CISTER
Research Centre in
Real-Time & Embedded
Computing Systems

Journal Paper

Secret Key Agreement for Data Dissemination in Vehicular Platoons

Kai Li*
Lingyun Lu
Wei Ni
Eduardo Tovar*
Mohsen Guizani

*CISTER Research Centre

CISTER-TR-190703

2019/07/02

Secret Key Agreement for Data Dissemination in Vehicular Platoons

Kai Li*, Lingyun Lu, Wei Ni, 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: kaili@isep.ipp.pt, lylu@bjtu.edu.cn, Wei.Ni@data61.csiro.au, emt@isep.ipp.pt

https://www.cister-labs.pt

Abstract

In a vehicular platoon, the lead vehicle that is responsible for managing the platoon's moving directions and velocity periodically disseminates messages to the following automated vehicles in a multi-hop vehicular network. However, due to the broadcast nature of wireless channels, this kind of communication is vulnerable to eavesdropping and message modification. Generating secret keys by extracting the shared randomness in a wireless fading channel is a promising way for wireless communication security. We study a security protocol for data dissemination in the platoon, where the vehicles cooperatively generate a shared secret key based on the quantized fading channel randomness. To improve conformity of the generated key, the probability of secret key agreement is formulated, and a novel secret key agreement algorithm is proposed to recursively optimize the channel quantization intervals, maximizing the key agreement probability. Numerical evaluations demonstrate that the key agreement probability achieved by our security protocol given different platoon size, channel quality, and number of quantization intervals. Furthermore, by applying our security protocol, the probability that the encrypted data being cracked by an eavesdropper is less than 5%.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2019.2926313, IEEE Transactions on Vehicular Technology

Secret Key Agreement for Data Dissemination in Vehicular Platoons

Kai Li, *Member, IEEE,* Lingyun Lu, Wei Ni, *Senior Member, IEEE,* Eduardo Tovar and Mohsen Guizani, *Fellow, IEEE*

***Abstract*—In a vehicular platoon, the lead vehicle that is responsible for managing the platoon's moving directions and velocity periodically disseminates messages to the following automated vehicles in a multi-hop vehicular network. However, due to the broadcast nature of wireless channels, this kind of communication is vulnerable to eavesdropping and message modification. Generating secret keys by extracting the shared randomness in a wireless fading channel is a promising way for wireless communication security. We study a security protocol for data dissemination in the platoon, where the vehicles cooperatively generate a shared secret key based on the quantized fading channel randomness. To improve conformity of the generated key, the probability of secret key agreement is formulated, and a novel secret key agreement algorithm is proposed to recursively optimize the channel quantization intervals, maximizing the key agreement probability. Numerical evaluations demonstrate that the key agreement probability achieved by our security protocol given different platoon size, channel quality, and number of quantization intervals. Furthermore, by applying our security protocol, the probability that the encrypted data being cracked by an eavesdropper is less than 5%.**

***Index Terms*—Autonomous vehicles, Data communication, Vehicular security, Optimization**

I. Introduction

Recent advances in inter-vehicle cognitive communications have enabled a new platoon-based driving pattern, in which the lead vehicle is manually driven and the others follow in a fully automatic manner (e.g., Safe Road Trains for the Environment project [1], and SafeCop project [2]). Each of the vehicles that follow maintains a small and nearly constant distance to its preceding vehicle [3]–[5]. In particular, Land Transport Authority in Singapore has planned to build dedicated smart highway lanes, on which the wirelessly connected vehicles move in platoons to increase the throughput of the roads [6]. The U.S. Department of Transportation has developed the Automated Highway as a future highway system, where vehicles drive in a tight formation of platoon at highway speeds [7].

Forming a vehicular platoon in highway scenarios is shown in Figure 1. The lead vehicle decides the platoon's driving status, i.e., driving speed, heading direction, acceleration/deceleration values, and road emergency. At time $T1$, the lead vehicle (managing the platoon) periodically broadcasts information on its vehicle position and velocity to update the platoon's vehicles. The following vehicle acts as a data-forwarding node, so that the messages from the leader can be disseminated to all vehicles in the platoon. In particular, the preceding vehicle disseminates the data to its following vehicle based on store-and-forward broadcasts at different times (e.g., $T2$, $T3$, and so on) without causing interference to other vehicles [8].

The platoon's driving status indicates emergent road conditions, such as traffic jams, crossroads, obstacles or car accidents [9], which affect mobility patterns of the platoon, e.g., decelerating, changing heading directions, and braking. However, due to the broadcast nature of wireless channels, vehicular communications in order to update the driving status in the platoon is vulnerable to eavesdropping and replay attacks [10]. Adversaries can launch attacks by tracking the locations of the vehicles of interest and abusing the mobility patterns of the platoon. Therefore, a secret key for data encryption/decryption is crucial to support data confidentiality, integrity, and sender authentication. In turn, it is also critical to the driving safety.

A key generation based on wireless fading channel randomness is a promising approach [11], [12], where two vehicles extract secret bits from the inherently random spatial and temporal variations of the reciprocal wireless channel between them. Essentially, the vehicles have to agree upon a shared secret key so that the disseminated data from the preceding vehicle can be successfully decoded by the following one. However, two critical challenges arise in the secret key agreement in the platoon. First, the channel between the two vehicles experiences independent and identically distributed (i.i.d.) additive white Gaussian noise (AWGN). Thus, it is difficult that multiple vehicles generate and agree on the shared secret key. Second, the channel randomness information obtained between a pair of vehicles cannot be transmitted over the insecure public channel that is observable to the eavesdropper, making it hard to reach key agreement in the platoon.

In this paper, we propose a new security protocol for the data dissemination in vehicular platoons to address both of the above challenges. Specifically, we consider that the vehicles in the platoon have been virtually grouped to multiple teams by applying state-of-the-art platoon/cluster management schemes [13], [14], as shown in Figure 1.

K. Li, and E. Tovar are with Real-Time and Embedded Computing Systems Research Centre (CISTER), 4249–015 Porto, Portugal (E-mail:{kaili,emt}@isep.ipp.pt).

L. Lu is with College of Computer Science, Beijing Jiaotong University, Beijing, P.R. China (E-mail: lylu@bjtu.edu.cn).

W. Ni is with Cyber-Physical System, Data61, Commonwealth Scientific and Industrial Research Organization (CSIRO), Sydney, N.S.W. 2122, Australia (E-mail: wei.ni@data61.csiro.au).

M. Guizani is with Computer Science and Engineering Department, Qatar University, Qatar (E-mail: mguizani@ieee.org).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2019.2926313, IEEE Transactions on Vehicular Technology

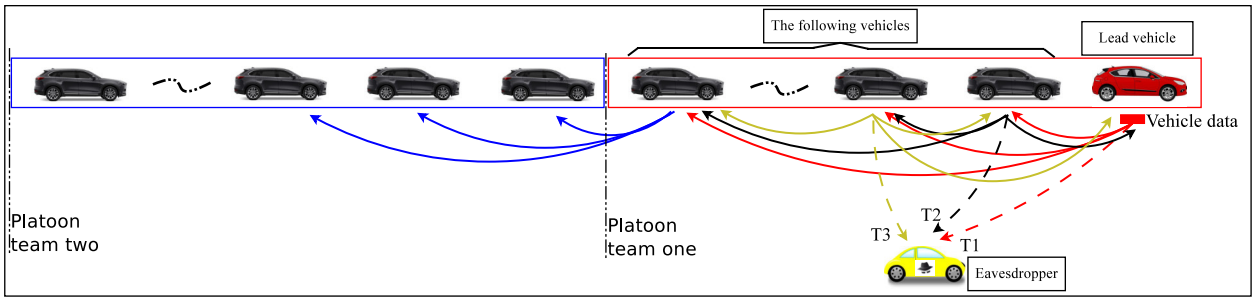

Fig. 1: A platoon of vehicles is composed of multiple teams. The vehicular information is disseminated by broadcasting over the insecure public channel.

The messages from the lead vehicle in a team are firstly delivered to the tail vehicle in the team. Then, the tail vehicle plays the role of the leader of the next team, and disseminates the messages to the tail vehicle in that team. Eventually, the messages from the lead vehicle of the first team can be disseminated to all teams in such way. In general, one dissemination cycle contains two stages, i.e., a secret key agreement period (SKAP) followed by an encrypted data transmission period (EDTP), where the two interchange periodically until all data packets from the lead vehicle are disseminated to the tail vehicle. During SKAP, the vehicles share channel randomness information by transmitting token packets. At the end of SKAP, we propose a Platooning Secret Key Agreement (PSKA) algorithm to quantize the channel gains between the vehicles, and cooperatively generate a unanimous secret key in the platoon, which is used for encrypting/decrypting of the disseminated packet in EDTP. The details on the protocol design will be investigated in Section III-A.

We also optimize the channel quality indicator (CQI) quantization intervals to maximize the key agreement probability by proposing a new recursive method, which recursively characterizes all the quantization intervals based on one of them. Note that the secret key is generated by the vehicle based on its quanzied fading channel randomness. In this case, the generated keys of all the vehicles could be different. Without optimizing the CQI quantization intervals, it would be difficult for multiple vehicles to agree on a shared secret key, leading to a poor key agreement probability. In addition, since the secret key generated by the PSKA algorithm comprehends the channel randomness over multiple vehicles, the eavesdropper at a different location experiences independent channel fading is not able to obtain the same key.

