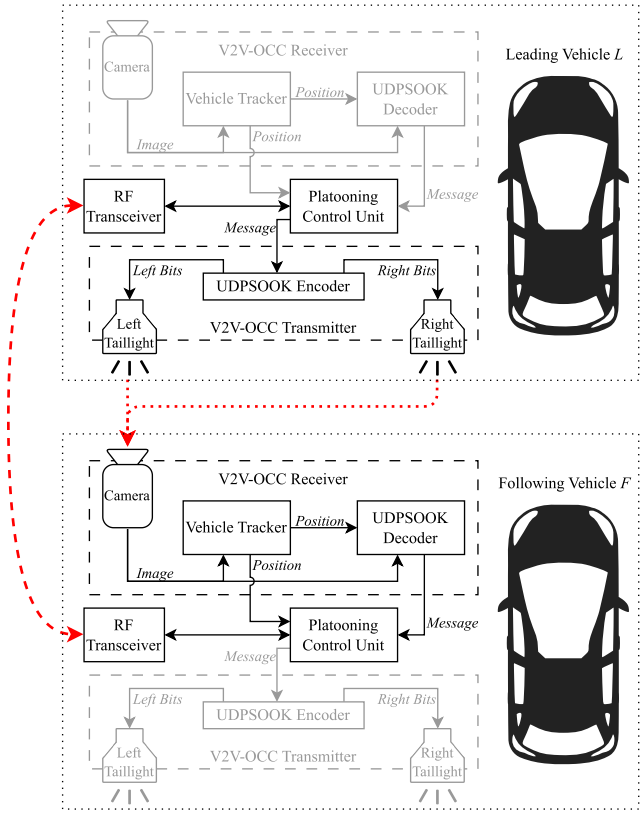


Fig. 7. System module block diagram.

algorithms, loosely similar to the initial protocol workflow in TLS [29], whereas the responder (leader) is allowed to choose a particular set of algorithms to be used for further communication. This message may also include additional formal requirements and restrictions, e.g., the minimum allowed asymmetric key length or the bitvector size of the chosen hash algorithm, if applicable. F and L now have agreed on the cryptographic algorithms used for the RF communication and are set to establish an encrypted communication link.

2) *Key pair creation and exchange* (via RF): Both vehicles independently create ephemeral public-key pairs. F starts by sending its public key $pubk_F$ as well as a nonce n_1 to F. L then signs n_1 by encrypting it with its own private key $privk_L$, and subsequently sends its public key $pubk_L$, the signed nonce sign($privk_L, n_1$) together with a newly created nonce n_2. Once the message is received by F, the signature of n_1 can be verified with the leader's public key $pubk_L$. F and L have now exchanged their public keys and F knows that L also possesses the matching private key $privk_L$.
3) *Frame rate and nonce transmission* (via RF): F requests the camera frame rate and the optimal code rate for the current environmental conditions from its V2V-OCC receiver module, which are both required for establishing the OCC channel. It then signs the previously received nonce n_2 with its private key $privk_F$, and creates a third and final nonce n_3 which is encrypted with the public key of the leader $pubk_L$ before transmitting frame rate, code rate, the signed nonce sign($privk_F, n_2$) and the encrypted nonce enc($pubk_L, n_3$) to L. L verifies the signed n_2 value

