CISTER
Research Centre in
Real-Time & Embedded
Computing Systems

Journal Paper

Confidentiality and Timeliness of Data Dissemination in Platoon-based Vehicular Cyber-Physical Systems

In press

Kai Li*
Wei Ni
Jingjing Zheng*
Eduardo Tovar*
Mohsen Guizani

*CISTER Research Centre

CISTER-TR-210402

2021

Confidentiality and Timeliness of Data Dissemination in Platoon-based Vehicular Cyber-Physical Systems

Kai Li*, Wei Ni, Jingjing Zheng*, Eduardo Tovar*, Mohsen Guizani

*CISTER Research Centre

Polytechnic Institute of Porto (ISEP P.Porto)

Rua Dr. António Bernardino de Almeida, 431

4200-072 Porto

Portugal

Tel.: +351.22.8340509, Fax: +351.22.8321159

E-mail: kai@isep.ipp.pt, Wei.Ni@data61.csiro.au, zheng@isep.ipp.pt, emt@isep.ipp.pt

https://www.cister-labs.pt

Abstract

Recent advances in inter-vehicle wireless communications allow for automated and coordinated vehicles 19 driving in platoon-based vehicular cyber-physical systems (PVCPS). This article presents a comprehensive low-latency cooperative security (LLCS) framework for secure and timely data dissemination in PVCPS. A new cooperative secret key agreement protocol is incorporated to produce secret keys for platooning vehicles based on their radio channel correlation. A new transmit rate adaptation mechanism is presented to minimize the end-to-end latency of the data dissemination in PVCPS. We also numerically test confidentiality and timeliness of the LLCS framework in terms of key agreement probability and dissemination delay. It is believed that the LLCS framework is the demand of the time to enable secure and reliable autonomous driving for future PVCPS.

Confidentiality and Timeliness of Data Dissemination in Platoon-based Vehicular Cyber-Physical Systems

Kai Li, Wei Ni, Jingjing Zheng, Eduardo Tovar, and Mohsen Guizani

Abstract—Recent advances in inter-vehicle wireless communications allow for automated and coordinated vehicles' driving in platoon-based vehicular cyber-physical systems (PVCPS). This article presents a comprehensive low-latency cooperative security (LLCS) framework for secure and timely data dissemination in PVCPS. A new cooperative secret key agreement protocol is incorporated to produce secret keys for platooning vehicles based on their radio channel correlation. A new transmit rate adaptation mechanism is presented to minimize the end-to-end latency of the data dissemination in PVCPS. We also numerically test confidentiality and timeliness of the LLCS framework in terms of key agreement probability and dissemination delay. It is believed that the LLCS framework is the demand of the time to enable secure and reliable autonomous driving for future PVCPS.

Index Terms—Cyber-physical systems, Autonomous vehicles, Wireless communications, Network security

1 Platoon-based Vehicular Cyber-Physical Systems

Vehicular platoons that group autonomous vehicles into a road train can improve road capacity and safety of automated motorway systems. The throughput of freeway traffic is expected to increase by forming vehicular platoons with small inter-vehicle spacings, and hence allowing more vehicles to fit on freeway [1]. The lead vehicle of a platoon, which drives manually or autonomously ahead of the platoon, determines the driving status of the following vehicles, i.e., velocity, heading, and acceleration/deceleration. The driving status of the platoon can be affected by emergent road conditions, e.g., rear-end collision, obstacles, animal crossing the road, or traffic congestion.

Both biologically inspired, platoon is different from swarm. The former follows strong leaderships from individuals (e.g., matriarchs of elephants). The latter is based on the collective behavior of less intelligent, decentralized knowledgeable and experienced individuals like many insects (e.g., bees and ants). Platoon can provide higher reliability, predictability, and controllability than swarm. Therefore, it is more suitable for the control of systems requiring reliability in fast-changing and potentially risky environments, such as highway.

Platoon-based Vehicular Cyber-Physical Systems (PVCPS) play an important role to provide wireless connectivity for platoon management [2]. Each vehicle in PVCPS is equipped with an on-board unit (OBU) for control message processing, and a wireless communication module for data dissemination [3]. The physical and MAC layers of the vehicle-to-vehicle communications in PVCPS can be based on Wireless Access in Vehicular Environment (WAVE) [4], aligning with industrial standards and roadmap. Other dedicated short range communications can also be used for the data dissemination in PVCPS.

Fig. 1 illustrates the data dissemination in PVCPS, where the driving control messages are generated by the lead vehicle to advise road conditions. The messages are disseminated to the following vehicles to update their driving status (e.g., based on the latest IEEE 802.11-OCB protocol). The formation of the platoon and the number of vehicles in the platoon are typically configured beforehand. A vehicle in PVCPS can be in either a transmitting state in which the vehicle transmits a message to its following vehicle, or a receiving state in which the vehicle receives the message from its preceding vehicles. The two states interchange, depending on the message generation rate at the lead vehicle.