The rest of the paper is organized as follows. Section II presents the related work on link-based secret key generation and vehicle network security. Section III presents the communication protocol, channel model, and the PSKA algorithm for the vehicular platoon. In Section IV, CQI quantization intervals optimization is studied for secret key agreement. Simulation results are shown in Section V, followed by conclusions in Section VI.

II. Related Work

In this section, we review the literature on the link-based secret key generation and vehicular communication security.

A. Link-based secret key generation

Key generation that exploits reciprocity and randomness of wireless fading channels has attracted considerable research attention [15]–[24]. A physical-layer secret key generation scheme improves the communication security between two legitimate nodes with the help of multi-antenna untrusted relays [15]. The scheme is designed to increase the secret key rate for non-, partially, and fully colluding modes of relays, adapting to different channel coherence time. In [16], a secure secret key agreement protocol is developed for a three-node cooperative wireless network over block-fading relay channels. The protocol provides lower and upper bounds on the secret key rate based on an advantage distillation scheme. A secret key generation protocol is presented in [17], which utilizes artificial interference to contribute to changes of channel states. In particular, a helper node needs to be deployed for broadcasting artificial interference to change the measurement value of channel states when the sender sends data to the receiver. Wang *et al.* present a key generation protocol in narrowband fading channels, where the sender and the receiver extract the channel randomness with the aid of relay nodes [18]. Their protocol applies a time-slotted key generation scheme, where each relay node contributes a small portion of key bits so that the complete global key bit information is not available to the relays.

However, the key generation with the aid of relay nodes is not applicable to the vehicular platoon since employing relay vehicles can be costly. In addition, the key agreement with relays would cause extra latency on data dissemination, which can lead to cruise control failures due to lack of timely updates on the driving status.

In [19], mapping-varied spatial modulation is studied to generate the secret key, while the mapping patterns of radiated information and antenna information are varied according to instantaneous CQI pattern of the legitimate link. By assuming eavesdroppers are blind to the CQI over the legitimate link, the confidential information is secured from the eavesdroppers. Xu *et al.* develop key generation

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2019.2926313, IEEE Transactions on Vehicular Technology

algorithms for two scenarios in terms of network size, i.e., the three-node network and the multi-node network [20]. To improve the key rates, their strategy is based on a combination of well established point-to-point pairwise key generation technique, multi-segment scheme (i.e., divide each pairwise key into multi-segments), and one-time pad. In [21], a communication security scheme uses random bits transmission with waveform shaking to generate a shared key for near field communication devices. Their scheme randomly introduces synchronization offset and mismatch of amplitude and phase for each secret bit transmission to prevent a passive attacker from determining the generated key. In [22], the channel response from multiple orthogonal frequency-division multiplexing subcarriers is utilized to provide channel information for generating secret keys in static and mobile networks. In [23], the authors study a secret key generation for the multi-antenna transmitter. It integrates opportunistic beamforming and frequency diversity to generate the secret key in real time. A secret key agreement protocol is studied for a multi-user time-division duplex system, where a base station with a large antenna array shares secret keys with users in the presence of non-colluding eavesdroppers [24]. By exploiting a relation between received signal strengths at the eavesdropper and its target user, an estimator is derived to measure the downlink channel gain from the base station to the eavesdropper. The amount of information leakage is quantified based on the estimated channel gain for the secret key generation.

Generating secret keys by extracting the randomness of a wireless channel is studied to improve the communication security in cyber-physical systems [25]. Based on experiments on a 2-hop wireless sensor network testbed, it is observed that the distance between the nodes and the number of quantization intervals affect the secret key agreement. Hence, it is important to dynamically fine-tune the quantization intervals. A secret key generation testbed for platoon-based vehicular cyber-physical system security is built based on off-the-shelf autonomous robotic vehicles and TelosB wireless transceivers [26]. The key generation explores received signal strength (RSS) measurements and channel estimation of the inter-robot radio channels.

It is worth noting that the link-based secret key generation can also be applied to vehicular communications, where the inherent randomness of wireless channels between vehicles can be exploited to generate cryptographic keys. However, most of the studies available in the literature generate the key to encrypt point-to-point communications based on mutually-known channel information. This can hardly meet the critical need for the key agreement of multiple users, e.g., vehicular platoon, where the secret key has to be generated and conformed at each vehicle based on the local channel observation.

B. Vehicle network security

Using wireless link dynamics to generate a shared secret key for two vehicles is considered in [27]. A weighted sliding window smoothing is developed to reduce white noise and mismatched sensing time of the two vehicles. A learning scheme is presented to adjust the settings of key generation, such as readings of channel measurement, window size, and length of the key, to help tolerate the noise in different environments and offer steady performance. Also to achieve a secure communication between two vehicles, a physical layer key management scheme is designed to generate symmetric secret keys [28]. The secret key length is based on the application scenario and communication latency. However, most of the studies in vehicular secret key generation have focused on the point-to-point communications, which is different from the problem of interest.

In [29], roadside units (RSUs) are deployed in vehicular networks as semi-trusted intermediaries between vehicles and a certificate authority. A secure and lightweight privacy-preserving protocol is presented to provide mutual authentication between vehicles and RSUs. Jin *et al.* study a pairwise key generation to reduce the key generation delay in vehicular networks with RSUs and random arrival vehicles [30]. Tzeng *et al.* in [31] introduce an identity-based batch verification scheme to enhance security and privacy preservations for communications between RSUs and vehicles. In [32], the RSU is able to independently verify the outputs from the verification function of the proxy vehicles. In [33], a conditional privacy preservation protocol is presented based on a short-time anonymous key generation between a vehicle and the RSU. Unfortunately, the security techniques presented in the literature require to deploy authorized RSUs along the road for the secret key generation, which causes non-ignorable communication delay on the automated following vehicles.

In [34], an energy-efficient legitimate proactive eavesdropping strategy is studied for information surveillance in unmanned aerial vehicle networks, where a legitimate surveilling vehicle overhears the communication of suspicious vehicles while tracking their movement. The jamming power of the legitimate vehicle is optimized to maximize the eavesdropping rate. An eavesdropping and jamming selection policy is presented to monitor malicious communications based on power consumption of the vehicles at different locations [35], [36]. The performance of the selection policy is evaluated under four typical wireless fading channel models, i.e., Rayleigh, Ricean, Weibull, and Nakagami.

III. Platooning Data Dissemination Security

In this section, we present a 2-stage communication protocol for the secure data dissemination in the vehicular platoon, followed by a radio channel model.

A. Secure data dissemination protocol

In the vehicular platoon, each intermediate vehicle acts as a data-forwarding node in a multi-hop vehicular network. In particular, a preceding vehicle disseminates the data to its following vehicle based on store-and-forward broadcasts. Given n vehicles in a platoon, the data dissemination in

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2019.2926313, IEEE Transactions on Vehicular Technology

the platoon forms (n-1) wireless hops. The vehicles are traveling in a straight single-lane highway with no need to change the platoon size or perform maneuvers (split, merge, leave, etc.), keeping the operations of the cruise control simple. The tracking of the vehicles in the platoon can be addressed by using the cooperative localization techniques [37], [38]. Moreover, traveling on a straight highway also allows the platoon to drive at highway speeds, where the key agreement problem is more critical than the one at low speeds.

In terms of the data dissemination security, we propose a 2-stage communication model, with secret key agreement period (SKAP) followed by encrypted data transmission period (EDTP) (see Figure 2). The two periods interchange periodically until all data packets from the lead vehicle are disseminated to the tail vehicle.

The purpose of SKAP is to share link information among the vehicles. Specifically, the ID number of v_i fits in a single token packet (TB$_i$) [39], where $i \in [1, n-1]$. Transmitting the token packet is initialized by the lead vehicle, which solely decides the driving status. TB$_i$ is broadcasted by v_i so that the following vehicle can measure the channel quality between v_i and itself. Once TB$_i$ is successfully received by the next vehicle, i.e., v_{i+1}, v_{i+1} sends TB$_{i+1}$ to the following vehicle all the way to the tail vehicle v_n. The vehicles in each team of the platoon check the radio channel by using carrier sensing to avoid packet collisions with the token transmission in other teams. The sender vehicle has to back off a random time to sense the channel again in case the token packet collision happens. Moreover, the token packet TB$_{i+1}$ is also an acknowledgement to TB$_i$. In particular, if TB$_{i+1}$ is not received by v_i, which indicates that TB$_i$ is not successfully received by v_{i+1}, then TB$_i$ will be retransmitted by v_i. At the end of SKAP, when all the vehicles in the team finish the token transmission, the PSKA algorithm is carried out to generate a unanimous secret key adapted to the time-varying channel, which will be discussed later in this section.

In terms of the encrypted data transmission, at the first time slot of EDTP in the dissemination cycle, the lead vehicle v_1 uses its secret key generated by the PSKA algorithm to encrypt its DATA packet, and immediately forwards to the posterior vehicle v_2. The following vehicles forward the received DATA packet all the way to the tail vehicle while using the generated secret key for the packet decryption. In addition, to enhance the transmission reliability of the DATA packet, the following vehicles utilize one-hop vehicle-to-vehicle communication [40], e.g., Wireless Access in Vehicular Environments (WAVE), or Dedicated Short-Range Communication (DSRC) [41], [42], which provides a collision-free transmission in EDTP.

From the perspective of an adversary, the eavesdropper overhears the TB packet in SKAP for generating the same secret key. However, the secret key generated by the PSKA algorithm comprehends the channel randomness over multiple vehicles (details will be given in later sections). The distance between the eavesdropper and any one of platooning vehicles is different from the one between any two vehicles in the platoon, which leads to independent channel fading. As a result, the eavesdropper is not able to generate the same secret key to decode the DATA packet in EDTP.