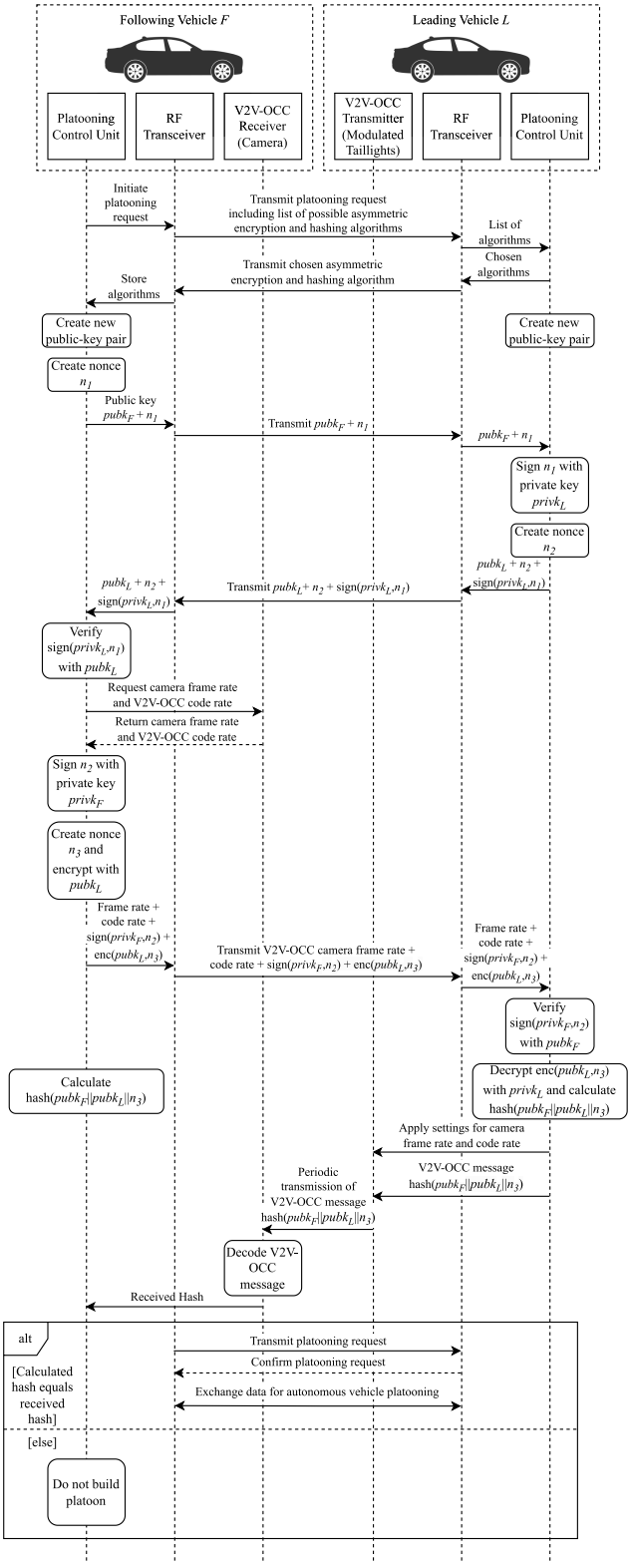


Fig. 8. Security protocol.

with $pubk_F$ and decrypts n_3 with $privk_L$. L now knows that F possesses the matching private key $privk_F$ and the first encrypted message containing n_3 has been transmitted.

4) *Hash transmission and verification* (via V2V-OCC): F and L both calculate the hash value of a string which concatenates both public keys and the decrypted n_3. The resulting hash value is then periodically retransmitted using the leader's V2V-OCC transmitter module. The follower's V2V-OCC receiver module, i.e., the front-facing camera, decodes the transmitted hash value using the recorded footage. Additionally, the transmitting vehicle L is visible in the same footage. So, it can be checked if L is really the car driving in front of F.
5) *Verification decision*: F compares the calculated hash value to the data received via V2V-OCC. Only if both values match and the transmitting car is driving in front of F, verification has been successful. F and L have now established an encrypted RF communication link that can be used to exchange safety-critical data for autonomous vehicle platooning.

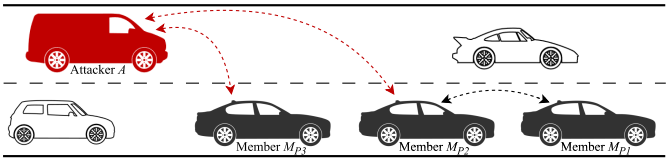
While a deeper technical discussion on cryptographic primitives is arguably out of scope regarding our proposal, the suggested security protocol is not based on or reliant on any particular set of cryptographic algorithms and hence follows an agnostic approach. Any modern type of asymmetric (public-key) algorithm which supports encryption and digital signatures, e.g., RSA or ElGamal, represents a functional alternative for the protocol sequence.

A. Threat Model

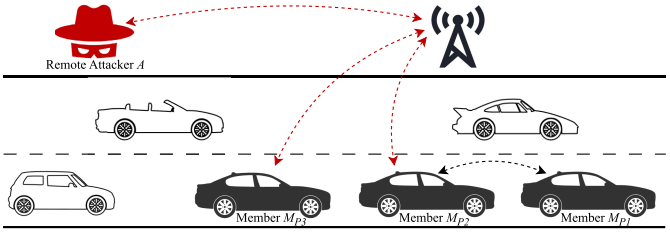
In general, modern asymmetric cryptography allows secure communication between all participants of a platoon. One of the major imposed threats our proposed protocol aims to solve is the *spoofing* or *impersonation* of vehicles with malicious intent, i.e., an attacker which is in RF proximity pretends to drive in front of a victim. Fig. 9 sketches two scenarios where attacker A is hijacking a platoon. Members M_{P2} and M_{P3} think they are getting data from each other, but instead A is injecting RF messages into the platoon. This potential threat should generally be resolved by our proposed V2V-OCC verification method, due to the fact that V2V-OCC essentially enforces a 2$^{\text{nd}}$-factor proximity-based visual platoon vehicle authentication system, before actual payload data is being exchanged via RF channels and therefore drastically limits the potential attack surface which would allow such attacks in the first place.

Another attack targeted towards the initialization phase of the protocol is commonly referred to as *downgrading attack* [29], in which an attacker tries to weaken the cryptographic communication to such a state that it can potentially be broken: Within the legitimate protocol workflow, the initiator is forced to only provide weak cryptographic algorithms and/or key sizes, such that the responder is not able to select a sufficiently secure cipher suite and hence continues with insecure or broken algorithms. Similar to TLS, this can be circumvented by periodically reassessing approved algorithms and the current state of algorithmic vulnerabilities.

As for most communications, replay attacks pose a threat in multiple scenarios by recording the RF transmission of messages (which may or may not be encrypted and hence directly readable by an attacker). In cryptographic protocols, replay attacks are typically countered by introducing ephemeral random numbers (nonces) which are only used



(a) Following-afar adversary.



(b) Remote adversary.

