Towards Secure Communication for High-Density Longitudinal Platooning

Markus Sontowski, Stefan Köpsell, Thorsten Strufe
Chair for Privacy & Security, TU Dresden
Dresden, Germany
{first.last}@tu-dresden.de

Christian Zimmermann
Corporate Research, Robert Bosch GmbH
Renningen, Germany
christian.zimmermann3@de.bosch.com

Andreas Weinand, Hans D. Schotten
Institute for Wireless Communication and Navigation, TU Kaiserslautern
Kaiserslautern, Germany
{weinand, schotten}@eit.uni-kl.de

Norbert Bißmeyer
ESCRYPT GmbH
Bochum, Germany
Norbert.Bissmeyer@escrypt.com

***Abstract*—Using V2X communication in platoons promises benefits regarding energy efficiency and fleet management. It is also a safety critical process with the potential to cause dangers to life and limb which needs to be secured against attackers. We propose two protocols for secure platoon communication and provide a comparative analysis of those protocols.**

***Index Terms*—Intelligent Transport Systems, High-Density Longitudinal Platooning, 5G, Data Security, Platooning Security Architecture**

I. Introduction

In 2016, the transportation sector was responsible for 33% of energy consumption in the European Union and 31.6% of greenhouse gas emissions. Road transportation alone was accountable for 82% of transportation energy consumption and 72% of greenhouse gas emission [1]. One technology envisioned to improve energy efficiency in heavy duty road transportation is High-Density Longitudinal Platooning (HDLP). In HDLP multiple trucks travel with short distances between them with the objective of reducing aerodynamic drag [2] and therefore achieve energy savings of up to 20% [3]. HDPL requires tight coordination of vehicles, which can be achieved by the usage of Cooperative Adaptive Cruise Control (CACC). CACC is similar to Adaptive Cruise Control (ACC) which uses sensors like cameras, radar and lidar to perceive vehicles in the vicinity and determine, e.g., distance to vehicles ahead. Additionally, CACC involves wireless communicating with nearby entities such as other vehicles or Road Side Units (RSUs). In our work we focus on 3GPP and IEEE/ITS based technologies for V2X communication, i.e., assisted (4G/5G network assisted sidelink) or non-assisted (4G/5G ad-hoc sidelink, IEEE 802.11p) direct communication. Owing to the introduction of cooperative communication and driving systems, new threats to safety, security and privacy arise. In this paper, we give an overview on data security and data protection challenges in HDLP and propose two protocols for securing platoon communication.

The paper is organized as follows. Section II discusses related work. Section III describes the life-cycle of a platoon and security aspects. In Section IV we propose a general security architecture and two specific security concepts. Section V concludes the paper.

II. Related Work

In the following, we provide an overview on existing work, both scientific and standards, covering platoon management and security.

A. Platoon Management

Logistic companies plan their vehicles' routes precisely to utilize their resources optimally. In addition to traditional route management, platoon booking, the process of finding suitable platoons for a vehicle to join, needs to be integrated into the planning process to optimally utilize platoon functionality.

Bhoopalam et al. [4] give an overview of planning in their survey and describe a platoon booking and forming environment. They describe three booking situations. In scheduled platoon planning, planning and creation of platoons is done before the start of the trips (static planning). In real-time platooning, trips are announced shortly before the start, or en route (dynamic planning). In opportunistic platooning, vehicles meet on the road where they can spontaneously join or form a platoon (ad-hoc platooning).

Ad-hoc platooning is also considered in [5]–[7]. However, Bhoopalam et al. note that ad-hoc platooning will play a minor role due to its limitation regarding finding optimal platoons.

In this paper we only address (static) planning and leave ad-hoc platooning to future work.

B. Security in HDLP

In the area of Vehicular Ad Hoc Networks (VANETs), a variety of publications address security issues [8]–[13]. However, work focusing especially on the issues in HDLP is, at the time of writing, still very recent and limited.