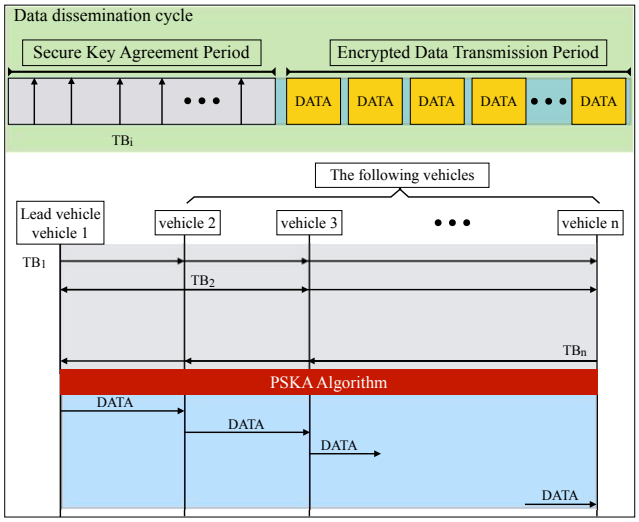

Fig. 2: The communication protocol for the secret key agreement and data dissemination in the vehicular platoon, where TB$_i$ is a token packet transmitted by vehicle i.

B. Channel model in vehicular platoons

In vehicular platoons, Line of Sight (LOS) communication between the vehicles is typically available as the vehicles travel on the same road segment and the antennas can be installed on top of each of the vehicles. Thus, a large-scale path loss that has taken the average effect of multipath into account is considered to model the inter-vehicle communication channel. Let P_i^{tx} denote the transmit power (in dB) of TB$_i$ at v_i. The receiving signal power at v_j ($j \in [i+1, n]$) is

$$P_j^{rx} = P_i^{tx} + \vartheta - 10\eta_{PL}\log_{10}(d_{i,j}) + \phi_{i,j}, \qquad (1)$$

where ϑ is a positive fixed constant relating to the channel, and η_{PL} is the path loss coefficient. The term $\phi_{i,j}$ denotes an independent shadow fading over different time epochs. $d_{i,j}$ in (1) is the distance between v_i and v_j, which can be further written as

$$d_{i,j} = 10^{\frac{H_{i,j}+\vartheta+\phi_{i,j}}{10\eta_{PL}}}, \qquad (2)$$

where $H_{i,j} = (P_i^{tx} - P_j^{rx})$ presents the channel gain of the link between sender v_i and receiver v_j.

Table I shows $H_{i,j}$, which is obtained after TB$_i$ is received by v_j from v_i. However, v_j is not aware of the channels between the other vehicles in the team, e.g., $H_{i,j-1}$. As a result, the secret key generated at different vehicles could be different from each other due to independent channel variations. Fortunately, as the inter-vehicle distance with random variance can be known statistically before forming the platoon, the channel gain between any other two platooning vehicles in highway scenarios can be estimated by v_j based on their distance gap, i.e.,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2019.2926313, IEEE Transactions on Vehicular Technology

TABLE I: Channel quality obtained at v_j after TB_i is received from v_i.

Token	$H_{i,j}$ obtained at v_j						
TB_1	—	$H_{1,2}$	$H_{1,3}$	$H_{1,4}$	...	$H_{1,j}$	...
TB_2	$H_{2,1}$	—	$H_{2,3}$	$H_{2,4}$	...	$H_{2,j}$	...
TB_3	$H_{3,1}$	$H_{3,2}$	—	$H_{3,4}$	...	$H_{3.j}$	...
TB_4	$H_{4,1}$	$H_{4,2}$	$H_{4,3}$	—	...	$H_{4,j}$	...
...	...	...	...	...	...	...	...
TB_i	$H_{i,1}$	$H_{i,2}$	$H_{i,3}$	$H_{i,4}$	...	—	...
...	...	...	...	...	...	...	...

$d_{i,j-1} = d_{i,j} - d_{j-1,j}$. Thus, we have $10^{\frac{H_{i,j-1}+\vartheta+\phi_{i,j-1}}{10\eta_{PL}}} = 10^{\frac{H_{i,j}+\vartheta+\phi_{i,j}}{10\eta_{PL}}} - 10^{\frac{H_{j-1,j}+\vartheta+\phi_{j-1,j}}{10\eta_{PL}}}$ with regards to (2), which is

$$H_{i,j-1} + \phi_{i,j-1} = H_{i,j} + \phi_{i,j} + 10\eta_{PL}\log(1 - 10^{\frac{H_{j-1,j}+\phi_{j-1,j}-H_{i,j}-\phi_{i,j}}{10\eta_{PL}}}). \quad (3)$$

C. Platooning secret key agreement

As shown in Figure 3, the steps that incorporate the secret key agreement during the SKAP in the proposed security protocol mainly include: channel gain measurement, CQI quantization, and platooning secret key generation.

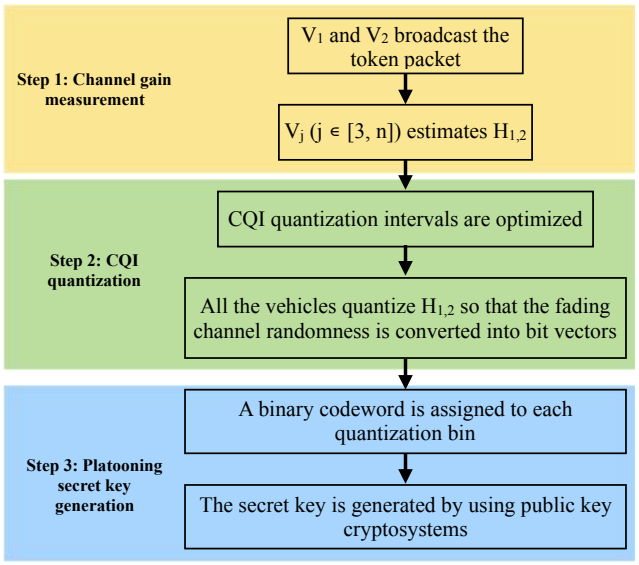

Fig. 3: The steps that incorporate the secret key agreement during the SKAP in the proposed security protocol.

Step 1: Channel gain measurement. v_i broadcasts TB_i in turn during the SKAP, where $i \in [1, 2]$. The following vehicle v_j ($j \in [3, n]$) measures Signal-to-Noise ratio (SNR) of the link between v_i and v_j according to the reception of TB_i. For illustration convenience, in this article, the first two vehicles, i.e., v_1 and v_2 are considered as token packet transmitters. v_j ($j \in [3, n]$) estimates the channel gain between v_1 and v_2, i.e., $H_{1,2}$, based on TB_1 and TB_2, using (3).

Step 2: CQI quantization. v_1 and v_2 quantize $H_{1,2}$, while the following vehicle v_j ($j \in [3, n]$) quantizes the estimated $H_{1,2}$ according to a predetermined quantization method so that the fading channel randomness is converted into bit vectors. Let ξ_l and L denote the l-th quantization interval and the total number of quantization intervals, respectively, where $l \in [1, L-1]$. We propose to optimize the CQI quantization intervals (denoted by $\xi_l^\star$) to maximize the key agreement probability, as will be described in Section IV.

Step 3: Platooning secret key generation. By applying $\xi_l^\star$ in Step 2, $H_{1,2}$ is quantized by each vehicle to one of the quantization intervals, i.e., $[\xi_l^\star, \xi_{l+1}^\star]$ ($l \in [1, L-1]$). Classical encoding techniques can be utilized to assign a binary codeword to each quantization bin $[\xi_l^\star, \xi_{l+1}^\star]$ for extracting the secret key. Based on the obtained binary codeword, public key cryptosystems are employed to generate the secret key to encrypt and protect the transmissions at every hop.

Actually, it can be known that the more vehicles transmitting the token packet, the higher key agreement probability can be achieved. Thus, reducing the number of token transmitters explores the key agreement performance in the worst case, though the proposed secret key agreement algorithm can also be applied to the platoon that more than two token packet transmitters. Moreover, for the accurate channel estimation, the platooning secret key is generated when the platoon is in linear formation. The security strength of the proposed approach is guaranteed based on the fact that it is infeasible for an adversary which is located at a different place with the transceivers to obtain the identical channel randomness for key generation. The details of the PSKA algorithm are presented in the following section.

IV. Optimization Of CQI Quantization Intervals

In this section, we first optimize the CQI quantization intervals in small and large platoon size, respectively. This is because problem formulation of the optimization under a small platoon size is easy to be simplified and validated. Similarly, the formulation that extends to large platoon size is easy to follow. Next, we study a new recursive algorithm that achieves platooning secret key agreement by optimizing the CQI quantization intervals to maximize the secret key agreement probability [43]. Additionally, we present the probability that the eavesdropper generates the same secret key as the platooning vehicles.

A. Three-vehicle platoon team

We first consider a small platoon of three vehicles. According to Step 1 in Section III-C, TB_1 is received by

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2019.2926313, IEEE Transactions on Vehicular Technology

vehicles v_2 and v_3, and TB_2 is received by vehicles v_1 and v_3. Let x_1, x_2, and x_3 define the random variables of $H_{1,2}$, $H_{2,3}$, and $H_{1,3}$, respectively. Given that the inter-vehicle channel is symmetric, $H_{1,2} = H_{2,1}$, $H_{2,3} = H_{3,2}$, and $H_{1,3} = H_{3,1}$. Based on (3), the randomness of packet reception at v_3 contains two parts, one is between v_1 and v_2, i.e., $x_1 + x_3$, and the other is between v_2 and v_3, i.e., x_2. Moreover, the quantization interval with the channel estimation error at v_3 needs to be larger than the mean error of the data reception at v_3, which is $\left|\frac{x_1+x_3-x_2}{2}\right|$.