Fig. 9. Attack scenarios that can be prevent using the proposed security model, based on [8].

once before being discarded. Our proposed system introduces nonces n_1 and n_2 during the key pair creation and exchange phase to ensure a) that the mutual communication partners indeed have access to the corresponding private key data of the previously exchanged public keys, and b) to ensure that messages which have been recorded and replayed in the past can be identified as such and hence abort the platooning request. The particular use of nonces is loosely based on the Needham-Schroeder protocol [30].

The most critical protocol segment is the transmission and verification of the V2V-OCC data, which the general platooning decision is based on. All previous phases, due to the fact only RF is used, may also lead to a positive outcome even though the communicating vehicles are not driving in a consecutive sequence. For this reason, we decided to extend the cryptographic parameters to the V2V-OCC phase: L can only transmit the correct V2V-OCC message if it is able to decrypt n_3 and if the transmitted hash value is based on the public keys of both vehicles. This should eliminate the feasibility of an attacker introducing malicious public keys, or claiming to possess the private key which belongs to L.

B. Limitations

A major limitation of the proposed protocol can be seen in a scenario, where an attacking vehicle A is placed between the benign leader L and follower F, i.e., a platoon segment consisting of three cars as shown in Fig. 10. L and F participate in legitimate RF communication while a malicious car A is driving in between. Although A does not have access to cryptographic keys created and used by F and L, the attacker can visually observe the V2V-OCC message ultimately sent by L and immediately transmit it without modification to the vehicle F behind. In such a scenario, F would then think it established an encrypted RF communication link with A instead of L. It would not be possible for A to inject or manipulate RF messages but the inconsistent data from communication and own sensors of F might result in confusion and hazardous situations and the platoon must be dissolved.

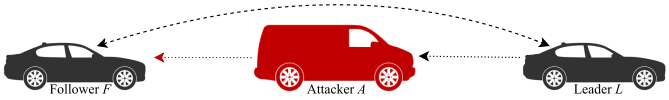


Fig. 10. V2V-OCC relay attack.

In order to prevent attacks that incorporate the hijacking of vehicle sequences, the platoon verification would have to be done in a bidirectional manner, i.e., not only the leader verifies itself as such, but also the follower. However, relying solely on the V2V-OCC method may not be sufficient, as attackers could easily spoof messages in both directions, similar to the scenario depicted above. Possible solutions could be proposals discussed by Dickey et al. [8] where the identity of the other vehicle is verified by using physical challenge-response verification. Another solution could be to extend the security protocol to exchange visual attributes of the communicating vehicles, e.g., license plate, car model, or paint color. These attributes could then be matched using the camera footage.

V. Experimental Setup

This section describes the experimental setup used to gather the evaluation data. The system was tested in a comprehensive experiment while driving approximately 900 km on public roads in Austria.

A. Receiver

For receiving the signal, a common CMOS camera can be used. This article evaluates the V2V-OCC system using two different types of cameras.

1) External Camera: The first one is a DJI Osmo Action[1] camera mounted on the inside of the following car's windshield using a suction cup mount. The camera is set to record videos with 30 FPS and with a fixed exposure time of 1/8000 of a second and an ISO of 3200. The short exposure time is necessary to receive the signal resulting in dark images. Thus, a high sensitivity of the sensor is needed. The carrier frequency f_c of the modulation signal is set to 120 Hz. This is the main camera used for the evaluated test drives for approximately 800 km.

2) Tesla Camera: The second camera used to receive the signal is the built-in front-facing camera of a Tesla Model 3 (model year 2022, Gigafactory Shanghai, China). The *Dashcam*[2] feature is used to store the video footage onto a thumb drive plugged into the USB port inside the glove box of the car. The Tesla camera is used without any modifications. The sampling rate f_s of this camera is 36 FPS. Thus, the carrier frequency f_c of the modulation signal is set to 144 Hz. This camera was used to prove that built-in cameras of modern consumer cars are capable of receiving the transmitted signal. Approximately 100 km of test drives have been conducted using the Tesla as the following vehicle.

B. Transmitter

The transmitting vehicle in the experimental setup is a BMW X1 (E84). The halogen light bulbs in the rear light

[1] https://www.dji.com/osmo-action (accessed Apr. 3, 2024)
[2] https://www.tesla.com/ownersmanual/model3 (accessed Apr. 3, 2024)

modules are replaced by LEDs. The LEDs can be modulated using an external controller. The taillights of this prototype car are specifically modified for test drives; however, any LED taillight integrated into a modern vehicle could serve as a transmitter in this system. While PWM is commonly used to adjust the brightness of LED taillights, it needs to be replaced with UDPSOOK modulation for this application. Notably, both modulation approaches exhibit similar effects on images captured using a camera with a short exposure time [31]. Although an additional circuit was utilized to evaluate the presented prototype, vehicle manufacturers should be capable of implementing the proposed modulation to modern LED taillights without additional hardware components.

C. Offline Evaluation

The recorded footage is evaluated offline using a Python script[3] to compare various configurations regarding the vehicle detection and tracking, taillight state classification for decoding the signal, amount of redundancy for RS error correction, etc. The proposed system does not depend on high computing performance. A modern vehicle equipped with computing hardware for ADAS should comfortably handle tracking the transmitting vehicle and decoding the signal in real-time.

VI. Evaluation

This section evaluates performance and applicability of the proposed V2V-OCC system in various conditions and configurations in public road scenarios. The data for this evaluation was recorded in multiple test drives. Only data points on highways are considered where the following car directly follows the transmitting prototype vehicle at a distance between 20 m and 60 m.