Vehicular ad hoc networks (VANETs) consist of vehicle-to-vehicle and vehicle-to-roadside communications to provide road users with wireless access services. Each vehicle in VANETs can produce a road condition update, e.g., traffic congestion and car accident reports. The vehicle can broadcast its road condition update to other vehicles or roadside units around it. In PVCPS, vehicular data and control messages are generated by the lead vehicle only to control the real-time operations of the following driverless vehicles in a platoon. For example, the platoon may change the mobility pattern of the vehicles due to sudden or unexpected road emergencies, e.g., cyclists and pedestrians. The following driverless vehicles rely on the observation, judgment and decision of the lead vehicle, or more specifically, the driver of the lead vehicle. The disseminated data contains safety-critical driving status information, such as the speed, heading, and/or location of the next stop, and other information. A hop-by-hop delivery of the messages with confirmed reception at every vehicle provides a reliable vehicle-to-vehicle communication mechanism for PVCPS. Upon the receipt of the disseminated data, the vehicles can

K. Li (Senior Member, IEEE), J. Zheng, and E. Tovar (Member, IEEE) are with CISTER Research Centre, Portugal (E-mail:{kai,zheng,emt}@isep.ipp.pt).
W. Ni (Senior Member, IEEE) is with Data61 Business Unit, CSIRO, Australia (E-mail: wei.ni@data61.csiro.au).
M. Guizani (Fellow, IEEE) is with Computer Science and Engineering Department, Qatar University, Qatar (E-mail:mguizani@ieee.org).

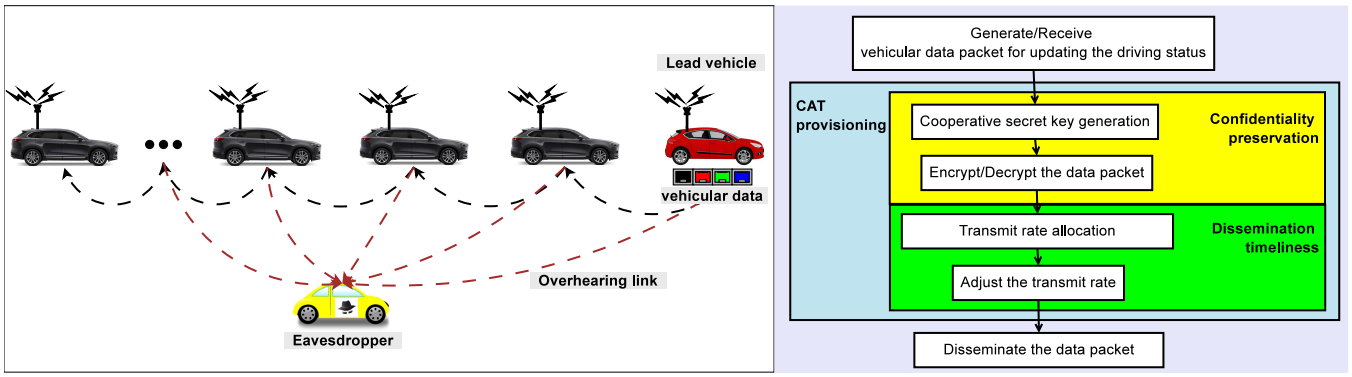


Fig. 1: Data dissemination in PVCPS. The control messages are disseminated from the lead vehicle to the following vehicles. The eavesdropping vehicle locating in communication range can overhear the data transmission. The low-latency cooperative security protocol can provision CAT to the data dissemination in PVCPS.

take consistent reactions, e.g., decelerating or changing the lane or heading, to protect vulnerable road users.

Wireless data dissemination in PVCPS can be susceptible to eavesdropping attacks due to the broadcast nature of radio. An eavesdropping vehicle within the communication range of PVCPS could overhear the data transmission of the platoon. The eavesdropping vehicle would extract critical data, such as time, location, vehicle identifier, technical description, and other trip details, and derive critical private driving information. In PVCPS, the disseminated data contains safety-critical driving status information. After overhearing the driving information of the PVCPS, the eavesdropping vehicle could potentially launch spoofing and replaying attacks to inject false control messages and abuse mobility patterns, e.g., falsifying the speed or heading. This would threat the safety and efficiency of the platoon, pedestrians, and other vehicles driving alongside the platoon.

This article presents a new framework for secure and timely data dissemination in PVCPS, where there are two critical new aspects: (1) A new distributed secret key agreement protocol, where all platooning vehicles can produce a consistent secret key at-one-go by measuring the received signal strengths from the first two vehicles and optimizing the quantization levels of the signal strengths; and (2) a new reliable rate adaptation mechanism which minimizes the end-to-end latency of the data dissemination with hop-by-hop confirmation.

The rest of the article is organized as follows. Section 2 presents the confidentiality and timeliness of the data dissemination in PVCPS. Section 3 and Section 4 study the secret key agreement and optimal rate adaptation of the low-latency cooperative security framework, respectively. Numerical analyses are presented in Section 5. Concluding remarks are drawn in Section 6.