Namely, $\xi_l + \left|\frac{x_1-(x_3-x_2)}{2}\right| \leq \left|\frac{x_1+x_3-x_2}{2}\right| \leq \xi_{l+1} - \left|\frac{x_1-(x_3-x_2)}{2}\right|$.

Proof: If $x_1 \geq x_3 - x_2$, ξ_l has to be smaller than $x_3 - x_2$, and ξ_{l+1} needs to be larger than x_1. Thus, we have

$$\xi_l \leq \frac{x_1 + x_3 - x_2}{2} - \frac{x_1 - x_3 + x_2}{2},$$
$$\xi_l + \frac{x_1 - (x_3 - x_2)}{2} \leq \frac{x_1 + x_3 - x_2}{2}. \tag{4}$$

Moreover, we can know $\xi_l + (-\frac{x_1-(x_3-x_2)}{2}) \leq \frac{x_1+x_3-x_2}{2}$ if $x_1 < (x_3 - x_2)$.

Similarly, given $\xi_{l+1} \geq x_1$, we know

$$\begin{cases} \xi_{l+1} - \frac{x_1-(x_3-x_2)}{2} \geq \frac{x_1+x_3-x_2}{2}, \text{ if } x_1 \geq (x_3 - x_2) \\ \xi_{l+1} - (-\frac{x_1-(x_3-x_2)}{2}) \geq \frac{x_1+x_3-x_2}{2}, \text{ if } x_1 < (x_3 - x_2) \end{cases} \tag{5}$$

Thus, we have $\xi_l + \left|\frac{x_1-(x_3-x_2)}{2}\right| \leq \left|\frac{x_1+x_3-x_2}{2}\right| \leq \xi_{l+1} - \left|\frac{x_1-(x_3-x_2)}{2}\right|$. ■

More specifically, if $x_1 \geq x_3 - x_2$, we know $\xi_l \leq x_3 - x_2$ and $\xi_{l+1} \geq x_1$. In this case, the probability is $\Pr(\xi_l \leq x_3 - x_2 \mid x_1 \geq x_3 - x_2) \Pr(\xi_{l+1} \geq x_1 \mid x_1 \geq x_3 - x_2) \Pr(x_1 \geq x_3 - x_2)$. Otherwise, we have $\xi_l \leq x_1$, and $\xi_{l+1} \geq x_3 - x_2$ with the probability of $\Pr(\xi_l \leq x_1 \mid x_1 < x_3 - x_2) \Pr(\xi_{l+1} \geq x_3 - x_2 \mid x_1 < x_3 - x_2) \Pr(x_1 < x_3 - x_2)$. Let ξ^{v_1}, ξ^{v_2}, and ξ^{v_3} denote the quantized values of $H_{1,2}$, $H_{2,3}$, and $H_{1,3}$, respectively. The probability that the three vehicles attain the same quantization interval, i.e., $[\xi_l, \xi_{l+1}]$, can be given by (see Appendix for details)

$$\Pr\left\{\xi^{v_1}, \xi^{v_2}, \xi^{v_3} \in [\xi_l, \xi_{l+1}]\right\} = \frac{\Pr(\xi_l \leq x_3 - x_2 \leq x_1 \leq \xi_{l+1})}{\Pr(x_1 \geq x_3 - x_2)} + \frac{\Pr(\xi_l \leq x_1 < x_3 - x_2 \leq \xi_{l+1})}{\Pr(x_1 < x_3 - x_2)}, \tag{6}$$

Furthermore, the inter-vehicle channel captures the effects of path-loss, shadowing, and i.i.d AWGN. We consider the scenario in which the fading coefficients are known to (i.e., accurately measured by,) the appropriate receivers, but not known to (or not exploited by,) the transmitters. Statistically, we model the distribution of $H_{1,2}$ as Gaussian random variables with zero mean and variance $\sigma_{1,2}^2$, so that $|H_{1,2}|^2$ is exponentially distributed with parameter $1/\sigma_{1,2}^2$ and the phases are uniformly distributed on $[0, 2\pi)$. Without loss of generality, the distribution of $H_{1,2}$ observed at v_1 and v_2 follows

$$x_1 \backsim \mathcal{N}(0, \sigma_{1,2}^2), \tag{7}$$

To attain the same quantization interval as v_1 and v_2, v_3 estimates channel attenuation of the link between v_1 and v_2 according to $(x_3 - x_2)$, and the channel estimation error follows

$$x_3' = (x_3 - x_2) \backsim \mathcal{N}(0, \sigma_{1,3}^2 + \sigma_{2,3}^2). \tag{8}$$

Given the general expression for the probability density function (PDF) of the channel distribution, $f(x) = \frac{1}{\sqrt{2\pi}\sigma} \exp(-\frac{x^2}{2\sigma^2})$, we have the joint PDF of ξ^{v_1} and ξ^{v_3}, i.e.,

$$\Phi(x_1, x_3') = \frac{e^{-\frac{x_1^2}{2\sigma_{1,2}^2} - \frac{(x_3')^2}{2(\sigma_{1,3}^2+\sigma_{2,3}^2)}}}{2\pi\sqrt{2\pi\sigma_{1,2}^2(\sigma_{1,3}^2 + \sigma_{2,3}^2)}}. \tag{9}$$

Figure 4 numerically plots $\Phi(x_1, x_3')$ based on the distribution of ξ^{v_1} and ξ^{v_3}. It is observed that the tail vehicle has a larger variance than the others due to the error propagation of channel estimation, which confirms correctness of $\Phi(x_1, x_3')$.

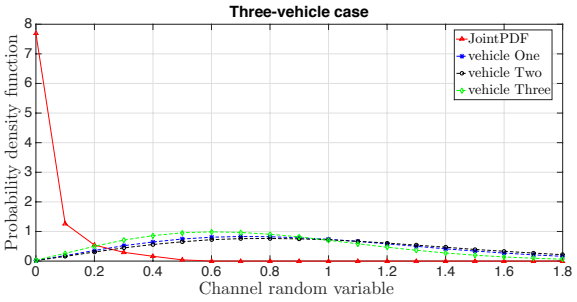

Fig. 4: The joint PDF of ξ^{v_1}, ξ^{v_2}, and ξ^{v_3} when $n = 3$.

Based on (6), $\Pr(\xi_l \leq x_3' \leq x_1 \leq \xi_{l+1})$ and $\Pr(\xi_l \leq x_1 < x_3' \leq \xi_{l+1})$ can be achieved by taking the integral $\iint_{[\xi_l, \xi_{l+1}]} \Phi(x_1, x_3') dx_1 dx_3'$, while $\Pr(x_3' \leq x_1)$ and $\Pr(x_1 < x_3')$ are fixed due to the known channel distribution. Therefore, consider the $\log_2^L$-bit channel quantization in **Step 2** of Section III-C at each vehicle. We have the desired probability when the channel gains, ξ^{v_1}, ξ^{v_2} and ξ^{v_3}, are quantized to the same l-th CQI quantization interval ξ_l $(l = 1, \cdots, L-1)$, which is

$$\Pr\left\{\xi^{v_1}, \xi^{v_2}, \xi^{v_3} \in [\xi_l, \xi_{l+1}]\right\} = \iint_{[\xi_l, \xi_{l+1}]} \Phi(x_1, x_3') dx_1 dx_3'$$

$$= \frac{\sqrt{\pi}}{4\pi\sqrt{2}} \left(\text{erf}(\frac{\xi_{l+1}}{\sqrt{2\sigma_{1,2}^2}}) - \text{erf}(\frac{\xi_l}{\sqrt{2\sigma_{1,2}^2}})\right) \cdot \left(\text{erf}(\frac{\xi_{l+1}}{\sqrt{2(\sigma_{1,3}^2 + \sigma_{2,3}^2)}}) - \text{erf}(\frac{\xi_l}{\sqrt{2(\sigma_{1,3}^2 + \sigma_{2,3}^2)}})\right). \tag{10}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2019.2926313, IEEE Transactions on Vehicular Technology

We proceed to optimize the quantization intervals to maximize the key agreement probability, for the sake of the secret key agreement in SKAP (as shown in Figure 2). Due to independent and identically distributed ($i.i.d$) random channels, the problem is formulated by

$$\textbf{P1:} \quad \max_{\{\xi_l\}} \sum_{l=1}^{L-1} \Pr\left\{\xi^{v_1}, \xi^{v_2}, \xi^{v_3} \in [\xi_l, \xi_{l+1}]\right\}$$

According to **Step 3** in Section III-C, a unique secret key is extracted at the platooning vehicle, and is used to encrypt the transmitted data.