A. Raw Data Transmission

Environmental conditions have a major influence on the performance of an OCC system used outdoors, especially in vehicular applications. To evaluate the raw data transmission performance, the BER within a 10-second time window is measured in various weather conditions. The box plots in Fig. 11 illustrate the distribution of the BER in seven different weather conditions using an external camera as receiver as described in section V-A1. Examples for the camera footage are shown in Fig. 12. For decoding the signal, the two different classifiers described in section III-C are used to either classify single taillight states or to classify state changes of the modulated taillights.

The box plots generally illustrate the influence of weather conditions on such a V2V-OCC system. The results for dry conditions are very good with mean error rates of less than 2%, represented by triangular markers. The bottom plot shows the results for wet conditions. A different scale on the vertical axis must be used to plot BER. For light rain, the results are still comparable to dry conditions, but the heavier the rain, the higher the BER. In wet conditions, the rain itself is not the only challenge to decoding the signal. On wet roads, the vehicle ahead swirls up spray, resulting in even poorer visibility. In addition, windshield wipers are activated and can block the camera's view in individual video frames, causing additional bit errors. An example for such a situations is shown in Fig. 13a.

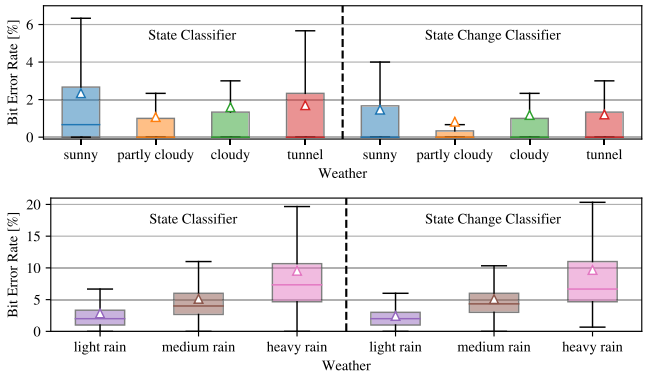


Fig. 11. Bit error rate comparison in various weather conditions.

The results in Fig. 11 also show that the taillight state change classifier gives significantly better results than the decoder with the single state classifier in dry conditions. The direct state change classifier is especially useful in situations where the camera detects ambiguous states of the modulated taillights. Fig. 13b shows an example where the right taillight of the vehicle in front is clearly on, but the left taillight appears to be only half on. In this case, it is difficult to properly classify the state itself, but if a phase shift is applied to the modulation signal, a change in the captured pattern of the taillight might still be detectable.

In wet conditions, there is so much noise in the resulting images that the state change classifier does not offer an advantage over using single state classification. The resulting BER is virtually identical with both types of classifiers. However, the distribution of the bit errors fits the used channel coding better when using single state classification. Thus, this article proposes to use the taillight state change classifier in dry conditions and the taillight state classifier in wet conditions to optimize the relevant performance.

B. Platoon Verification Time

In the proposed security protocol for vehicle platoon verification, the leading vehicle L verifies that it is driving directly in front of the follower F by transmitting a hash value calculated from the two public keys $pubk_F$ and $pubk_L$ and a secret nonce n_3 via the proposed V2V-OCC channel. Besides security, the most important metric to quantify the performance and applicability of the described system is the time the vehicle platoon verification takes. The system only allows to transmit one bit per captured camera frame and per modulated taillight, e.g., with a frame rate of 30 FPS and two modulated taillights a gross throughput of 60 bit/s can be achieved. With such a low data rate, the verification message should be as short as possible to get acceptable platoon verification times. The bitvector size of cryptographic hash algorithms must be at least 256 bits for cryptographic security. Additional redundancy is needed to transmit RS forward error correction data. The calculated hash value is periodically

[3]Source code available at https://github.com/Platti/v2v-occ

(a) Sunny. (b) Partly cloudy. (c) Cloudy. (d) Tunnel.

(e) Light rain. (f) Medium rain. (g) Heavy rain.

Fig. 12. Examples for footage of external camera.

(a) Taillight occluded by windshield wiper. (b) Zoomed image of ambiguous taillight state.

Fig. 13. Examples of error-causing situations.

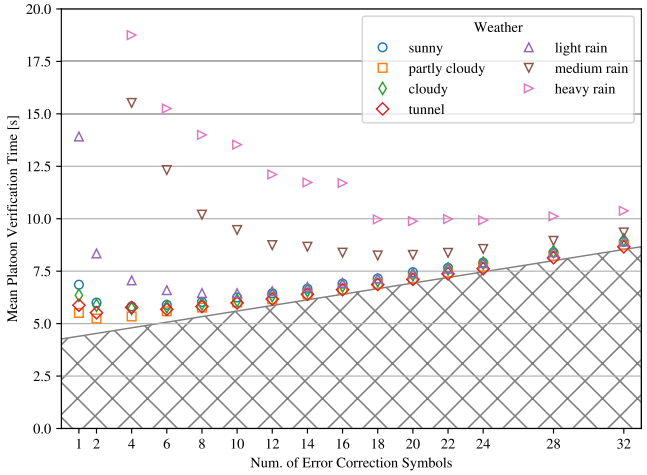


Fig. 14. Mean vehicle platoon verification time.

retransmitted via V2V-OCC. The V2V-OCC receiver of F can decode the signal either by using one period and combining the data from both taillights or by considering two periods from one of the two modulated taillights. If neither of the three options results in the correct code word, the transmission continues until the code word could be decoded successfully. For this evaluation, always the minimum time for the three decoding options is considered. The needed time for the RF communications phases of the presented security protocol is negligible compared to the V2V-OCC phase for transmitting the verification key. Hence, only the V2V-OCC transmission time is considered as the time it takes to verify a platoon.