2 Confidentiality and Timeliness

Beamforming could be potentially used for directional inter-vehicle communication to narrow the radio coverage. However, beamforming alone is not enough to preserve the confidentiality of control message dissemination in PVCPS. This is because typically non-negligible sidelobes of the beams would leak confidential information.

A secret key which can encrypt the control messages in PVCPS is crucial to protect the platoon's driving status from eavesdropping, hence ensuring driving safety. Group secret key has been studied in vehicular ad-hoc networks [5]. However, a group secret key has to be generated, distributed and updated by a trusted group head (either the lead vehicle or roadside units), resulting in non-negligible data dissemination delays in PVCPS. Public key signatures can be generated to verify the identity of vehicles against impersonation attacks in vehicular ad-hoc networks [6]. However, public key cryptography requires a fixed key management infrastructure and pairwise handshaking processes. The vehicular communication security in cellular vehicle-to-everything (C-V2X) has also been studied in the fifth generation (5G) wireless networks [7]. Despite being envisioned with seamless coverage, the C-V2X technologies, or more broadly the 5G technologies, can still face coverage challenges in reality, in many cases, due to the lack of incentives and profitability to 5G operators. This has been the case of highways in remote and unpopulated areas, e.g., the highways across central Australia and New Zealand, during the roll-out of 3G, 4G and National Broadband Network (NBN). To this end, the provision of confidentiality and timeliness to PVCPS based on the inter-vehicle communication provides an effective and efficient solution to these scenarios.

A key generation that exploits fading channel dynamics and randomness has been widely studied to achieve physical-layer security [8]. Two vehicles in PVCPS can exploit the reciprocity of their wireless channel to extract secret key bits [9], [10]. Two critical new challenges make the key agreement in PVCPS nontrivial. The first challenge is that the channel between any two vehicles is time-varying and undergoes random fading. It is difficult for multiple vehicles in PVCPS to generate and agree on a unanimous secret key. The second challenge is that the channel randomness measured between a pair of vehicles must not be transmitted over any insecure public channel, due to potential eavesdropping.

In PVCPS, every vehicle (except the lead vehicle) has to maintain a small and nearly constant distance to the preceding vehicle, for the sake of driving safety. However, the actual inter-vehicle distance can be time-varying, due to slightly different instantaneous driving speeds (and accel-

erations) of the vehicles. The fading channel dynamics can cause losses of the encrypted data at the receiver vehicle. A packet loss is particularly destructive in PVCPS because of the criticality of the disseminated information for driving control. Every vehicle must correctly receive the information and confirm the reception, so that the platoon can operate (e.g., change its driving course) consistently and safely. Moreover, the packet loss in PVCPS can significantly reduce the timeliness of the cruise control and platoon management due to packet retransmissions. A high transmit rate could speed up transmissions but increase the bit error rate (BER) of the transmissions. The data dissemination latency could be extended, as the high BER would result in retransmissions. Therefore, the transmit rate needs to be properly assigned.

With consideration of driving safety, PVCPS needs to preserve the confidentiality of data dissemination from eavesdropping attacks, and provide timely data dissemination for cruise control and platoon management. This article presents Low-Latency Cooperative Security (LLCS), which is a comprehensive solution to provisioning Confidentiality and Timeliness (CAT) to the data dissemination in PVCPS. As shown in Fig. 1, unanimous keys that are cooperatively generated in LLCS are used by the platooning vehicles to encrypt and decrypt the disseminated data. For fast data dissemination, LLCS optimizes the transmit rate allocation at each vehicle adapting to the time-varying channel of every hop. Furthermore, we study performance of the data dissemination in terms of:

- Key agreement probability, which characterizes the robustness of the key generation.
- Dissemination delay, which measures the latency of data dissemination.

The vehicles in PVCPS are traveling along a straight lane on highway with no need to change the platoon size or perform maneuvers (split, merge, leave, etc.), hence keeping the operations of the cruise control simple. Moreover, traveling on a straight highway also allows the platoon to drive at highway speeds, while the problem of CAT is prominent, as compared to low speeds.

3 Cooperative Secret Key Generation

To enhance confidentiality preservations for the data dissemination in PVCPS, all vehicles cooperatively generate unanimous shared secret keys for data encryption/decryption. The secret key agreement enables the following vehicles to successfully decode the data packets that are encrypted by the lead vehicle. We study a new physical-layer secret key agreement in LLCS, where the fading channel randomness is quantized at the vehicles to cooperatively generate the same secret key based on the inter-vehicle channels.