B. n-vehicle platoon team

We consider an n number of vehicles in the platoon, where $n \geq 3$. Similar to the three-vehicle case, we also consider the first two platooning vehicles, i.e., v_1 and v_2, transmit the token packet. Note that our formulation can be extended to any number of sender vehicles given the channel gain between two vehicles v_i and v_j ($\forall i, j \in [1, n]$) in Table I. Moreover, the distribution of the channel between vehicles v_1 and v_2 is estimated by the following vehicle v_i ($i \geq 3$) when it receives TB_1 and TB_2, which follows

$$x_i' = (x_i - x_{i-1}) \backsim \mathcal{N}(0, \sigma_{1,i}^2 + \sigma_{2,i}^2). \tag{11}$$

Accordingly, the joint PDF of the channel distribution observation at the vehicles is

$$\Phi(x_1, \ \ldots \ x_n') = \frac{e^{-\frac{x_1^2}{2\sigma_{1,2}^2} - \frac{(x_3')^2}{2(\sigma_{1,3}^2+\sigma_{2,3}^2)} - \ldots - \frac{(x_n')^2}{2(\sigma_{1,n}^2+\sigma_{2,n}^2)}}}{\sqrt{(2\pi)^n \sigma_{1,2}^2(\sigma_{1,3}^2+\sigma_{2,3}^2)\ldots(\sigma_{1,n}^2+\sigma_{2,n}^2)}}. \tag{12}$$

In the case of $n \geq 3$, the desired probability that the channel quantization at all vehicles fall into the same interval is given by (13). Specifically, the distribution of the channel measurement is statistically modeled as lognormal distributions by using typically the least square (LS) curve fitting. The path loss exponent is meticulously calibrated so that the residual errors (or variations) of the channel measurements in the log-domain are Gaussian. As observed in (13), the channel estimation error at the vehicle v_i with the channel measurement randomness can affect the key agreement probability in the vehicular platoon. Therefore, we consider to optimize the quantization intervals of n vehicles to achieve the key agreement, given the channel randomness.

Similar to **P1**, the optimal allocation of $\{\xi_l, \xi_{l+1}\}$ ($l \in [1, L-1]$) is obtained by solving the following problem

$$\textbf{P2:} \quad \max_{\{\xi_l\}} \left\{P_L\right\}$$

where $P_L = \sum_{l=1}^{L-1} \Pr\left\{\xi^{v_1}, \xi^{v_2}, ..., \xi^{v_n} \in [\xi_l, \xi_{l+1}]\right\}_{n \geq 3}$.

Apparently, the partial derivative of P_L with respect to ξ_l depends on its adjacent CQI quantization intervals, ξ_{l-1} and ξ_{l+1} (in case of $l = L-1$, only ξ_l, and itself, ξ_{l+1}). Since $\xi_L = +\infty$ and $\text{erf}(+\infty) = 1$, the partial derivative can be given by (14), where $l \in [1, L-1]$. By exploiting the first-order necessary condition of a maximum on (14), $\partial P_L / \partial \xi_l = 0$ can be rewritten as (15). The optimal solution can be given by $\xi_l^* = \arg(G(\xi_l^*))$, where $G(\xi_l^*)$ denotes the LHS of (15). As $\partial P_L / \partial \xi_l < 0$, P_L monotonically decreases, which indicates that ξ_l^* is the optimal CQI quantization interval maximizing P_L.

According to (14), we can also observe that $\xi_l^\star$ is a function of $\xi_{l-1}^\star$, i.e., $\xi_l^\star = G(\xi_{l-1}^\star)$. Thus, the problem now is to obtain $\xi_{l-1}^\star$, where $\xi_{l-1}^\star = \arg(G(\xi_l^\star))$. Recursively, when $l = 2$, we have $\xi_1^\star = \arg(G(\xi_2^\star))$. Since $\xi_1^\star = 0$ is known apriori, $\xi_l^\star$ ($l \in [1, L-1]$) can be recursively optimized.

Note that two vehicles v_1 and v_2 are considered to transmit the token in **P2**. However, the formulation of optimal CQI quantization can be further extended to the case where the number of vehicles transmitting the token is more than two. In this case, the joint PDF of the channel distribution needs to be considered for multiple vehicles that transmit the token. Moreover, each platooning vehicle needs to estimate all the channels among the token sender vehicles.

C. Secret key generation

Next, we demonstrate the PSKA algorithm to optimize the channel quantization intervals and generate the unanimous secret key, as shown in Algorithm 1. Specifically, $\xi_l^\star$ ($1 \leq l \leq L$) is obtained by conducting **Steps 1 and 2** to derive (15). Note that any two vehicles in the platoon using the same channel quantization intervals generate the same secret key. In the case that the inter-vehicle channels in the platoon experience a large variation of random noise and significant estimation errors, $\xi_l^\star$ and $\xi_{l+1}^\star$ in **P1** and **P2** can be optimized to the lower bound or upper bound of the quantization intervals, i.e., $\xi_l^\star = \xi_0$ and $\xi_{l+1}^\star = \xi_{L+1}$. As a result, the bits in the unified secret key at each vehicle could be either all zeros or all ones so as to maximize the key agreement probability.

In terms of the platooning secret key generation in **Step 3**, firstly, the vehicle v_i ($i \geq 3$) quantizes the channel between v_1 and v_2 based on $H_{1,2}^{v_i} = (H_{1,i} - H_{2,i})$. As the value of $H_{1,2}^{v_i}$ is within $[\xi_l^\star, \xi_{l+1}^\star]$, where $1 \leq l \leq L-1$, an encoding scheme, i.e., $f_{\text{encoding}}^{v_i}(l, l+1)$ is utilized to assign a binary codeword to each quantization bin $[\xi_l^\star, \xi_{l+1}^\star]$ for extracting the secret key K_i. Without loss of generality, we implement Gray coding as an example of $f_{\text{encoding}}^{v_i}(l, l+1)$ as follows.

- Let $k_i(l)$, $l \in [1, L-1]$ denote the complement bit of the codeword, where

$$k_i(l) = \begin{cases} 1, \ l \mod 4 \geq 2; \\ 0, \ \text{otherwise}. \end{cases} \tag{16}$$

- Generate a Gray codeword list whose two neighboring codewords only have one-bit difference. Moreover, the list contains 2^Q possible codewords, where Q denotes length of the Gray codeword.
- Define $f_i^+(l) = \lfloor (l-1)/4 \rfloor$. Thus, $K_i^+(l) \in \{0,1\}^Q$ is the $f_i^+(l)$-th Gray codeword.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2019.2926313, IEEE Transactions on Vehicular Technology

$$\begin{aligned}
&\Pr\left\{\xi^{v_1},\xi^{v_2},...,\xi^{v_n}\in[\xi_l,\xi_{l+1}]\right\}_{n\geq 3}\\
&=\int\cdots\int_{[\xi_l,\xi_{l+1}]}\Phi(x_1,\ ...\ x_n')dx_1...dx_n'\\
&=\frac{\pi\Big(\text{erf}(\sqrt{\frac{1}{2\sigma_{1,2}^2}}\xi_{l+1})-\text{erf}(\sqrt{\frac{1}{2\sigma_{1,2}^2}}\xi_l)\Big)}{2\sqrt{(2\pi)^n(\sigma_{1,3}^2+\sigma_{2,3}^2)...(\sigma_{1,n}^2+\sigma_{2,n}^2)}}\prod_{n\geq 3}\sqrt{\frac{\pi(\sigma_{1,n}^2+\sigma_{2,n}^2)}{2}}\Big(\text{erf}(\sqrt{\frac{1}{2(\sigma_{1,n}^2+\sigma_{2,n}^2)}}\xi_{l+1})-\text{erf}(\sqrt{\frac{1}{2(\sigma_{1,n}^2+\sigma_{2,n}^2)}}\xi_l)\Big)
\end{aligned}\tag{13}$$

$$\begin{aligned}
\frac{\partial P_L}{\partial\xi_l}&=\frac{\partial\sum_{l=1}^{L}\int\cdots\int_{[\xi_l,\xi_{l+1}]}\frac{e^{-\frac{x_1^2}{2\sigma_{1,2}^2}-\frac{(x_3')^2}{2(\sigma_{1,3}^2+\sigma_{2,3}^2)}-\cdots-\frac{(x_n')^2}{2(\sigma_{1,n}^2+\sigma_{2,n}^2)}}}{\sqrt{(2\pi)^n\sigma_{1,2}^2(\sigma_{1,3}^2+\sigma_{2,3}^2)\cdots(\sigma_{1,n}^2+\sigma_{2,n}^2)}}dx_1...dx_n'}{\partial\xi_l}\\
&=\frac{\pi\prod_{n\geq 3}\sqrt{\frac{\pi(\sigma_{1,n}^2+\sigma_{2,n}^2)}{2}}}{2\sqrt{(2\pi)^n(\sigma_{1,3}^2+\sigma_{2,3}^2)...(\sigma_{1,n}^2+\sigma_{2,n}^2)}}\cdot\\
&\Big(\frac{-2e^{-\frac{1}{2\sigma_{1,2}^2}\xi_l^2}}{\sqrt{\pi}}\Big(\text{erf}(\sqrt{\frac{1}{2\sigma_{1,2}^2}}\xi_{l+1})-\text{erf}(\sqrt{\frac{1}{2\sigma_{1,2}^2}}\xi_l)\Big)\prod_{n\geq 3}\Big(\text{erf}(\sqrt{\frac{1}{2(\sigma_{1,n}^2+\sigma_{2,n}^2)}}\xi_{l+1})-\text{erf}(\sqrt{\frac{1}{2(\sigma_{1,n}^2+\sigma_{2,n}^2)}}\xi_l)\Big)+\\
&\sum_{n\geq 3}\Big(\text{erf}(\sqrt{\frac{1}{2\sigma_{1,2}^2}}\xi_{l+1})-\text{erf}(\sqrt{\frac{1}{2\sigma_{1,2}^2}}\xi_l)\Big)\prod_{n\geq 3,n'\neq n}\frac{-2e^{-\frac{1}{2(\sigma_{1,n}^2+\sigma_{2,n}^2)}\xi_l^2}}{\sqrt{\pi}}\Big(\text{erf}(\sqrt{\frac{1}{2(\sigma_{1,n'}^2+\sigma_{2,n'}^2)}}\xi_{l+1})-\text{erf}(\sqrt{\frac{1}{2(\sigma_{1,n'}^2+\sigma_{2,n'}^2)}}\xi_l)\Big)\Big)
\end{aligned}\tag{14}$$