Amoozadeh et al. [14] investigate different string stability insider attacks in a platoon with a Platoon Leader (PLL), such as falsification, radio jamming, and tampering attacks, on

978-1-7281-1220-6/19/$31.00 ©2019 IEEE

vehicles equipped with CACC. They propose several solutions such as plausibility checking, majority vote, or downgrading to ACC. Dadras et al. [15] describe an insider attack on string stability during maintaining of the platoon. The attacker causes oscillation in a platoon, i.e., members need to decelerate or accelerate more often. Hence, the benefit of energy efficiency is lost and crashes can be provoked. As a solution the authors propose platoon management rules. Gerdes et al. [16] also consider an insider attack on the efficiency of the system during maintaining of the platoon. They assume a mixed platoon (trucks and, e.g., passenger cars). They state that their attack leads to an efficiency loss of 20-300% by strategical slowing down and speeding up. DeBruhl et al. [17] propose mitigation against insider attacks by vehicles in the platoon. They present a modeling based solution, in which, based on normal behavior, a model of each member is created and as soon as a member's actions deviate from this model the safety distance is increased so driving with ACC is viable. Asplund [18] analyzed six different insider attacks on the membership protocol during joining of a platoon. They propose to use neighbor identity verification, message consistency check and Sybil detection to mitigate these attacks. Petrillo et al. [19] consider Denial-of-Service (DoS), spoofing, message alteration and burst transmission attacks from insiders. They proposed a control strategy mixed with a voting technique to mitigate the addressed attacks.

All of these prior works focus on a scenario with a PLL and primarily consider insider attackers. Furthermore, we are not aware of any holistic security architecture covering the entire HDLP scenario.

C. Standards

On standardization side different actions are already taken in the direction of security and data protection in Intelligent Transport Systems (ITS).

ETSI describes a general ITS architecture [20] and a specific Security Architectures [21]–[23]. In the EU C-ITS Certificate Policy [24], a trust model based on a Public Key Infrastructure (PKI) is defined. It refers to ETSI specifications and describes legal and technical requirements for the management of public key certificates for C-ITS applications. The EU C-ITS Security Policy [25] defines different security levels for ITS message types and information on the number of certificates to be stored.

ETSI ITS and C-ITS focus mainly on Cooperative Awareness Messages (CAMs), which contain information about vehicles such as position, heading, speed, driving direction and vehicle ID. They consider a different security architecture than we do, due to a different scenario (VANET) in which public broadcast is the prevalent communication mode.

In HDLP a different message type is needed due to more detailed requirements such as breaking power and weight. Furthermore, additional information about the platoon needs to be communicated such as platoon ID, desired platoon ID or platoon length. Requirements on the security architecture are also different due to a different setup.

III. Platoon Life-Cycle and System Model

In the following, we describe our platoon system model and life-cycle. Subsequently, we briefly introduce our attacker model and identify security requirements for HDLP.

A. Platooning System Model

A vehicle interested and capable to take part in a platoon is a Platooning Candidate (PC). When a PC joins a platoon it becomes a Platoon Member (PLM). A Platoon Management System (PMS) is a control system keeping the state of the platoon and managing local decisions such as initiating joining and leaving of vehicles. It can be cloud-based or contained in a PLM acting as Platoon Leader (PLL). A Platoon Booking Service (PBS) describes a system managing the registration of PCs and creation of platoons.

In this work, we build upon the platooning environment described by Bhoopalam et al. [4]. A HDLP can use broadcast or unicast communication to establish communication between PLMs and a PC wanting to join. Message sizes should be small due to latency and real time requirements.

There are external messages for unicast communication with platoon-external entities (e.g. the PBS) and platoon-internal messages used for communication between PLMs. We assume that the algorithm to control a platoon is based on the one developed within the 5GNetMobil project (https://5g-netmobil.de/). Therefore, every PLM frequently broadcasts a Platooning Control Message (PCM). Each PLM adapts its driving speed based on the received PCMs and its own state. As mentioned earlier, in the C-ITS vehicles are supposed to regularly send CAMs. The constant sending of CAMs poses threats to privacy [26]. In this work we do not focus on CAM-related risk, as this is a general issue of VANETs. However, our goal is that HDLP shall not pose additional privacy and security risks.

B. Platoon-Life-Cycle

A HDLP's life-cycle system can be divided into four stages:

1) Booking: During the booking stage, PCs are coordinated regarding planning of joining and leaving points. Platooning-relevant parameters (e.g. top speed, breaking power, etc.) of PCs can be checked to ensure all platoon specific requirements are satisfied. As a result, PCs have selected a platoon and hold all necessary information (e.g., joining place and time) to join. Booking can be performed in a centralized or decentralized manner. The advantages and disadvantages of this two approaches are out of scope of this paper. For our work we assume a centralized PBS.

2) Joining: If the platoon does not exist yet, it will be created. Parameters communicated in the booking stage are checked by the platoon to ensure the compatibility of PCs with the platoon. A PC will becomes a PLM after finishing the joining procedure.