As shown in Fig. 2, LLCS employs a secret key agreement period, i.e., from t_{T0} to t_{key}, followed by a data dissemination period, i.e., from t_{D1} to $t_{D_{n-1}}$. The ID number of the lead vehicle can fit in a small token packet, Token_0. The transmission of the token packet is initiated by the lead vehicle which decides the driving status on its own. The second vehicle in PVCPS transmits Token_1 once it

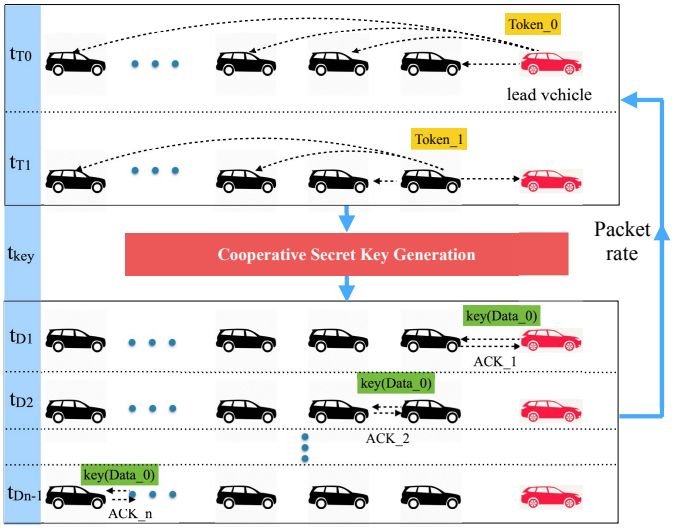


Fig. 2: A cooperative secret key is generated by LLCS for data encryption and decryption in PVCPS.

successfully receives Token_0. Token_1 can also be treated as an acknowledgement to the lead vehicle. If Token_1 is not received by the lead vehicle, then Token_0 is retransmitted. At t_{key}, the token transmissions are completed. The channel information is obtained by the vehicles, and each vehicle can carry out LLCS to generate unanimous secret keys.

For the data dissemination, the lead vehicle forwards a data packet that is encrypted by the secret key of LLCS to the next vehicle in the platoon. Then, the following vehicles in PVCPS can use their own keys generated by LLCS to decrypt the received packet while forwarding the data packet all the way to the tail vehicle.

The secret key agreement in LLCS can be implemented in three steps: (1) inter-vehicle channel estimation, where the platooning vehicles estimate channel randomness between the first two vehicles; (2) channel quality indicator (CQI) quantization, which optimizes the quantization intervals to allow the individual platooning vehicles to quantize the estimated channel randomness with the maximum probability of consistency between the vehicles; and (3) secret key agreement, where the vehicles distributively produce a consistent unanimous secret key in PVCPS based on the quantization intervals. The details of the three steps are provided in the following.

- **Step 1: Inter-vehicle channel estimation.** Token packets are broadcasted by the lead vehicle and its immediate follower. All the vehicles in PVCPS measure the channel quality of the tokens. Each of the vehicles can estimate the channel gain between the lead vehicle and its immediate follower [11].
- **Step 2: CQI quantization.** Each vehicle quantizes its estimated channel gain between the first two vehicles of the platoon to one of the CQI quantization intervals. The CQI quantization can convert the fading channel randomness into bit vectors which are used to generate secret key bits. Specifically, each CQI quantization interval can correspond to a unique binary bit vector. The estimated channel gain falling into one of the quantization intervals can be coded

as a sequence of binary bits. We can maximize the key agreement probability with which the estimated channel gain of all the vehicles in PVCPS are quantized to the same interval. Given the number of quantization intervals, the maximization is achieved by recursively optimizing the CQI quantization intervals [12].

- **Step 3: Secret key agreement.** Given the optimal CQI quantization intervals obtained in Step 2, the channel gain between the lead vehicle and its next vehicle can be quantized at each of the platooning vehicles. Classical encoding techniques and symmetric key methods, such as Gray coding or Gillham coding, can be employed to assign each quantization bin with a binary codeword. The codewords of two consecutive quantization bins only have a one-bit difference. As a result, the estimated channel gain can be encoded into a binary codeword, and an agreeable symmetric secret key can be generated at the platooning vehicles.

As the vehicles of the platoon drive in a fully autonomous fashion at a highway speed, one lane on the highway is reserved for vehicular platoons, for driving safety. Any vehicle occupying the reserved lane can be identified as a potential eavesdropper. Despite that, the eavesdropping vehicles may still travel in parallel to the PVCPS and listen to the token packets. The channel between a vehicle in PVCPS and the eavesdropping vehicle can be quantized by the eavesdropping vehicle in an attempt to recover the secret key. However, the secret key agreement achieved by LLCS encloses the fading channel dynamics over multiple vehicles in PVCPS. The same secret key cannot be obtained by the eavesdropping vehicle that undergoes independent channel randomness at other locations [13]. Note that we consider the worst-case scenario, where an eavesdropper remains close and relatively stationary to the platoon in an attempt to reproduce the secret key of the platoon. In the presence of a stationary eavesdropper deployed at the roadside, the channel gain between the platooning vehicles and the stationary eavesdropper can change very fast, much faster than that between the platooning vehicles or between the platooning vehicles and the above-mentioned eavesdropping vehicle. As a result, the stationary roadside eavesdropper is expected to be less threatening than the eavesdropping vehicle, given the proposed protocol in place.