Fig. 14 shows the mean platoon verification time in different weather situations using various amount of redundancy if the transmission started at an arbitrary point in time of the test drives. In this evaluation, a 256-bit hash value is transmitted. The number of error correction bytes defines the code rate of the channel coding. The size of the code word increases with additional redundancy, the hatched gray area in the chart marks platoon verification times that are impossible to achieve with this system even with error-free transmission. For example, 4 error correction symbols describe an RS(36,32) channel code which has a code word size of 36 bytes and a code rate of 88.9%. This channel code would allow to detect and correct 2 erroneous bytes in the code word and still decode the correct data.

For dry conditions, i.e., sunny, partly cloudy, cloudy or in a tunnel, using 4 error correction symbols leads to the optimal mean platoon verification time of 5.7 seconds at a payload bit rate of 45 bit/s. Using more redundancy results in longer code words without a significant reduction of the error rate. In wet conditions, more bit errors occur when decoding the signal. This means the optimal amount of redundancy to achieve short platoon verification times is higher. The optimum for light rain in the recorded test drives would be to use 8 error correction symbols, i.e., a code rate of 80%. The mean platoon verification time in light rain would be 6.5 seconds at 39 bit/s. For rain with higher intensity, the optimal number of error correction bytes is 20, i.e., a code rate of 61.5%. Despite poor visibility being the primary limiting factor of this V2V-OCC system, a mean platoon verification time of 8.2 seconds at 31 bit/s and 9.9 seconds at 26 bit/s can be achieved for medium and heavy rain, respectively.

The code rate for the V2V-OCC transmission needs to be selected beforehand. This means the optimal amount of redundancy has to be estimated, e.g., by considering the current camera images, rain sensors, brightness sensors, etc.

Some situations during the data transmission might cause error bursts in the data, e.g., ambiguous states of the taillights or inaccurate vehicle tracking. This might result in longer platoon verification times. To depict these potential bad cases, Fig. 15 shows the 95th percentile of the platoon verification times. This means in 95% of the cases, the platoon verification takes less time. For dry conditions and for light rain, the

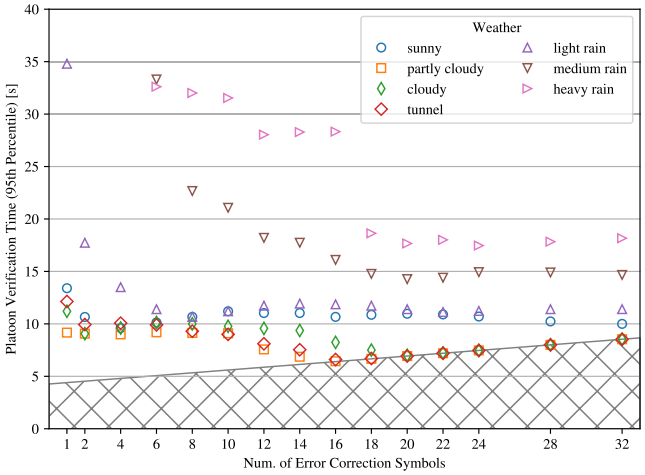


Fig. 15. 95th percentile of vehicle platoon verification time.

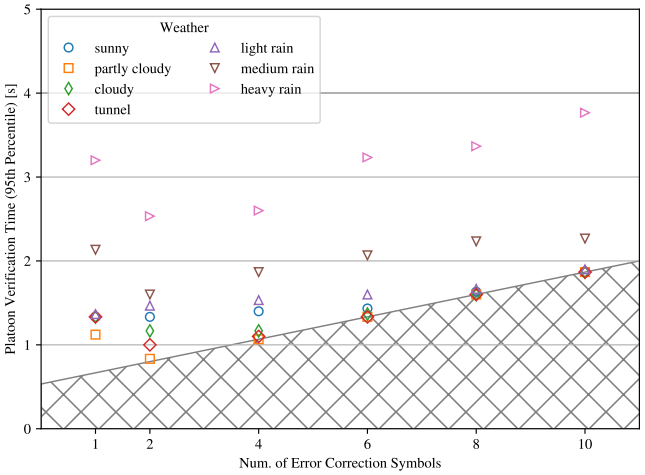


Fig. 16. 95th percentile of accelerated vehicle platoon verification time.

respective chosen amount of redundancy would lead to platoon verification times of less than 10 seconds. For medium rain and heavy rain, the platoon verification time would be less than 14 seconds and less than 18 seconds, respectively.

C. Accelerated Platoon Verification

Platoon verification time of 10 seconds might sound long but this process is only necessary before building a platoon. After this platoon verification process, the two vehicles can exchange time-sensitive and safety-critical data via a low-latency verified encrypted communication link and follow each other in a platoon for many kilometers. If the following vehicle is using adaptive cruise control (ACC) during the verification process, the passengers would barely notice the delay.