3) Maintaining: Maintaining the platoon means to keep the HDLP in a platooning-enabled state. Hence, intra-platoon communication is actively used to ensure that platooning parameters such as distance between PLMs ahead are met.

4) Leaving: In this stage, a PLM leaves the HDLP. This can be due to the end of its platooning cycle or due to extraordinary circumstances such as safety-critical situations.

C. Attacker Model

We consider outsiders and insiders and focus on a global, active (modifying) attacker. The attacker is able to listen on all communication links and to manipulate all messages. Further, we consider a well-financed attacker, equipped with state-of-the-art computing power and possibly specialized hardware (e.g. Software Defined Radio (SDR)). Nevertheless, we assume that the attacker is not able to break cryptographic algorithms and protocols widely believed to be secure.

D. Security Requirements

In HDLP, security measures are needed to, among others, guarantee safety, i.e. to protect people, machines and transported commodities. Additionally protecting business secrets is one goal of security as further explained below.

1) Protection Goals: Protection goals describe the properties a system should fulfill in order to mitigate threats with the purpose of reducing risks and damage. Commonly known protection goals are confidentiality, integrity, and availability (CIA). An additional important protection goal considered in this work is accountability.

Confidentiality — Protection of data and information against disclosure to unauthorized parties. The messages shall be protected against outsiders and against the PBS regarding certain information (coordination messages between PLMs). Confidentiality between PLM and PMS regarding messages is not intended as this information is necessary for functionality of the system. PC which are booked for a certain platoon shall be able to read messages which are necessary for joining this platoon.

Integrity of data and information — prevention or at least detection of unauthorized modification. Integrity of intra-platoon messages shall be ensured as well as of data transmitted between PC and the PBS during the booking process.

Availability — The degree of functionality and accessibility of a system, services, data, and information with respect to authorized entities. Messages send between PLMs and PMS shall have a high availability to ensure the safety of the system. Regarding external messages, availability is less important as it does not affect the safety.

Accountability — The sender / recipient cannot challenge that he is the sender / receiver of a given message. The system shall be able to hold PLMs liable for their actions.

Anonymity – Protection of the identity of a participant, such that it "[...] is not identifiable within a set of subjects [...]" [27]. To a certain extend and towards certain entities of the system, PLMs shall be able to not need to expose their real and full identity to take part in the system.

Unlinkability – Different data or information cannot be connected or related to each other even with knowledge before or after observing this information [27]. For instance, a PC should not be able to determine whether it previously performed platooning with its future platoon partners.

2) Conclusion: To protect against above-described attacker importance levels of different protection goals need to be defined. The 5G NetMobil consortium considers integrity, availability and accountability of platoon communication critical to ensure functionality and safety of the HDLP [28]. Platoon-internal messages are broadcasted to all PLMs and, hence, confidentiality is not of importance locally. Further the PMS is allowed to read messages from the platoon. Still, confidentiality against outsiders and other insiders such as the PBS is of high importance. In this work we focused mainly on confidentiality, integrity and unlinkability of data.

Due to constrain on latency and message size, security measures need to be validate against these requirements. Hence, certain protection goals will only be achievable under some constrains. This concerns key sizes and selection of algorithms and methods which are not interfering with the safety of the system.

IV. Concepts for secure HDLP communication

In the following, we introduce and discuss possible protocols for securing communication in HDLP.

A. General Mechanism for Confidentiality and Authenticity

To protect the confidentiality of the PCM, we use symmetric encryption with a key shared among the PLMs. Remember that each PCM is broadcasted to all PLMs. Therefore, confidentially is only important with respect to platoon-external entities.

To address authenticity of the PCM, we identified six different methods:

1) Group symmetric authentication (A1): Each PLM holds the same shared symmetric key. If one PLM leaves the platoon, a new key needs to be negotiated. In case a PC joins the platoon, no action is required. All messages sent within the platoon are verified with this key. Advantages of this method are easy key management, low communication and computation overhead. However, confidential key exchange is required, no accountability and authenticity with respect to individual PLMs is feasible (internal spoofing possible).

2) Individual symmetric authentication (A2): Makes use of multiple (pairwise) symmetric keys for securing the communication in the platoon. Each participant holds $n-1$ symmetric keys, one for communicating with each of the other $n-1$ PLMs. Messages from a given PLM are verified with the key of this PLM. Therefore, the sender has to append $n-1$ Message Authentication Codes (MACs), each MAC generated with one of the $n-1$ keys the sender holds. Here the advantages are an overall better performance compared to asymmetric cryptography and sender authenticity. A drawback is that a confidential key exchange is required. Further, this method does not provide accountability and the high number of keys to manage as well as the high computational/communication overhead is a disadvantage.