Since the eavesdropper attempts to obtain the control information on the driving status of PVCPS, the eavesdropper may not want to disrupt the key agreement and the data dissemination. Moreover, it is not practical for the eavesdropping vehicle to measure the SNR of every point along the whole highway in advance. Thus, the eavesdropping vehicle does not have the a-priori knowledge of the time-varying SNR between two platooning vehicles.

LLCS is more tolerant to an external jammer, as compared to other key generation and distribution mechanisms. The reason is that all the vehicles in LLCS only need to listen to a round of token transmissions between the lead vehicle and its immediate follower, and derive the secret keys independently if the token transmissions are unjammed. Given the much shorter transmissions of only two tokens (than hop-by-hop distributions of secret keys), LLCS significantly reduces the adverse impact that could be caused by the jammer. Moreover, the secret key does not have to change as frequently as the channels, in order to reduce the overhead of token transmissions. On the other hand, frequently changing channels can update the secret keys more often, when needed, which prevents a secret key from being used too long and reduces the risk of the key being exposed.

4 Low-Latency Transmit Rate Allocation

To enhance timeliness for the secure data dissemination in PVCPS, we come up with the optimal low-latency transmit rate allocation in LLCS for fast data dissemination while guaranteeing successful delivery of the data at each vehicle. If the data transmission of a vehicle is successful, an acknowledgement is returned from the following vehicle, as shown in Fig. 2. Otherwise, the transmit rate of the vehicle needs to be updated for a retransmission.

It is known that the vehicle with an excessively high modulation order can achieve fast data transmission, but suffer from a high packet loss (or BER) and power consumption. On the other hand, an unnecessarily low modulation order can prolong the data transmission. To this end, LLCS is designed to minimize the data dissemination latency by optimizing the transmit rate allocation in PVCPS.

Given the aforementioned link quality dynamics, allocating a transmit rate to the vehicle in PVCPS can lead to two possible outcomes: 1) the data is successfully sent to its following vehicle, and the overall data dissemination latency depends on the packet transmission time determined by the allocated transmit rate at the vehicle; and 2) the data of the vehicle is not successfully transmitted. The transmission latency remains the same as the preceding vehicle. Therefore, the transmission latency of each vehicle in PVCPS can be minimized by properly allocating the transmit rate according to the BER requirement and the transmit power, which minimizes the overall data dissemination latency.

Since the transmission latency towards a vehicle depends on the transmit rate allocation at its preceding vehicles, the transmit rate can be recursively optimized by formulating a chain-based transmit rate allocation to minimize the total data dissemination latency from the lead vehicle to the tail in PVCPS. The chain-based transmit rate allocation problem can be broken down into a series of overlapping subproblems and solved one-by-one recursively, where every subproblem minimizes the data dissemination latency for a vehicle.

To obtain the optimal transmit rate for the vehicles in PVCPS, dynamic programming is adopted by LLCS to iterate over the state of each vehicle in uncertainty spaces. In particular, a state indicates the dissemination latency consumed by the preceding vehicles that have successfully received the disseminated data packet. LLCS calculates the transmit rate and the corresponding policy for the optimal transmit rate allocation from the lead vehicle to the tail vehicle. Moreover, the subproblem of minimizing the transmission time of the vehicle is solved by LLCS at each decision stage of the transmit rate allocation. The optimal

solution to the transmit rate is saved in a table, thereby avoiding recomputing the solution.

Dynamic programming (DP) is an effective tool to solve problems which can be decomposed into overlapping sub-problems, including the optimization of the chain-based transmit rate allocation [14]. Specifically, the transmit rate of vehicle $(N-1)$ is first assessed. The outcome is then used to determine the transmit rate of vehicle $(N-2)$. This continues until the transmit rate of vehicle 1 is evaluated; and the optimal transmit rates of all vehicles can be finally determined with backward induction (i.e., tracing back the possible allocations and picking up the best) [15]. This transmit rate allocation can be done in prior, and stored in a lookup table at the lead vehicle. By checking the lookup table, LLCS can assign the transmit rate allocation of PVCPS. The allocation information can be added into the token or data packet delivered to the following vehicles.

In terms of the implementation of LLCS, the channel information, e.g., Received Signal Strength Indicator (RSSI) or Channel State Information (CSI), is accessible in the off-the-shelf OBUs. Moreover, the vehicular communication standards and protocols supported by the OBUs, such as Dedicated Short-Range Communications (DSRC) and Intelligent Transportation Systems-G5 (ITS-G5), support multiple modulation schemes and adaptive switch between the modulation schemes, adapting to the changing wireless channels. Hence, LLCS can be implemented using the existing OBUs with limited hardware or firmware modifications.

5 Confidentiality and Timeliness Analysis of LLCS

In this section, we analyze the performance of LLCS. The transmission range of the typical off-the-shelf OBU can be greater than 100 m. The packet length is 32 bytes, and the required maximum BER is set to 0.05%.