However, there are options to further improve the platoon verification time. The V2V-OCC receiver in this evaluation only records at 30 FPS. If a camera with higher sampling rate is used, the data rate increases proportionally. For example, when using a camera with a frame rate of 60 FPS, the platoon verification time could be halved.

Another option to accelerate the platoon verification would be to transmit a shorter verification key. In the previous evaluation, cryptographic security of the used hash algorithm is mandatory. However, the hashed data only contains the two public keys used for encryption in the main RF channel that are public by definition and an ephemeral secret nonce that is only used once. A potential attacker does not achieve anything by breaking the transmitted hash. Ignoring the cryptographic attributes of the used hash algorithm, a much shorter verification code can be transmitted. This verification code would only be a checksum for the established communication link.

Fig. 16 depicts the 95th percentile of the platoon verification time if a 32-bit verification key would be used. The system transmits this verification key successfully within less than 1.6 seconds in 95% of the cases in all evaluated conditions except for heavy rain with a mean of less than 1 second. In heavy rain, the 95th percentile is 2.6 seconds. These are again results of using a camera with 30 FPS. Of course, such a shorter verification key could also be combined with a faster

(a) Low sun. (b) Rain.

Fig. 17. Examples for footage of Tesla camera.

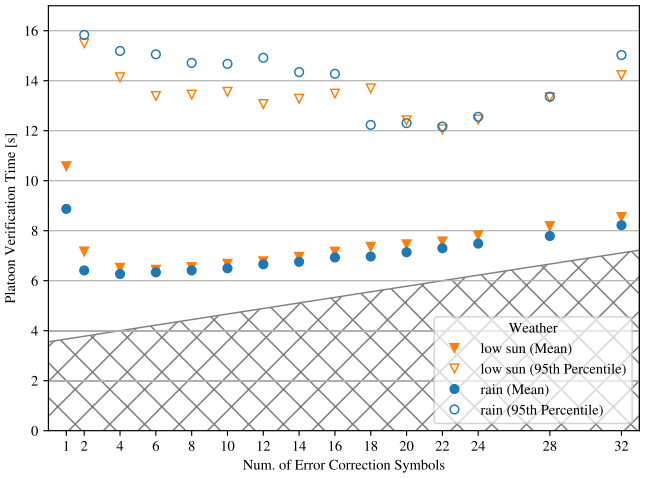


Fig. 18. Vehicle platoon verification time using Tesla camera.

camera. This would easily lead to verification times of less than 1 second for a platoon.

D. Evaluation Using Built-in Tesla Camera

The experiments for the previous evaluation have all been conducted using an external camera for receiving the V2V-OCC signal as described in section V-A1. This article also demonstrates that any CMOS camera can be used as a V2V-OCC receiver, even the ones that are already built into modern consumer vehicles without any modification.

The following evaluated results are recorded using the built-in camera of a Tesla Model 3 as described in section V-A2. The respective test drives are carried out under particularly difficult conditions, in low sun and rain.

Example images for the recorded footage in those conditions are depicted in Fig. 17. It is noticeable that the overall brightness of the images is the same in both conditions, even though the ambient brightness is much higher in sunlight. The Tesla camera strives to always keep the overall brightness of the image at a medium level. Nevertheless, the exposure time is very short even in darker environments. The main reason for this is to reduce motion blur. This is advantageous for the proposed V2V-OCC system, since a short exposure time is required for its operation.

Fig. 18 evaluates potential platoon verification times using a Tesla camera recording 36 FPS as receiver while transmitting a 256-bit hash value for verification. With optimal redundancy, the mean platoon verification time is just over 6 seconds at a payload bit rate of 41 bit/s for low sun and in rain. The system performs particularly well in rainy conditions due to the automated brightness adjustments of the camera while keeping the exposure time low. Additionally, the camera is mounted at the top center of the windshield close to the glass. This results in clear images with good contrast to receive the signal even in such challenging conditions.

VII. Conclusion

V2V communication is a vital part of autonomous vehicle platooning. Verifying this communication link is crucial, as the platoon members rely on the shared data of other member vehicles to make driving decisions. The proposed security protocol intends to establish an encrypted RF communication link between two following vehicles and verify it by transmitting a verification key via V2V-OCC. Modulated taillights of the leading vehicle are used as transmitters, a front-facing camera of the following vehicle receives the signal. The following vehicle is able to use the camera footage to associate the transmitted data with the transmitting vehicle. Thus, it can be verified that the RF communication link is established with the car in front and the car in front possesses valid cryptographic keys. The frequency of the modulation signal is within a spectrum where only cameras using short exposure are able to capture distinct states of the taillights. The flickering is not perceivable by the human eye, thus other traffic participants are not affected.

The main benefit of this platoon verification mechanism is that an attacker outside of the platoon is not able to pretend to be a platoon member and hence it is not possible to inject malicious messages into the RF communication of the platoon. In comparison to alternative approaches for verifying the V2V communication link, such as utilizing LPR [9], the proposed platoon verification process offers several advantages:

- Unlike approaches involving CAs or PKGs for identity-based cryptography, the proposed platoon verification process does not necessitate a trusted third-party.
- The cameras employed in the presented experiments are well-suited for OCC. However, at typical following distances, the license plates of other vehicles may not be readable due to insufficient resolution, as observed in Fig. 12 and Fig. 17.
- The proposed protocol incorporates perfect forward secrecy, enhancing the communication security.