$$\begin{aligned}
&\Big(\frac{-2e^{-\frac{1}{2\sigma_{1,2}^2}\xi_l^2}}{\sqrt{\pi}}\Big(1-\text{erf}(\sqrt{\frac{1}{2\sigma_{1,2}^2}}\xi_l)\Big)\prod_{n\geq 3}\Big(1-\text{erf}(\sqrt{\frac{1}{2(\sigma_{1,n}^2+\sigma_{2,n}^2)}}\xi_l)\Big)+\sum_{n\geq 3}\Big(1-\text{erf}(\sqrt{\frac{1}{2\sigma_{1,2}^2}}\xi_l)\Big)\cdot\\
&\prod_{n\geq 3,n'\neq n}\frac{-2e^{-\frac{1}{2(\sigma_{1,n}^2+\sigma_{2,n}^2)}\xi_l^2}}{\sqrt{\pi}}\Big(1-\text{erf}(\sqrt{\frac{1}{2(\sigma_{1,n'}^2+\sigma_{2,n'}^2)}}\xi_l)\Big)\Big)=0
\end{aligned}\tag{15}$$

- Define $f_i^-(l)=\lfloor((l+1)\mod L)/4\rfloor$. Thus, $K_i^-(l)\in\{0,1\}^Q$ is the $f_i^-(l)$-th Gray codeword. Moreover, $K_i^-(l)$ can be the codeword list that circularly shifts $K_i^+(l)$ by two elements.

Note that $f_{\text{encoding}}^{v_i}(l,l{+}1)$ can be employed by other existing encoding schemes, e.g., Gillham coding, and Lucal coding.

Based on the codeword of $f_{\text{encoding}}^{v_i}(l,l+1)$, well-studied symmetric or asymmetric secret keys can be straightforwardly generated to encrypt and protect the transmissions at every hop. Take Elliptic-curve cryptography (ECC) for example. v_i and v_{i+1} agree on an elliptic curve and a base point G. They generate private keys K_i^{prv} and K_{i+1}^{prv}, and the corresponding public keys $K_i^{\text{pub}}=K_i^{\text{prv}}*G$ and $K_{i+1}^{\text{pub}}=K_{i+1}^{\text{prv}}*G$, where $*$ stands for the operation of elliptic curve scalar multiplication. In particular, v_i and v_{i+1} agree with the same private key after executing PSKA algorithm, i.e., $K_i^{\text{prv}}=K_{i+1}^{\text{prv}}$. Therefore, we have $K_i^{\text{pub}}=K_{i+1}^{\text{pub}}$. v_i computes $K_i^{\text{prv}}*K_{i+1}^{\text{pub}}$, and v_{i+1} computes $K_{i+1}^{\text{prv}}*K_i^{\text{pub}}$, and both vehicles can achieve a common shared secret $S=K_i^{\text{prv}}*K_{i+1}^{\text{pub}}=K_{i+1}^{\text{prv}}*K_i^{\text{pub}}=K_i^{\text{prv}}*K_{i+1}^{\text{prv}}*G=K_{i+1}^{\text{prv}}*K_i^{\text{prv}}*G$. Such a ECC-based secret key can be generated and verified with the Elliptic Curve Digital Signature Algorithm [44]. The key generation and encryption are straightforward and beyond the scope of this paper.

Algorithm 1 Platooning Secret Key Agreement with Optimal CQI Quantization Intervals

1: **Initialize:** n, L, TB_1, TB_2, $\{\xi^{v_1},\xi^{v_2},...,\xi^{v_n}\}=0$, $\xi_1=0$, $\xi_L=+\infty$.
2: **Optimal Channel Quantization:**
3: TB_1 and TB_2 are broadcasted in sequence.
4: $\xi^{v_i}\leftarrow\mathcal{N}(0,\sigma_{1,i}^2+\sigma_{2,i}^2)$, where $i\in[1,n]$.
5: **while** $1\leq l\leq L-1$ **do**
6: $\quad\xi_{l+1}^{\star}\leftarrow$ (15).
7: $\quad l\leftarrow l+1$.
8: **end while**
9: **Output:** $\{\xi_1^*,...,\xi_L^*\}$.
10: **Generate PSK:**
11: $H_{1,2}^{v_i}\leftarrow(H_{1,i}-H_{2,i})$, where $\forall i\in[3,n]$.
12: **if** $H_{1,2}^{v_i}\in[\xi_l^{\star},\xi_{l+1}^{\star}]$ **then**
13: $\quad K_i\leftarrow f_{ECC}(f_{\text{encoding}}^{v_i}(l,l+1))$.
14: **end if**
15: The secret key is used by v_i to encrypt/decrypt the data.
16: **Output:** $\{\xi_1^*,...,\xi_L^*\}$ and the Q-bit secret key.

Note that multiple token packets can be transmitted by vehicle v_1 and v_2 in one data dissemination cycle. In this case, the PSKA algorithm can be conducted in Δ iterations ($\Delta\geq 1$), and Δ secret keys can be generated

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2019.2926313, IEEE Transactions on Vehicular Technology

at each vehicle. The larger Δ is, the smaller the estimation errors are, and in turn, the higher likelihood that the keys become consistent due to $1-\left(1-\Pr\left\{\xi^{v_1},\xi^{v_2},...,\xi^{v_n}\in[\xi_l,\xi_{l+1}]\right\}_{n\geq 3}\right)^{\Delta}$ (where $0\leq\Pr\left\{\xi^{v_1},\xi^{v_2},...,\xi^{v_n}\in[\xi_l,\xi_{l+1}]\right\}_{n\geq 3}\leq 1$). Therefore, increasing Δ can raise the key agreement probability. Particularly, we consider $\Delta=1$ in this article to explore the key agreement performance of the proposed algorithm in the worst case.

In addition, we also note that the proposed PSKA algorithm is compatible with secret key reconciliation schemes, such as Cascade [45], low density parity check [46], and Turbo code [47]. Given a high key agreement probability achieved by the PSKA algorithm, overhead of the reconciliation is significantly reduced.

D. The eavesdropper's vehicle

As the vehicles of the platoon drive in a fully automatic fashion at a highway speed, one lane is likely to be reserved on highway for vehicular platoons, for driving safety. Any other vehicle occupying the reserved lane can be identified as the eavesdropper by observation. Moreover, the eavesdropper's vehicle, wavelengths away from the platoon, can experience an independent radio channel [48], [49]. Despite that, the eavesdropper's vehicle can also quantize the channels from the platooning vehicles in the attempt to recover the secret key.

Let v_x denote the eavesdropper's vehicle that drives at the same velocity as the platoon and 2 meters away in parallel to the platoon. v_x also applies the PSKA algorithm to generate its secret key based on either $\sigma_{1,x}$ or $\sigma_{2,x}$, when it overhears TB_1 and TB_2. The channel estimation error at v_x follows $\mathcal{N}(0,\sigma_{1,x}^2+\sigma_{2,x}^2)$. Consequently, the probability that the eavesdropper generates the same secret key as the platooning vehicles is given by

$$\begin{aligned}P_{\text{adv}}&=\Pr\left\{\xi^{v_x}\in[\xi_l^*,\xi_{l+1}^*]\right\}\\&=\int_{\xi_l^*}^{\xi_{l+1}^*}\frac{e^{-\frac{x_0^2}{2(\sigma_{1,x}^2+\sigma_{2,x}^2)}}}{\sqrt{2\pi(\sigma_{1,x}^2+\sigma_{2,x}^2)}}dx_0\\&=\frac{1}{2}\big(\text{erf}(\frac{\xi_{l+1}^*}{\sqrt{2(\sigma_{1,x}^2+\sigma_{2,x}^2)}})-\text{erf}(\frac{\xi_l^*}{\sqrt{2(\sigma_{1,x}^2+\sigma_{2,x}^2)}})\big),\end{aligned}\tag{17}$$

where x_0 defines the random variable of the channel between v_1 and v_x. $l\in[1,L_{\text{adv}}]$, and L_{adv} is fixed at 20 intervals. Note that ξ^{v_x} is independent of ξ^{v_i} in **P2** due to independent channel fading at different locations. Therefore, P_{adv} of the eavesdropper can be different in terms of relative locations to the platoon team, as will be numerically demonstrated in Section V-D.

V. Numerical Results and Discussion

In this section, we first demonstrate the value of n given the key agreement probability achieved by the proposed PSKA algorithm. To obtain the performance under different quantization levels and fading channel conditions, the PSKA algorithm is simulated with regards to three quantization intervals, i.e., $L=10$, 15, and 70, and two SNRs of the inter-vehicle channel, i.e., 5 dB and -10 dB.

Second, to explore the key agreement probability under various channel conditions, we show the performance of the PSKA algorithm, given three predetermined CQI quantization intervals and SNRs of the inter-vehicle channel. Here, the channel gain increases from 0 dB to 32 dB, or the number of CQI quantization intervals increases from 25 to 75. For comparison purpose, we also simulate the probability that the eavesdropper generates the same secret key as the platooning vehicles, when it overhears TB_1 and TB_2. Particularly, the eavesdropper's vehicle has the same velocity as the platoon, and travels in parallel to the platoon but 2 meters away from the center of the platoon.