5.1 Secret key agreement probability

To exploit the key agreement of LLCS, the number of CQI quantization intervals is set to 10, 15, or 70. The average SNR of the inter-vehicle channel is 5 dB or -10 dB.

Assuming a total of N vehicles in PVCPS, Fig. 3 presents the key agreement probability achieved by LLCS according to the platoon size N. Specifically, the key agreement probability with LLCS is higher than 80% when the number of vehicles is less than 10 and the average SNR is 5 dB. When the SNR of the inter-vehicle channel drops to -10 dB, the number of vehicles in PVCPS has to be less than 6 vehicles to maintain the key agreement probability beyond 78%. Essentially, Fig. 3 indicates that the platoon size should not be excessively large to maintain the key agreement probability with LLCS when the channel condition is poor.

It is also observed in Fig. 3 that reducing the quantization intervals in LLCS can improve the key agreement probability. When the number of vehicles in PVCPS is three, the key agreement probability with LLCS grows from 74% to 95% when the quantization intervals, denoted by L, drops from 70 to 10. Moreover, the key agreement probability achieved by LLCS with (L = 15 and SNR = -10 dB) is higher than the one with (L = 70 and SNR = 5 dB) when the

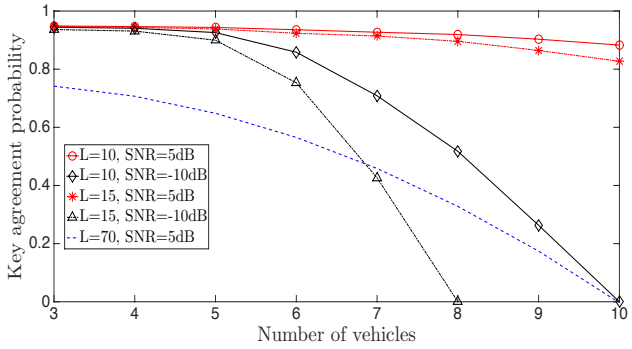


Fig. 3: The key agreement performance of LLCS in respect to number of vehicles in PVCPS.

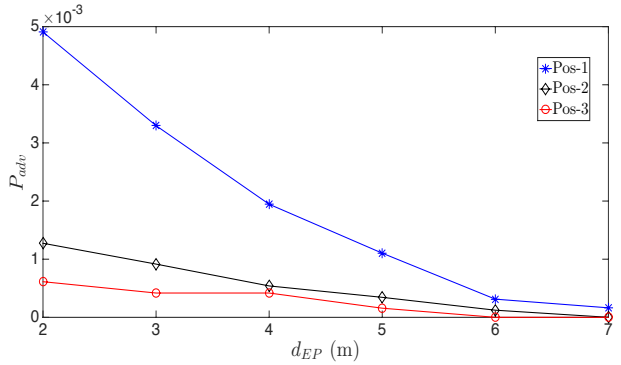


Fig. 4: The probability that the eavesdropper generates the same secret key as PVCPS with respect to their relative positions.

number of vehicles in PVCPS is smaller than 7. This reveals that the quantization interval dominates the key agreement performance of LLCS with a small platoon size. Conversely, LLCS with (L = 70 and SNR = 5 dB) outperforms the one with (L = 15 and SNR = -10 dB) when PVCPS has more than 7 vehicles. This indicates that SNR of the inter-vehicle channel becomes the dominating factor.

Let P_{adv} denote the probability that the eavesdropper generates the same secret key as PVCPS. In particular, we consider that the platoon has 7 vehicles, and the quantization intervals in LLCS are 15. d_{EP} defines the distance between the eavesdropper and the platooning vehicle in PVCPS. We consider three specific positions of the eavesdropper. Specifically, the eavesdropper in parallel with vehicle 2 is Pos-1, the position in parallel with vehicle 4 is Pos-2, and Pos-3 is the position in parallel with vehicle 7.

Fig. 4 plots P_{adv} with the increase of d_{EP}, where the eavesdropper is at Pos-1, Pos-2, or Pos-3. Particularly, the safe distance of PVCPS is set to 2 m, namely, PVCPS can identify the eavesdropper by observation when d_{EP} is shorter than the safe distance. As observed, the highest P_{adv} is 0.49% where the eavesdropper is at Pos-1 and d_{EP} = 2 m. This is because Pos-1 is close to the first two vehicles of the platoon, who transmit Token_0 and Token_1. The SNR of the overhearing channel can be correlated with the one between the first two vehicles. As a result, the overhearing channel might be quantized to the same quantization intervals as

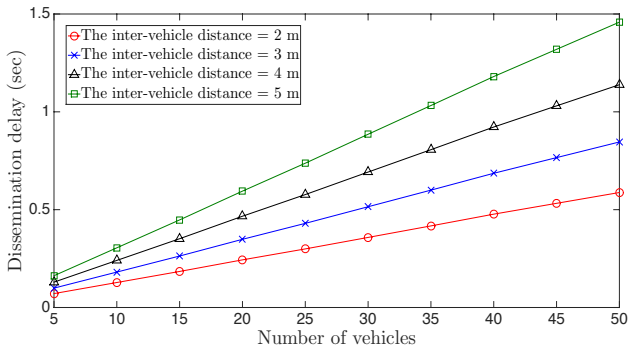


Fig. 5: Timeliness of LLCS with respect to different inter-vehicle distances, where the platoon size increases from 5 to 50 vehicles.