3) Group asymmetric signing (A3): All participants hold the same private key and all PLMs know the corresponding public key, which is used to verify all messages. If a PLM leaves the platoon, a new private/public key pair needs to be negotiated. The benefit is that less keys are needed compared to individual key methods A2 and A4. The downside is the higher computational overhead compared to A1, no accountability and no authenticity with respect to individual platoon members (internal spoofing possible).

4) Individual asymmetric signing (A4): Each PLM holds its own private key and all PLMs hold $n-1$ different public keys, one for each of the other $n-1$ PLMs. Messages from a given PLM are verified with the public key of this PLM. The advantages are the possibility of public key exchange and spoofing protection. It is the only solution which offers accountability. Disadvantages are, higher computational overhead compared to A1 and A2, and the high number of keys needed to be managed.

5) Privacy-preserving signatures (Attribute-based (anonymous) credentials, group signatures) (A5): Each participant holds its own private key and all participants can check the validity of messages. The benefits are a privacy-preserving method of proving identity and authorization. Drawbacks are the high computational overhead and large message sizes.

6) Physical layer based authentication (A6): The PHY-layer/channel meta data is analyzed, in order to make decisions about the transmitter of a message [29]. Each PLM needs to calculate $n-1$ statistical models, one for each of the other $n-1$ PLMs. Received messages from a given PLM are verified by checking whether the corresponding meta data is correlated to the meta data acquired in previous transmissions. In case of time varying features (e.g. channel impulse response or received signal strength indicators), the models need to be updated. The advantage is a lower message security overhead compared to A1. However, cryptography is required in the initialization phase and as a probability based approach, wrong decisions are possible.

B. Security Protocols

In the following, we present and compare two approaches towards securing platoon communication. Particularly, we introduce two protocols for key distribution and re-keying, as well as for encrypting platoon communication based on these keys. In both protocols, the goal is to establish one or more common secret key(s) among a group of PLMs. We assume the existence of a credential system, e.g., the C-ITS PKI [24] or a similar system (see Section II-C). Its main purpose is to allow vehicles to prove that they are legitimate PC, e.g., that the candidate fulfills all requirements (technical, regulatory etc.) to participate in a platoon.

In the following we first present the "Diffie-Hellman Key Exchange Platooning Protocol (DKEPP)", which is based on Diffie-Hellman Key Exchange (DHKE) and employs approach (A1) to protect intra-platoon messaging. Subsequently, we present the "Central Key Exchange Platooning Protocol (CKEPP)", which relies on both key distribution executed by a PLL and local key derivation. Further, CKEPP includes regular re-keying in order to support unlinkability of platoon messages and to prevent tracking based on key identifiers. This protocol combines features of approaches (A1) and (A2) to protect intra-platoon communication. Both approaches also rely on certificates and the PKI for certain steps.

1) Diffie-Hellman Key Exchange Platooning Protocol (DKEPP): We assume that the PBS can authenticate its messages using digital signatures that all PCs, and PLMs can verify. Moreover, we require that the communication between a PC/PLM and the PBS is encrypted, e.g. by utilizing (D)TLS.

Remember, that the PBS should not learn the shared secret key used by a given platoon. Rather, the key shall only be available to PLMs.

Based on the four stages defined in the Platoon-Life-Cycle the protocol is established as follows.

a) Booking: In the first step of this stage a PC (V_i) sends all information necessary to form platoons to the PBS (e.g. route, time, truck capabilities etc.). To avoid DoS attacks a PC authenticates this information (e.g. with the help of a digital signature or by showing an anonymous credential), proving that the information is fresh and was sent by an entity which is authorized to become a PLM. In order to simplify the explanation, we assume that this step ends at a well-known time (e.g. x minutes before the platoon should actually be formed).