It is demonstrated that V2V-OCC can be used to transmit the verification key in less than 10 seconds, even in challenging conditions, e.g., rain, low sun, darkness. Comparable mechanisms, e.g., [4], [5], [6], [7], and [8], typically require a minimum of 10 seconds and often extend to more than a minute. If line-of-sight is interrupted within these 10 seconds, e.g., when the transmitting vehicle exits the camera frame or is obscured by another vehicle that cut in between the two communicating vehicles, the platoon verification process is designed to fail. Consequently, no platoon should be established under such circumstances.

Modern vehicles are already equipped with the necessary hardware components for V2V-OCC. This is shown by testing the V2V-OCC system on public roads with an external camera and a built-in Tesla camera as receiver. The implementation of such a V2V-OCC system would be cost efficient for vehicle manufacturers.

Future Work

A potential vulnerability of this security protocol is that an attacker could eavesdrop and relay the V2V-OCC communication. This results in the follower believing to communicate with a benign leading vehicle directly in front via RF, but an attacker is driving between the two communicating vehicles. The attacker would not be able to manipulate the RF communication because they do not know the valid cryptographic keys. To prevent such an attack, the security protocol could be extended to additionally exchange information about visual attributes of the benign leader, e.g., license plate, car model, or paint color. The follower could match the transmitted attributes with the attributes recognized in the camera footage. This extension could be part of future research.

The presented article also evaluates the optimal code rate of the channel coding used for V2V-OCC. If the code rate is selected statically, the platoon verification time might not be as short as possible in all driving conditions. Future research might investigate models to estimate the best code rate for the current conditions before starting the transmission of the verification key via V2C-OCC.

References

[1] C. Bergenhem, S. Shladover, E. Coelingh, C. Englund, and S. Tsugawa, "Overview of platooning systems," in *Proc. 19th ITS World Congr.*, 2012, pp. 1–8.

[2] S. Tsugawa, S. Jeschke, and S. E. Shladover, "A review of truck platooning projects for energy savings," *IEEE Trans. Intell. Veh.*, vol. 1, no. 1, pp. 68–77, Mar. 2016.

[3] A. Studer, M. Luk, and A. Perrig, "Efficient mechanisms to provide convoy member and vehicle sequence authentication in vanets," in *Proc. 3rd Int. Conf. Secur. Privacy Commun. Netw. Workshops*, 2007, pp. 422–432.

[4] C. Lai, R. Lu, and D. Zheng, "SPGS: A secure and privacy-preserving group setup framework for platoon-based vehicular cyber-physical systems," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3854–3867, Nov. 2016.

[5] J. Han, M. Harishankar, X. Wang, A. J. Chung, and P. Tague, "Convoy: Physical context verification for vehicle platoon admission," in *Proc. 18th Int. Workshop Mobile Comput. Syst. Appl.*, Feb. 2017, pp. 73–78.

[6] C. Vaas, M. Juuti, N. Asokan, and I. Martinovic, "Get in line: Ongoing co-presence verification of a vehicle formation based on driving trajectories," in *Proc. IEEE Eur. Symp. Secur. Privacy*, Apr. 2018, pp. 199–213.

[7] Z. Xu, J. Li, Y. Pan, L. Lazos, M. Li, and N. Ghose, "PoF: Proof-of-following for vehicle platoons," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2022, pp. 1–7.

[8] C. Dickey et al., "Wiggle: Physical challenge-response verification of vehicle platooning," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2023, pp. 54–60.

[9] T. Andreica and B. Groza, "Secure V2V communication with identity-based cryptography from license plate recognition," in *Proc. 6th Int. Conf. Internet Things, Syst., Manage. Secur. (IOTSMS)*, Oct. 2019, pp. 366–373.

[10] S. Rowan, M. Clear, M. Gerla, M. Huggard, and C. Mc Goldrick, "Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels," 2017, *arXiv:1704.02553*.

[11] M. Schettler, A. Memedi, and F. Dressler, "The chosen one: Combating VLC interference in platooning using matrix headlights," in *Proc. IEEE Veh. Netw. Conf. (VNC)*. Washington, DC, USA: Combat, Dec. 2019, pp. 1–4.

[12] B. Turan, S. Ucar, S. C. Ergen, and O. Ozkasap, "Dual channel visible light communications for enhanced vehicular connectivity," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Dec. 2015, pp. 84–87.

[13] W.-H. Shen and H.-M. Tsai, "Testing vehicle-to-vehicle visible light communications in real-world driving scenarios," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Nov. 2017, pp. 187–194.

[14] S. Nishimoto et al., "Overlay coding for road-to-vehicle visible light communication using LED array and high-speed camera," in *Proc. 14th Int. IEEE Conf. Intell. Transp. Syst. (ITSC)*, Oct. 2011, pp. 1704–1709.

[15] T. Yamazato et al., "Image-sensor-based visible light communication for automotive applications," *IEEE Commun. Mag.*, vol. 52, no. 7, pp. 88–97, Jul. 2014.