Third, to further reveal the impact of the eavesdropper's relative locations to the platoon, we analyze the probability that the eavesdropper, 2 m$\sim$7 m far from the platoon, generates the same secret key as the platooning vehicles.

Last, it is revealed that a driver has to stay at least two seconds behind the vehicle that is directly in front of his or her vehicle [50]. Thus, the safe driving velocity is derived by the safe driving distance between two adjacent/consecutive vehicles in the platoon over two seconds. Note that the variation of the safe driving velocity can lead to the varying the SNR of the channel between the vehicles. This, in turn, affects the key agreement probability achieved by the PSKA algorithm. Based on this, we study a tradeoff between the safe driving velocity, CQI quantizations, and the key agreement probability, where the driving velocity increases from 0 km/h to 100 km/h, and L increases from 10 to 15 intervals.

Without loss of generality, the block fading is assumed on the inter-vehicle channels. In other words, the channel gain of a wireless link keeps constant during the key agreement and the transmission within a TDMA frame, but varies between frames. This assumption is reasonable, because the duration of a frame is typically up to 10 ms during which the distance that a vehicle has traveled is negligible.

A. Team size

We demonstrate the team size of the platoon, i.e., n, given a specific key agreement probability. L is set to 10 or 15. The average SNR between the two vehicles denoted by $\overline{H_{i,j}}$ ($i\neq j,\ \forall i,j\in[1,n]$), is set to 5 dB or -10 dB. Figure 5 shows the supported team size of a platoon given the key agreement probability. Specifically, when $\overline{H_{i,j}}=5$ dB, the team size of the platoon can be extended to 11 vehicles while the key agreement probability achieved by the PSKA algorithm is around 78%. Moreover, the team size of the platoon has to be small under poor channel quality so as to maintain the achieved key agreement probability. For example, the team size has to be reduced to 6 vehicles so that the key agreement probability is achieved beyond 76% when $L=10$ and $\overline{H_{i,j}}=-10$ dB.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2019.2926313, IEEE Transactions on Vehicular Technology

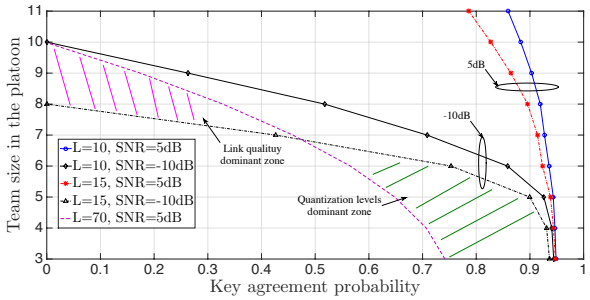

Fig. 5: The team size of a platoon given a required key agreement probability.

In Figure 5, it is observed that increasing the quantization intervals, i.e., L, degrades the key agreement probability. In particular, given a team of three vehicles, the key agreement probability drops from 95% to 74% while L grows from 10 to 70 intervals. Moreover, we see that the PSKA algorithm with $(L = 15,\ \overline{H_{i,j}} = 5)$ achieves a higher key agreement probability than the one with $(L = 70,\ \overline{H_{i,j}} = 5)$ when n is smaller than 7 vehicles. It confirms the fact that L has the dominating effect on the key agreement probability in a small platoon team. Conversely, when $n \geq 7$, the PSKA algorithm with $(L = 70,\ \overline{H_{i,j}} = 5)$ performs better than the one with $(L = 15,\ \overline{H_{i,j}} = -10)$, which indicates that the link quality between the vehicles becomes the dominating factor.

In respect of Figure 5, we also see that the less number of vehicles the team of the platoon has, the higher key agreement probability the PSKA algorithm achieves. However, it has to be noted that a small team size can result in a large control overhead of platoon management, which degrades the delivery ratio of data dissemination [51]. Furthermore, Table II presents the runtime of PSKA algorithm, which is equivalent to the secret key generation latency, in 7 platoons with different team sizes. The platoon size is fixed at 21 vehicles. The platoon is partitioned to a number of teams, where each team of the platoon has n vehicles $(n \in [2, 8])$, and $(L = 10,\ \overline{H_{i,j}} = -10)$. The runtime is calculated by summing up the execution time of PSKA algorithm in each team when the packet is disseminated from the lead vehicle to the tail vehicle of the platoon.

The key generation delay decreases from 570.51 ms to 57.26 ms with the growth of the team size. This is because the lead vehicle of each team has to generate a new secret key to encrypt the packet for its following vehicles. Since the platoon with the small team size contains more teams than the one with the large team size, more key generations are carried out for data encryption/decryption. Therefore, the platoon with a small team size costs a long data dissemination latency.

B. Channel condition

In this case, we consider different channel dynamics between the vehicles, i.e., $\sigma_{1,i}$ and $\sigma_{2,i}$, where n is 3 or 10 vehicles, and L is set to 10, 15 or 20. Figure 6 shows

TABLE II: Total key generation delay.

n in each team	Delay (ms)
2	570.51
3	285.53
4	171.31
5	142.78
6	114.64
7	85.75
8	57.26

the key agreement probability of the PSKA algorithm and P_{adv} in terms of n and L, where $\overline{H_{i,j}}$ increases from 0 dB to 32 dB. In general, the key agreement probability grows with $\overline{H_{i,j}}$ given two team sizes, $n = 3$ or $n = 10$. Particularly, the PSKA algorithm with $(n = 3,\ L = 20)$ performs 55% higher than the one with $(n = 10,\ L = 20)$ when $\overline{H_{i,j}} = 0$ dB. Furthermore, both platoons achieve 100% key agreement when $\overline{H_{i,j}}$ is larger than 24 dB. This is because the large channel gain leads to small channel randomness. Thus, $\Pr\left\{\xi^{v_1}, \xi^{v_2}, ..., \xi^{v_n} \in [\xi_l, \xi_{l+1}]\right\}_{n\geq 3}$ in Eq. (13) increases.

"SIM: n = 10, L = 20" presents the simulated key agreement probability under time-varying random channels using the achieved optimal CQI quantization intervals. Figure 6 also confirms that the simulation results are close to the numerical results achieved by PSKA algorithm. The differences are less than 10%, and diminish as the SNR of the inter-vehicle channel $\overline{H_{i,j}}$ increases.

Additionally, increasing L from 10 to 20 intervals downgrades the key agreement probability of the two platoon teams by 5% and 40%, respectively, which is further evaluated in the next case.

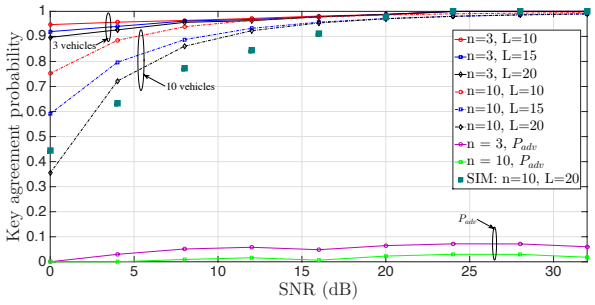

Fig. 6: Key agreement probability achieved by the PSKA algorithm with an increasing SNR.

As observed, P_{adv} of the eavesdropper also increases when $\overline{H_{i,j}}$ is raised. Fortunately, thanks to cooperative key generation of the PSKA algorithm, P_{adv} does not exceed 5% even with a high SNR of 32 dB. Therefore, the probability that the encrypted platoon's data being cracked by the eavesdropper is less than 5%.

C. CQI quantization intervals

In this case, we assess the performance of the PSKA algorithm when it operates on two platoon teams with either $n = 3$ or $n = 10$, as L increases from 25 intervals

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2019.2926313, IEEE Transactions on Vehicular Technology

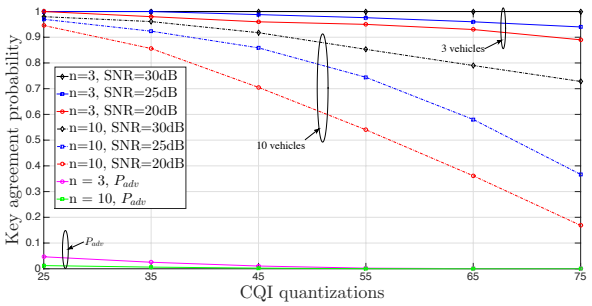

Fig. 7: Key agreement probability achieved by the PSKA algorithm with regards to the total quantization intervals, i.e., L.

to 75 intervals. Figure 7 depicts that the key agreement probability generally decreases with the growth of L. Specifically, the key agreement probability of the 3-vehicle team is 29% higher than the 10-vehicle team when $L = 75$ and $\overline{H_{i,j}} = 30$ dB. This is because the increasing number of vehicles brings down the key agreement probability, as also observed in Figure 5. Moreover, given $n = 3$ and $\overline{H_{i,j}} = 20$ dB, the key agreement probability drops from 100% to 89.5%. In contrast, the probability drops from 95% to 19% when $n = 10$. It indicates that L has to be smaller than 35 intervals for a team with a size of up to 10 vehicles to maintain the key agreement probability above 85%.

Additionally, we also note that reducing L further results in the rise of P_{adv}, where the eavesdropper may generate the same key to decode the data. Therefore, it is critical to comprehensively configure L according to the required key agreement probability, team size, and link quality.