PVCPS. Moreover, P_{adv} significantly drops with the increase of d_{EP}. P_{adv} falls to 0 when the eavesdropper is at Pos-3 with d_{EP} = 6 m. The reason is that the overhearing channel experiences independent fading when the eavesdropper is far away from the first two vehicles that transmit Token_0 and Token_1. Therefore, it is difficult for the eavesdropper to obtain the same quantization intervals as PVCPS for the key generation due to a low channel correlation.

5.2 Data dissemination latency

Fig. 5 demonstrates the average latency achieved by LLCS with regards to different inter-vehicle distances. The average data dissemination latency grows with the platoon size since the overall latency counts on the transmission delay at each of the vehicles. Moreover, a large inter-vehicle distance results in a high data dissemination latency in PVCPS. The reason is that extending the inter-vehicle distance can attenuate the SNR of the inter-vehicle channel. The dissemination latency of LLCS could be extended, as the low SNR would result in packet retransmissions.

Although a small inter-vehicle distance can reduce the data dissemination latency, as shown in Fig. 5, the small inter-vehicle distance shortens the reaction time in a braking response, which can increase the safety risks of PVCPS. Therefore, the inter-vehicle distance needs to be properly configured in PVCPS according to the driving safety and timeliness of the data dissemination.

Fig. 5 indicates that there is a tradeoff between confidentiality and timeliness of data dissemination in PVCPS. While the secret keys encrypting the vehicular data can improve the confidentiality, the data dissemination of PVCPS can incur a long delay due to the key generation and distribution. To speed up the data dissemination, LLCS carries out the optimal low-latency transmit rate allocation to minimize the overall data dissemination latency. As shown in Fig. 5, the dissemination time between two adjacent vehicles, achieved by the proposed LLCS, is shorter than 0.1 second in the case of 5 vehicles in a platoon. Therefore, the safety of PVCPS can be guaranteed with LLCS.

LLCS only requires the first two vehicles in the platoon to broadcast tokens. The other vehicles estimate the channel gain between the first two vehicles, and generate the agreeable secret key in a distributed fashion. The overhead of token transmission is much lower, as compared to the size of a data packet. For example, we consider that 20 token packets are transmitted by the first two vehicles (10 from each) in one dissemination cycle, and each token has 10 bits and contains the ID of the vehicle. The total overhead of the token transmission is 200 bits, much less than a data packet. Considering a data rate of 250 kbps, the transmission time of the tokens is just about 0.4 ms at a vehicle. Therefore, the cost of the token transmission is comparatively negligible.

5.3 Compatibility of LLCS

The LLCS framework generates secret keys for platooning vehicles based on their radio channel information, e.g, received signal strength (RSS). This is because RSS is universally available for off-the-shelf wireless devices, hence leading to significant cost savings.

The optimal transmit rate adaptation of LLCS, minimizing the end-to-end data dissemination latency, is compatible with the existing or emerging vehicle-to-vehicle communication standards, such as dedicated short-range communications (DSRC) or wireless access in vehicular environments (WAVE). LLCS is also compatible with collision avoidance mechanisms in the DSRC or WAVE systems. There are possibilities that the transmissions collide between the platooning vehicles and vehicles outside the platoon. LLCS does not mitigate these transmission collisions. Nevertheless, LLCS can incorporate the standard exponential backoff and retransmission techniques, and minimize the end-to-end data dissemination latency with guaranteed BER.

6 Conclusions and Future Directions

This article presents the CAT of data dissemination in PVCPS. We study the LLCS framework to preserve confidentiality of the low-latency data dissemination. By quantizing the inter-vehicle channel randomness, LLCS recursively optimizes the channel quantization intervals so that unanimous secret keys can be cooperatively generated for secure data delivery. LLCS also utilizes dynamic programming to optimize the transmit rate allocation such that the data dissemination latency is minimized while guaranteeing successful data reception at each vehicle.

In the future, the LLCS framework will be extended to improve the CAT of data dissemination in dynamic driving scenarios, e.g., making turns, driving on mixed lanes in urban areas, etc. Guaranteeing the CAT of data dissemination with different mobility patterns of PVCPS also has to be considered as part of our future work.

Acknowledgements

This work was partially supported by National Funds through FCT/MCTES (Portuguese Foundation for Science and Technology), within the CISTER Research Unit (CEC/04234); also by national funds through the FCT, under CMU Portugal partnership, within project CMU/TIC/0022/2019 (CRUAV).

REFERENCES

[1] A. Vinel, L. Lan, and N. Lyamin, "Vehicle-to-vehicle communication in C-ACC/platooning scenarios," *IEEE Communications Magazine*, vol. 53, no. 8, pp. 192–197, 2015.

[2] D. Jia, K. Lu, J. Wang, X. Zhang, and X. Shen, "A survey on platoon-based vehicular cyber-physical systems," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 263–284, 2016.

[3] V. K. Kukkala, J. Tunnell, S. Pasricha, and T. Bradley, "Advanced driver-assistance systems: A path toward autonomous vehicles," *IEEE Consumer Electronics Magazine*, vol. 7, no. 5, pp. 18–25, 2018.

[4] H. Abou-Zeid, F. Pervez, A. Adinoyi, M. Aljlayl, and H. Yanikomeroglu, "Cellular V2X transmission for connected and autonomous vehicles standardization, applications, and enabling technologies," *IEEE Consumer Electronics Magazine*, vol. 8, no. 6, pp. 91–98, 2019.

[5] L. Zhang, X. Men, K.-K. R. Choo, Y. Zhang, and F. Dai, "Privacy-preserving cloud establishment and data dissemination scheme for vehicular cloud," *IEEE Transactions on Dependable and Secure Computing*, no. 1, pp. 1–1, 2018.

[6] H. Hartenstein and L. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Communications magazine*, vol. 46, no. 6, 2008.

[7] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679–695, 2018.

[8] Y. Yang and M. Guizani, "Mapping-varied spatial modulation for physical layer security: Transmission strategy and secrecy rate," *IEEE Journal on Selected Areas in Communications*, 2018.

[9] G. Epiphaniou, P. Karadimas, D. K. B. Ismail, H. Al-Khateeb, A. Dehghantanha, and K.-K. R. Choo, "Nonreciprocity compensation combined with turbo codes for secret key generation in vehicular ad hoc social IoT networks," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2496–2505, 2017.

[10] J. Wan, A. Lopez, and M. A. A. Faruque, "Physical layer key generation: Securing wireless communication in automotive cyber-physical systems," *ACM Transactions on Cyber-Physical Systems*, vol. 3, no. 2, p. 13, 2018.

[11] K. Li, W. Ni, Y. Emami, Y. Shen, R. Severino, D. Pereira, and E. Tovar, "Design and implementation of secret key agreement for platoon-based vehicular cyber-physical systems," *ACM Transactions on Cyber-Physical Systems*, vol. 4, no. 2, pp. 1–20, 2019.

[12] K. Li, L. Lu, W. Ni, E. Tovar, and M. Guizani, "Secret key agreement for data dissemination in vehicular platoons," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 9, pp. 9060–9073, 2019.

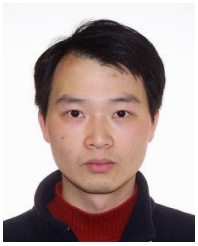
[13] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, pp. 17–30, 2009.

[14] K. Li, W. Ni, E. Tovar, and M. Guizani, "Optimal rate-adaptive data dissemination in vehicular platoons," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 10, pp. 4241–4251, 2019.

[15] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to algorithms*. MIT press, 2009.

7 BIOGRAPHIES

Kai Li [S'09-M'14-SM'20] (kai@isep.ipp.pt) is a Senior Research Scientist and Project Leader at CISTER Research Centre, Portugal. He is also a research fellow with Carnegie Mellon Portugal Research Program. He serves as the Associate Editor for IEEE Access Journal and Elsevier Ad Hoc Networks Journal since 2018.



Wei Ni [M'09-SM'15] (wei.ni@data61.csiro.au) received his B.E. and Ph.D. degrees from Fudan University, Shanghai, China, in 2000 and 2005, respectively. Currently he is the Group Leader, Cybernetics Group, CSIRO, Australia, and an adjunct professor at the University of Technology Sydney and honorary professor at Macquarie University. He serves as the Chair of the IEEE VTS NSW Chapter and an Editor for IEEE Transactions on Wireless Communications.

Jingjing Zheng (zheng@isep.ipp.pt) is currently working toward the Ph.D. degree with Electrical and Computer Engineering, University of Porto/CISTER Research Center, Porto, Portugal.

Eduardo Tovar (emt@isep.ipp.pt) is a Professor of Industrial Computer Engineering in the Computer Engineering Department, Polytechnic Institute of Porto (ISEP-IPP), and the director of CISTER, Portugal.

Mohsen Guizani [S'85-M'89-SM'99-F'09] (mguizani@ieee.org) received the B.S. (with distinction) and M.S. degrees in electrical engineering, and the M.S. and Ph.D. degrees in computer engineering from Syracuse University, Syracuse, NY, USA, in 1984, 1986, 1987, and 1990, respectively. He is currently a professor at the CSE Department at Qatar University, Qatar. He is an IEEE Fellow and a Senior Member of ACM.