[16] I. Takai, S. Ito, K. Yasutomi, K. Kagawa, M. Andoh, and S. Kawahito, "LED and CMOS image sensor based optical wireless communication system for automotive applications," *IEEE Photon. J.*, vol. 5, no. 5, Oct. 2013, Art. no. 6801418.

[17] P. Ji, H.-M. Tsai, C. Wang, and F. Liu, "Vehicular visible light communications with LED taillight and rolling shutter camera," in *Proc. IEEE 79th Veh. Technol. Conf.*, May 2014, pp. 1–6.

[18] E. Eso, A. Burton, N. B. Hassan, M. M. Abadi, Z. Ghassemlooy, and S. Zvanovec, "Experimental investigation of the effects of fog on optical camera-based VLC for a vehicular environment," in *Proc. 15th Int. Conf. Telecommun. (ConTEL)*, Jul. 2019, pp. 1–5.

[19] M. Plattner and G. Ostermayer, "Camera-based vehicle-to-vehicle visible light communication–A software-only solution for vehicle manufacturers," in *Proc. 32nd Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2023, pp. 1–7.

[20] J. R. Ziehn, M. Roschani, M. Ruf, D. Bruestle, J. Beyerer, and M. Helmer, "Imaging vehicle-to-vehicle communication using visible light," *Adv. Opt. Technol.*, vol. 9, no. 6, pp. 339–348, Dec. 2020.

[21] S. Hecht and S. Shlaer, "Intermittent stimulation by light: V. The relation between intensity and critical frequency for different parts of the spectrum," *J. Gen. Physiol.*, vol. 19, no. 6, pp. 965–977, 1936.

[22] M. Plattner and G. Ostermayer, "Undersampled differential phase shift on–off keying for visible light vehicle-to-vehicle communication," *Appl. Sci.*, vol. 11, no. 5, p. 2195, Mar. 2021.

[23] N. Liu, J. Cheng, and J. F. Holzman, "Undersampled differential phase shift on-off keying for optical camera communications," *J. Commun. Inf. Netw.*, vol. 2, no. 4, pp. 47–56, Dec. 2017.

[24] M. Plattner and G. Ostermayer, "A visible light vehicle-to-vehicle communication system using modulated taillights," in *Proc. 12th Int. Conf. Adapt. Self-Adaptive Syst. Appl.*, 2020, pp. 7–12.

[25] M. Plattner and G. Ostermayer, "A camera-based vehicular visible light communication system using modulated taillights in public road scenarios," *Veh. Commun.*, vol. 43, Oct. 2023, Art. no. 100651.

[26] A. G. Howard et al., "MobileNets: Efficient convolutional neural networks for mobile vision applications," 2017, *arXiv:1704.04861*.

[27] D. S. Bolme, J. R. Beveridge, B. A. Draper, and Y. M. Lui, "Visual object tracking using adaptive correlation filters," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, Jun. 2010, pp. 2544–2550.

[28] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *J. Soc. Ind. Appl. Math.*, vol. 8, no. 2, pp. 300–304, Jun. 1960.

[29] T. Dierks and E. Rescorla, "The transport layer security (TLS) protocol version 1.2," RFC 5246, Aug. 2008, p. 104, doi: 10.17487/RFC5246.

[30] W. Stalling, *Cryptography and Network Security: Principles and Practice*. Prentice-Hall, 1995.

[31] M. Plattner and G. Ostermayer, "Vehicle-to-vehicle optical camera communications for platoon verification," in *Proc. Wireless Commun. Netw. Conf.*, 2024.

Michael Plattner received the B.Sc. and M.Sc. degrees in mobile computing from the University of Applied Sciences Upper Austria, Hagenberg, Austria, in 2017 and 2019, respectively. He is currently pursuing the Ph.D. degree with the Institute for Communications Engineering and RF-Systems, Johannes Kepler University Linz, Austria. Since 2019, he has been an Assistant Professor with the University of Applied Sciences Upper Austria. His research interests include optical camera communications, automotive computing, vehicular communications (vehicle-to-vehicle and vehicle-to-infrastructure), automated driving, and traffic simulation.

Erik Sonnleitner received the Ph.D. degree in computer science from Johannes Kepler University Linz, Austria, in 2013. He is currently a Professor of secure mobile systems with the University of Applied Sciences Upper Austria, Hagenberg, Austria. His research interests include mobile and network security and distributed ledger systems.

Gerald Ostermayer (Member, IEEE) received the Dipl.-Ing. and Ph.D. degrees in communications engineering from Vienna University of Technology, Vienna, Austria, in 1992 and 1998, respectively. He was a Research and Teaching Assistant with the Applied Electronics Laboratory, where he worked in the field of wireless sensing using code-division multiple-access methods. In 1997, he joined Siemens, where he was responsible for several projects in the field of radio resource management (RRM) algorithms and network simulation issues for UMTS. Since 2005, he has been with the University of Applied Sciences Upper Austria, Hagenberg, Austria where he heads the Degree Program "Automotive Computing" and the Research Group Networks and Mobility. He has authored or coauthored around 80 technical papers in the fields of wireless sensing, mobile communications, and mobile and automotive computing in international conferences and journals. He holds seven patents in the field of mobile communications and wireless sensing. He is an Associate Editor of IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS.