As per UGC guidelines an electronic bar code is provided to secure your paper

International Journal for Modern Trends in Science and Technology
Volume 11, Issue 07, pages 162-171
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol11issue07.html
DOI: https://doi.org/10.5281/zenodo.16130961

Vehicle to Vehicle Optical Camera Communications for Platoon Verification

M. Ravi, A. Charan Sai, P. Ramu Yadav, N. Nickypeterson

Department of Electronics and Communication Engineering, Andhra Loyola Institute of Engineering and Technology, Vijayawada, India.

To Cite this Article
M. Ravi, A. Charan Sai, P. Ramu Yadav & N. Nickypeterson (2025). Vehicle to Vehicle Optical Camera Communications for Platoon Verification. International Journal for Modern Trends in Science and Technology, 11(07), 162-171. https://doi.org/10.5281/zenodo.16130961

Article Info
Received: 14 May 2025; Accepted: 06 July 2025.; Published: 17 July 2025.

Copyright © The Authors ; This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

KEYWORDS

communication protocols, Raspberry Pi Pico, Transceiver (Esp-01), Text Communication, Wireless Communication, Hardware.

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 the 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.

1. 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 us 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 us 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.

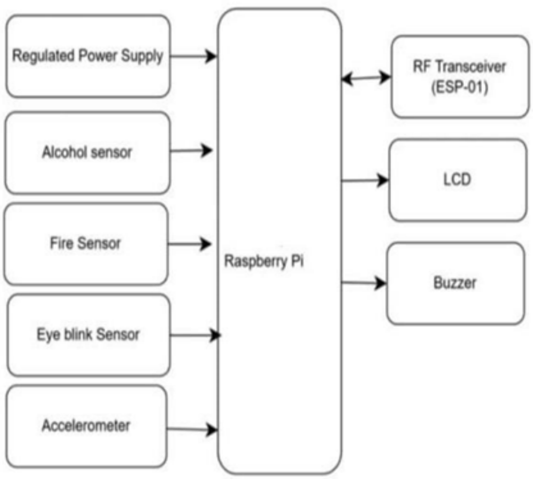


Fig: Block Diagram

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.

2. Related Work:

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

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 pubkl used by the leading vehicle is associated with its license plate lpL . F needs to be provided with pubkL 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 privkm and the master public key pubkm . L requests its private key privkL from the PKG based on its identity, i.e., lpL . The PKG generates privkL using privkm and lpL . All potential communication participants need to know pubkm . F uses its front camera to read lpL and generate pubkL using lpL and pubkm . After all participants are provided with their private keys and know pubkm , 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.

3. 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.

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 60Hz [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]. 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. It depicts an LED taillight modulated using a 120Hz square wave signal that was captured using a smartphone camera with an exposure time of 1/8000 of a second.

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, three consecutive images recorded by a receiving camera demonstrate these changes. The states of the left and right taillights transition, resulting in the reception of two logic 1's. Subsequently, 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".

4. Security Protocol:

The general security protocol of the proposed vehicle platooning verification methodology is depicted. 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. Depicts a platoon P of length 3, where the platoon member MP2 is the follower F of the platoon segment with MP1 , but the leader L in the platoon segment with MP3. RF communication links are depicted with dashed arrows, V2V-OCC with dotted arrows.

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 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 pubkF as well as a nonce n1 to F. L then signs n1 by encrypting it with its own private key privkL , and subsequently sends its public key pubkL , the signed nonce sign(privkL,n1) together with a newly created nonce n2 . Once the message is received by F, the signature of n1 can be verified with the leader's public key pubkL . F and L have now exchanged their public keys and F knows that L also possesses the matching private key privkL.

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 n2 with its private key privkF , and creates a third and final nonce n3 which is encrypted with the public key of the leader pubkL before transmitting frame rate, code rate, the signed nonce sign(privkF,n2) and the encrypted nonce enc(pubkL,n3) to L. L verifies the signed n2 value with pubkF and decrypts n3 with privkL . L now knows that F possesses the matching private key privkF and the first encrypted message containing n3 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 n3 . 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. sketches two scenarios where attacker A is hijacking a platoon. Members MP2 and MP3 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 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.

B. Limitations

A major limitation of the proposed protocol can be seen in a scenario, where n attacking vehicle A is placed between the benign leader L and follower F, i.e., a platoon segment consisting of three cars 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.

5.A.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 900km on public roads in Austria.

B.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 Action1 camera mounted on the inside of the following car’s windshield using a suction cup mount. The camera is set to record videos with 30FPS 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 fc of the modulation signal is set to 120Hz. This is the main camera used for the evaluated test drives for approximately 800km.

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 Dashcam2 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 fs of this camera is 36FPS. Thus, the carrier frequency fc of the modulation signal is set to 144Hz. This camera was used to prove that built-in cameras of modern consumer cars are capable of receiving the transmitted signal.

Approximately 100km 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 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 script3 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.

6. 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 20m and 60m.

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. Illustrate the distribution of the BER in seven different weather conditions using an external camera as receiver as described in Section V- A1. 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.

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 pubkF and pubkL and a secret nonce n3 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 30FPS and two modulated taillights a gross throughput of 60bit/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 256bits for cryptographic security. Additional redundancy is needed to transmit RS forward error correction data. The calculated hash value is periodically 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.

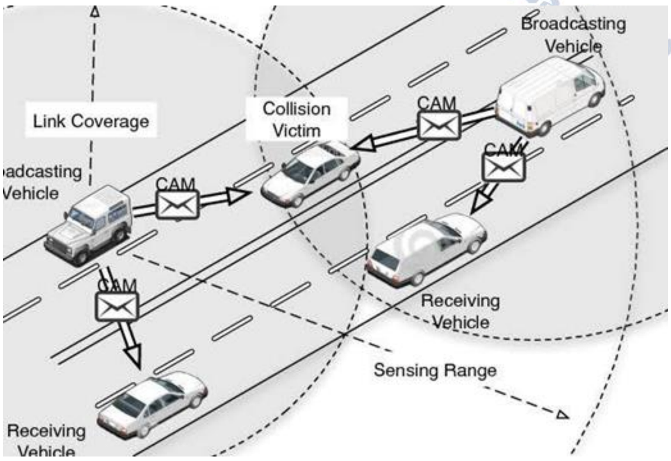
C.Accelerated Platoon Verification:

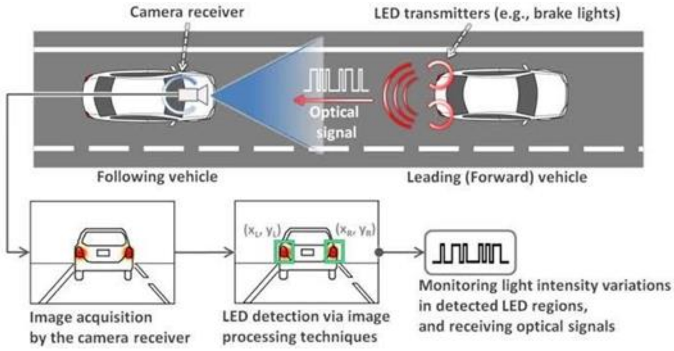
Platoon verification time of 10 seconds might sound long but this process is only necessary before building a platoon. After this platoon verification process, the two vehicles can exchange time-sensitive and safety-critical data via a low- latency verified encrypted communication link and follow each 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 30FPS. 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 60FPS, 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.

7. Result:





8. 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 transmittinga 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.

• 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.

A. 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.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

References

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

[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", Proc. 3rd Int. Conf. Secur. Privacy Commun. Netw. Workshops, pp. 422-432, 2007.

[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", Proc. 18th Int. Workshop Mobile Comput. Syst. Appl., pp. 73-78, Feb. 2017.

[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", Proc. IEEE Eur. Symp. Secur. Privacy, pp. 199-213, Apr. 2018.

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

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

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

[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", arXiv:1704.02553, 2017.

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

[12] B. Turan, S. Ucar, S. C. Ergen and O. Ozkasap, "Dual channel visible light communications for enhanced vehicular connectivity", Proc. IEEE Veh. Netw. Conf. (VNC), pp. 84-87, Dec. 2015.
[13] 13.W.-H. Shen and H.-M. Tsai, "Testing vehicle-to-vehicle visible light communications in real-world driving scenarios", Proc. IEEE Veh. Netw. Conf. (VNC), pp. 187-194, Nov. 2017.
[14] S. Nishimoto et al., "Overlay coding for road-to-vehicle visible light communication using LED array and high-speed camera", Proc. 14th Int. IEEE Conf. Intell. Transp. Syst. (ITSC), pp. 1704-1709, Oct. 2011.
[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.

International Journal for Modern Trends in Science and Technology
IJMTST