In the second step platoons are formed based on the collected information. The PBS creates a list of proposed platoons and publishes this list. Thereby, the list is authenticated (e.g. by applying a digital signature) by the PBS, so that each vehicle can verify that the list is fresh and indeed created by the PBS. Each platoon on this list has a unique Platoon ID (P_{ID}). Note that "publishing" could mean that each PC requests the list from the PBS. We assume no permanent connection from the PBS to the PC and no other way for the PBS to push the information to the PC. To add some confidentiality, requesting the list should involve again a prove of being a PC. However, in general the assumption is that the list is indeed public. Therefore, one needs to elaborate what the minimal set of required information is. Only this minimal set of required information will be published on that list (e.g. only route and time per platoon, but not number of vehicles interested in that platoon etc.). In any case the list will not contain assignments of individual trucks to platoons.

Instead this assignment is initiated by a PC in the third step, the platoon booking. In this step all cryptographic material is exchanged which later allows a PC to actually join a platoon. This step can further be subdivided into two phases: first a booking request is issued by a PC. After all booking requests are collected by the PBS, it informs each PC, how many vehicles actually participate in a given platoon.

As stated above DKEPP utilizes an authenticated group key exchange protocol based on the Diffie-Hellman-Key-Agreement protocol such as [30].

A PC V_i which later wants to join a given platoon creates a fresh signature key pair (t_{V_i}, s_{V_i}) (of some digital signature

scheme) and sends a booking request to the PBS. This request contains the P_{ID} and the public signature test key t_{V_i}. Moreover, the request is authenticated by the PC (i.e. the vehicle proves that it is indeed a valid PC). If this is the first request for booking of platoon P_{ID}, the PBS creates and stores the public Diffie-Hellman parameters, i.e. a cyclic group G of prime order q and a generator g of G. The PBS generates a certificate cert_{V_i} containing the public signature test key t_{V_i} and the platoon id P_{ID}. The PBS sends this certificate together with the parameters G and g to the PC.

b) Joining: In this stage the shared secret, used for securing the internal messages, is established among PCs. This stage can be subdivided into two phases. In the first phase, a PC expresses that it wants to join the platoon at this moment. In the second phase information for actually calculating the key is broadcasted among PCs.

In the first phase each PC V_i generates a random secret value $r_i \ni G$ and broadcasts the value $z_i = g^{r_i}$. More specific this message $\text{Sig}(z_i)$ contains the platoon id P_{ID}, the value z_i, and the certificate obtained in the first phase. The whole message is signed by the PC using s_{V_i}. After receiving such a message, each PC verifies the signature and certificate. It stores the value z_i and the certificate in an ordered list (according to the value z_i). At the end of the first phase — i.e. the maximal number of platoon members was reached or after a timeout -– each PC changes its status to PLM and the second phase starts. In this phase each PLM calculates a value $X_i = (\frac{z_{i+1}}{z_{i-1}})^{r_i}$. Note that values z_{i+1} and z_{i-1} are taken form the ordered list (relative to the value z_i). The indices are calculated $\bmod n$, the number of entries in that list (e.g. $z_n = z_0$). Each PLM broadcasts a signed message containing the platoon id P_{ID}, the value X_i, and the index i. After a PLM has received and verified (using the stored certificates) all the values X_i, it calculates the shared key k as follows:

$$k{=}(z_{i-1})^{nr_i} X_i^{n-1} X_{i+1}^{n-2} ... X_{i+n-2}{=}g^{r_1 r_2} * g^{r_2 r_3} * ... * g^{r_n r_1}$$

Figure 1 depicts broadly the different steps in the booking and joining stage of the protocol.

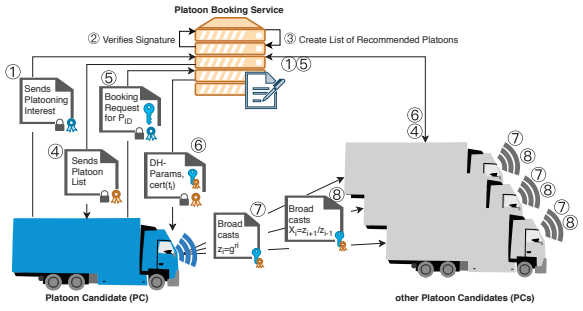

Fig. 1. High-level Overview of DKEPP

c) Maintaining: During platooning, keys can be renewed periodically or randomly, even if the set of PLMs does not change.

If a new PC is requesting to join, a new shared key needs to be created. Therefore, the new PC has to send the value $z_x = g^{r_x}$ (first phase). It will receive the current ordered list of $(\text{Sig}(z_i), \text{cert}_{V_i})$ from one PLM (e.g. the one owning the lowest value of z). Additionally, only PLMs which now have new values for X_i need to send them. The new shared key k' is calculated from these new values as described above.

d) Leaving: If a PLM leaves a new shared key needs to be generated. Thereby only the second phase of the procedure described under "Joining" needs to be executed. Moreover, only the PLMs having a new value X_i need to send it.

2) Central Key Exchange Platooning Protocol (CKEPP): The CKEPP relies on a central PMS for key distribution and uses asymmetric encryption for platoon establishment and joining and symmetric encryption for securing intra-platoon communication.

a) Booking: In CKEPP, PCs receive from a central management system a selected PLL's certificate to enable them to send encrypted messages to the PLL. The keys necessary for platoon communication are then distributed in the joining phase by the PLL as described in the following. The details of the booking and selecting a platoon suited for the PC are omitted here. Figure 2 provides an overview on the approach sans the interactions with the PKI.

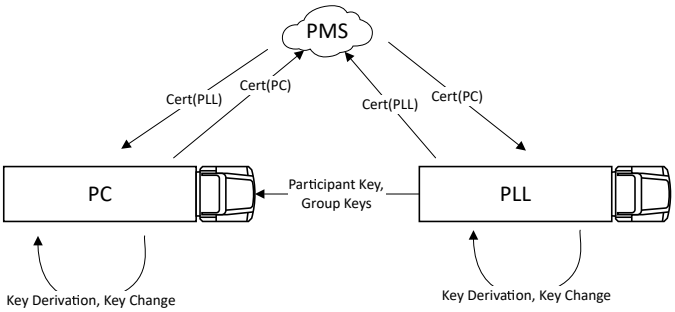

Fig. 2. High-level Overview of CKEPP

b) Joining: In contrast to DKEPP, CKEPP relies on key distribution by the PLL instead of on DHKE. The PMS relays the PC's certificate to the PLL and vice versa. In the wake of this, authorizations encoded in the certificates are checked. After successful certificate exchange, the PLL distributes three keys to the PC. The key distribution is secured using asymmetric encryption utilizing the keys associated with the respective certificates received beforehand from the PMS.

One the one hand, the PLL sends to the PC a symmetric "participant key" to be used exclusively for securing communication between the PLL and the future PLM. On the other hand, the PLL sends two symmetric group keys to the PC, to be used for securing messages to be broadcasted to the whole platoon. The PC confirms key reception by broadcasting a confirmation message encrypted with the first of the two received group keys.

c) Maintaining: During platooning, group keys and participant keys are regularly changed as depicted in Figure 3.

It is assumed that PLMs will have to regularly change their ETSI ITS Authorization Tickets (ATs) [23] and respective identifiers [25]. In CKEPP, re-keying is conducted in line with

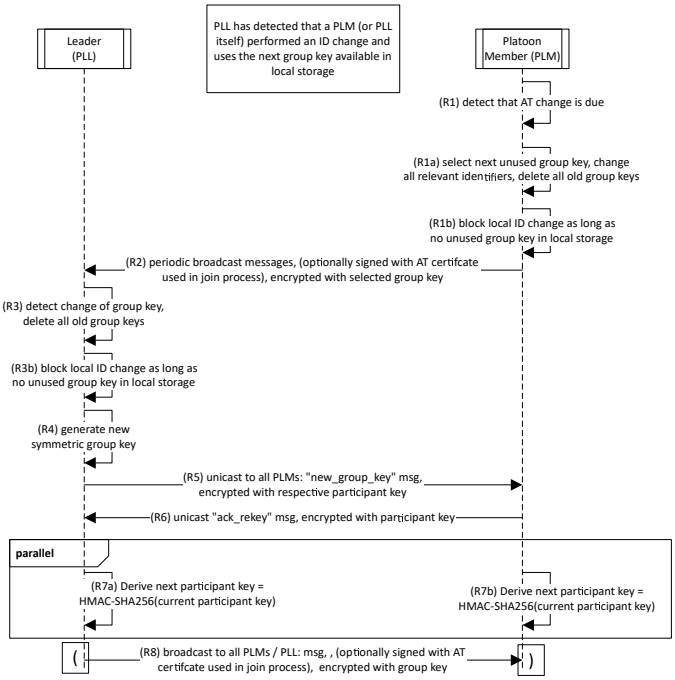

Fig. 3. Re-keying in CKEPP

AT change. When a PLM (or the PLL) is about to change its AT, it notifies the rest of the platoon about the pending change so that AT change can be blocked for all members and no other member will initiate an AT change during re-keying. PLL will then create a new group key which it sends to all members encrypted with their respective participant keys. After confirmation of all participants, PLL will continue broadcasting internal messages using the second group key (while the newly transmitted third group key is stored for use in the next re-keying process). Additionally, all PLMs and the PLL derive new participant keys as depicted in the figure (steps R7a and R7b). Note that re-transmission of ACKs and confirmation of received ACKs are omitted from the sequence diagram.

d) Leaving: If a PLM is about to leave the platoon, it broadcasts its request to leave the platoon to notify all PLMs. In response, the PLL broadcasts a conformation message and waits for the leaving PLM's acknowledgement of the confirmation. Subsequently, the PLL sends a new group key to the remaining PLMs, encrypted individually with the respective participant keys. Finally, an ID change and re-keying is performed to refill the pool of group keys.

C. Comparative Analysis

While the protocols presented here have several similarities they differ in crucial aspects. These are the number of keys used, the method to distribute or negotiate keys and the (non-)existence of a re-keying mechanism aimed at increasing unlinkability of platoon messages.

Obviously, CKEPP, featuring a larger number of symmetric keys to be stored at the same time, requires a larger key storage than DKEPP. However, given the size of symmetric keys this can be considered negligible.

An advantage of CKEPP over DKEPP is that it allows for more easy leave maneuvers. Particularly, CKEPP does not require key negotiation between the remaining PLMs. Instead, the new key can directly be distributed by the PLL. Besides the increased easiness of "leave" maneuvers, CKEPP can be expected to provide greater unlinkability than DKEPP, due to its re-keying mechanism. However, this hypothesis still requires testing, which we will pursue in future work.

A benefit of DKEPP is the decentralized approach which does not require a PLL. PLM exchange keys and communicate directly with each other, meaning the reduction of a possible single point of failure. On the downside a regular change of keys would generate a certain overhead as keys are always negotiated directly between PLMs.

A formal analysis of the protocols' security properties is out of scope of this paper. However, it is to be expected that both protocols perform similarly as they both rely on well-known primitives and protocols. However, a closer and more formal analysis is left to future work.

V. Conclusion & Future Work

In this paper, we discussed security and privacy aspects related to HDLP. We analyzed related work and concluded that research was mainly done into separate stages of the HDLP but especially regarding an overall solution considering the whole process from booking until leaving we did not find much work. Hence, we proposed a general security architecture derived from general and specific security requirements. Finally, we discussed security concepts for HDLP. In future work we will extend the proposed solutions for HDLP to a full specification.

Acknowledgment

This work has been supported in part by the Federal Ministry of Education and Research of the Federal Republic of Germany (BMBF) in the framework of the project 5G NetMobil with funding number 16KIS0692. The authors alone are responsible for the content of the paper.

References

[1] D.-G. for Mobility and Transport, *Statistical pocketbook 2018*, Oct. 2, 2018. DOI: 10.2832/05477.

[2] W.-H. Hucho and G. Sovran, "Aerodynamics of road vehicles," *Annual Reviews*, vol. 1, 1993.

[3] T. Robinson and E. Coelingh, "Operating platoons on public motorways: An introduction to the sartre platooning programme," Oct. 2010.

[4] A. K. Bhoopalam, N. Agatz, and R. Zuidwijk, "Planning of truck platoons: A literature review and directions for future research," *Transportation Research Part B: Methodological*, vol. 107, 2018. DOI: 10.1016/j.trb.2017.10.016.

[5] R. Janssen, H. Zwijnenberg, and I. B. and Janiek de Kruijff, *Truck platooning driving the future of transportation*, Feb. 2015.

[6] K. Liang, J. Mårtensson, and K. H. Johansson, "Fuel-saving potentials of platooning evaluated through sparse heavy-duty vehicle position data," in *2014 IEEE Intelligent Vehicles Symposium Proceedings*, Jun. 2014. DOI: 10.1109/IVS.2014.6856540.

[7] P. Mallozzi, M. Sciancalepore, and P. Pelliccione, "Formal verification of the on-the-fly vehicle platooning protocol," in *Software Engineering for Resilient Systems*, I. Crnkovic and E. Troubitsyna, Eds., Cham: Springer International Publishing, 2016, ISBN: 978-3-319-45892-2.

[8] E. B. Hamida, H. Noura, and W. Znaidi, "Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures," *Electronics*, vol. 4, no. 3, 2015. DOI: 10.3390/electronics4030380. [Online]. Available: http://www.mdpi.com/2079-9292/4/3/380.

[9] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on vanet security challenges and possible cryptographic solutions," *Vehicular Communications*, vol. 1, no. 2, 2014. DOI: 10.1016/j.vehcom.2014.05.001.

[10] C. Bernardini, M. R. Asghar, and B. Crispo, "Security and privacy in vehicular communications: Challenges and opportunities," *Vehicular Communications*, vol. 10, 2017. DOI: 10.1016/j.vehcom.2017.10.002.

[11] F. Qu, Z. Wu, F. Wang, and W. Cho, "A security and privacy review of vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, Dec. 2015. DOI: 10.1109/TITS.2015.2439292.

[12] M. K. Nasir, A. D. Hossain, M. S. Hossain, M. M. Hasan, and M. B. Ali, "Security challenges and implementation mechanism for vehicular ad hoc network," *International journal of scientific & technology research*, vol. 2, no. 4, 2013.

[13] M. Raya and J.-P. Hubaux, "Security aspects of inter-vehicle communications," in *5th Swiss Transport Research Conference (STRC)*, 2005.

[14] M. Amoozadeh, A. Raghuramu, C. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Communications Magazine*, vol. 53, no. 6, Jun. 2015. DOI: 10.1109/MCOM.2015.7120028.

[15] S. Dadras, R. M. Gerdes, and R. Sharma, "Vehicular platooning in an adversarial environment," in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, ser. ASIA CCS '15, Singapore, Republic of Singapore: ACM, 2015. DOI: 10.1145/2714576.2714619.

[16] R. M. Gerdes, C. Winstead, and K. Heaslip, "Cps: An efficiency-motivated attack against autonomous vehicular transportation," in *Proceedings of the 29th Annual Computer Security Applications Conference*, ser. ACSAC '13, New Orleans, Louisiana, USA: ACM, 2013. DOI: 10.1145/2523649.2523658.

[17] B. DeBruhl, S. Weerakkody, B. Sinopoli, and P. Tague, "Is your commute driving you crazy?: A study of misbehavior in vehicular platoons," in *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, ser. WiSec '15, New York, New York: ACM, Jun. 2015. DOI: 10.1145/2766498.2766505.

[18] M. Asplund, "Poster: Securing vehicular platoon membership," in *2014 IEEE Vehicular Networking Conference (VNC)*, Dec. 2014. DOI: 10.1109/VNC.2014.7013324.

[19] A. Petrillo, A. Pescapé, and S. Santini, "A collaborative approach for improving the security of vehicular scenarios: The case of platooning," *Computer Communications*, vol. 122, 2018. DOI: 10.1016/j.comcom.2018.03.014.

[20] *Intelligent transport systems (its); communications architecture*, ETSI EN 302 665 v1.1.1, ETSI, Sep. 2010.

[21] *Intelligent transport systems (its); security; security services and architecture*, ETSI TS 102 731 v1.1.1, ETSI, Sep. 2010.

[22] *Its communication security architecture and security management*, ETSI TS 102 940 v1.3.1, ETSI, Apr. 2018.

[23] *Intelligent transport systems (its); security; trust and privacy management*, ETSI TS 102 941 v1.2.1, ETSI, May 2018.

[24] *Certificate policy for deployment and operation of european cooperative intelligent transport systems (c-its)*, Release 1, C-ITS, Jun. 2017.

[25] *Security policy & governance framework for deployment and operation of european cooperative intelligent transport systems (c-its)*, Release 1, C-ITS, Dec. 2017.

[26] M. Ullmann, T. Strubbe, and C. Wieschebrink, "Technical Limitations, and Privacy Shortcomings of the Vehicle-to-Vehicle Communication," in *Fifth International Conference on Advances in Vehicular Systems*, Barcelona, Spain, 2016.

[27] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management," 2010.

[28] J. Caldenhoven, S. Köpsell, T. Lang, G. Schulte, M. Sontowski, A. Weinand, and C. Zimmermann, *Deliverable 2.1c – towards a 5g netmobil security architecture: Security requirements and initial concepts*, Nov. 8, 2018.

[29] A. Weinand, M. Karrenbauer, J. Lianghai, and H. D. Schotten, "Physical layer authentication for mission critical machine type communication using gaussian mixture model based clustering," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, Jun. 2017. DOI: 10.1109/VTCSpring.2017.8108527.

[30] J. Katz and M. Yung, "Scalable protocols for authenticated group key exchange," in *Annual International Cryptology Conference*, Springer, 2003.