D. P_{adv} and eavesdropper's positions

Next, we demonstrate the P_{adv} value of the eavesdropper in terms of its relative locations to the platoon team. In particular, n is set to 7 vehicles and L is fixed at 15 intervals. We define d_{EP} as the distance between the eavesdropper and the platoon, as shown in Figure 8. In particular, we consider three specific locations of the eavesdropper given each d_{EP}. Specifically, Pos-1 is the location of v_x next to v_2, Pos-2 is the one next to v_4, and Pos-3 is the one next to v_7. The received signal power at v_x is $P^{rx}_{v_x} = P^{tx}_i + \vartheta - 10\eta_{PL}\log_{10}(\sqrt{d^2_{EP} + d^2_{i,j}}) + \phi_{i,v_x}$ based on (1), where $j = \{2, 4, 7\}$ according to Pos-1, Pos-2, or Pos-3. Thus, the channel gain is $H_{i,v_x} = (P^{tx}_i - P^{rx}_j) = 10\eta_{PL}\log_{10}(\sqrt{d^2_{EP} + d^2_{i,j}}) - \vartheta - \phi_{i,v_x}$. Figure 8 shows that P_{adv} of the eavesdropper in terms of its relative distance position to the platoon, where d_{EP} enlarges from 2 m to 7 m. We assume that the eavesdropper can be identified by observation when d_{EP} is less than 2 m.

As observed, the highest P_{adv} is around 0.49%, where d_{EP} is 2 m at Pos-1. Moreover, P_{adv} significantly drops with the increase of d_{EP}. The P_{adv} falls to 0 when the eavesdropper is 6 m away from the platoon at Pos-3. The reason can be explained by Figures 6 and 7, where the eavesdropper can only derive P_{adv} based on independent distribution of $\sigma_{1,x}$ and $\sigma_{2,x}$.

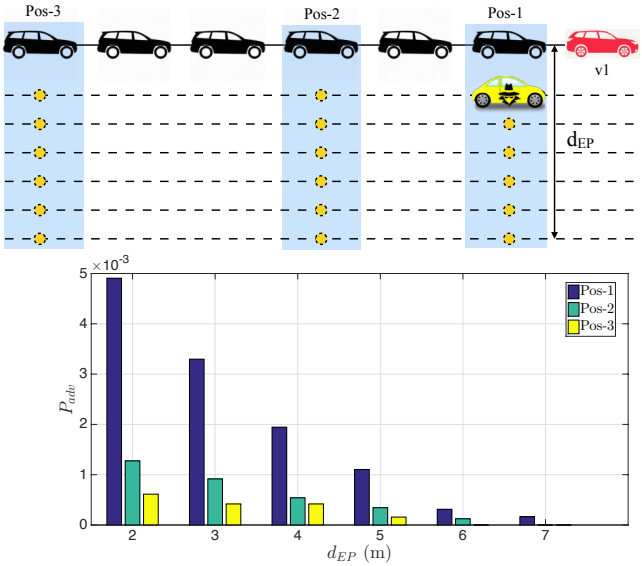

Fig. 8: P_{adv} of the eavesdropper in terms of its relative distance position to the platoon.

E. Safe driving velocity

Figure 9 shows the key agreement probability achieved by applying the proposed PSKA algorithm, with respect to the CQI quantizations and safe driving velocity. In particular, the safe driving velocity is derived based on the safe driving distance between two neighbor vehicles in the platoon, and *Two-second rule* [50].

In Figure 9, it is observed that the key agreement probability drops from 100% to 40% with the growth of a safe driving velocity given 10 quantization intervals. The reason is that increasing the velocity extends inter-vehicle safe driving distance (due to the Two-second rule), which attenuates SNR of the inter-vehicle channel. As a result, the key agreement probability drops. Moreover, the key agreement probability decreases from 40% to 18% with the growth of CQI quantization intervals, when the platoon maintains the velocity of 100 km/h.

Essentially, Figure 9 implies a tradeoff between the velocity of the platoon and data dissemination security. For example, the safe driving velocity has to be maintained below 40 km/h to achieve the key agreement probability above 90%, in other words, reducing the safe driving velocity of the platoon downgrades the driving velocity, however, the low driving velocity achieves a high key agreement probability for the data encryption/decryption, which improves the data dissemination security. In addition, when the platoon drives at a high velocity, e.g., 80 km/h, the key agreement probability can be enhanced by reducing the CQI quantization intervals to less than 10. However, the drop in CQI quantizations results in a fall of the communication security (as discussed in Section V-C). Therefore, the safe driving velocity and the CQI quantizations need to be

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2019.2926313, IEEE Transactions on Vehicular Technology

balanced, so as to achieve the agreement of the generated secret key.

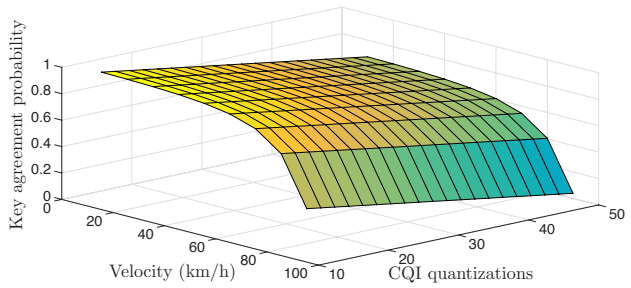

Fig. 9: Safe driving velocity given the specific key agreement probability and CQI quantizations.

VI. Conclusions and discussion

In this paper, we study the data dissemination security in vehicular platoons, where the vehicles cooperatively generate an unanimous secret key based on the quantized fading channel randomness. The 2-stage communication protocol is presented for secret key agreement and data transmission, where the vehicles share the link information for key agreement in SKAP, and transmit the encrypted data in EDTP. In terms of the secret key generation, the problem of maximizing the key agreement probability is formulated to optimize the CQI quantization intervals in the three-vehicle platoon, which is further extended to the n-vehicle platoon. In addition, the PSKA algorithm is proposed to recursively optimize the CQI quantization intervals, maximizing the secret key agreement probability, and cooperatively generate the secret key for data encryption/decryption. Based on the numerical analysis, we have demonstrated that the key agreement probability is effected by the quantization intervals and channel quality. We have also shown that the probability that eavesdroppers generate the same secret key, which is far lower than the one using the PSKA algorithm.

The proposed PSKA algorithm focuses on a secure data dissemination for the platoon on a straight highway. Indeed, the work presented in this article could be extended in many interesting directions. For example, in our future work, the PSKA algorithm will be developed for the key agreement when the platooning vehicles make turns or perform maneuvers, such as split, merge, or leave. In this case, the channel gain between v_1 and v_2 can be estimated at v_i by formulating a statistical process, e.g., measuring the variance of $H_{1,i}$ and $H_{2,i}$ for a period of time, which is unknown to the eavesdropper, since the platoon is nonlinear. The link-based secret key agreement with a time-varying platooning control is a challenging topic for further investigation.

Acknowledgements

This work was supported by National Funds through FCT/MEC (Portuguese Foundation for Science and Technology) and co-financed by ERDF (European Regional Development Fund) under the PT2020 Partnership, within the CISTER Research Unit (CEC/04234); also by FCT/MEC and the EU ECSEL JU under the H2020 Framework Programme, within project ECSEL/0002/2015, JU grant nr. 692529-2 (SAFECOP).

The authors would like to thank the editors and the anonymous reviewers for their constructive comments on the article.

Appendix

The probability that the three vehicles use the same quantization interval is given by (21).

References

[1] E. Chan, "Overview of the sartre platooning project: technology leadership brief," SAE Technical Paper, Tech. Rep., 2012.

[2] P. Pop, D. Scholle, H. Hansson, G. Widforss, and M. Rosqvist, "The SafeCOP ECSEL project: Safe cooperating cyber-physical systems using wireless communication," in *Euromicro Conference on Digital System Design (DSD)*. IEEE, 2016, pp. 532–538.

[3] 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.

[4] J. Cheng, J. Cheng, M. Zhou, F. Liu, S. Gao, and C. Liu, "Routing in internet of vehicles: A review," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 5, pp. 2339–2352, 2015.

[5] L. Li, D. Wen, and D. Yao, "A survey of traffic control with vehicular communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 15, no. 1, pp. 425–432, 2014.

[6] C. TAN and K. THAM, "Autonomous vehicles, next stop: Singapore," Nov 2014. [Online]. Available: https://www.lta.gov.sg/ltaacademy/doc/J14Nov_p05Tan_AVnextStep Singapore.pdf

[7] R. A. Ferlis, "The dream of an automated highway," Aug 2007. [Online]. Available: https://www.fhwa.dot.gov/publications/publicroads/07july/07.cfm

[8] K. Li, W. Ni, E. Tovar, and M. Guizani, "LCD: Low latency command dissemination for a platoon of vehicles," in *IEEE International Conference on Communications (ICC)*, arXiv preprint arXiv:1801.06153, 2018.

[9] C.-H. Wang, C.-T. Chou, P. Lin, and M. Guizani, "Performance evaluation of ieee 802.15. 4 nonbeacon-enabled mode for internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 3150–3159, 2015.

[10] J. Xu, K. Li, L. Duan, and R. Zhang, "Proactive eavesdropping via jamming over HARQ-based communications," in *IEEE Global Communications Conference (Globecom)*, arXiv preprint arXiv:1708.09801, 2017.

[11] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[12] K. Zeng, "Physical layer key generation in wireless networks: challenges and opportunities," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 33–39, 2015.

[13] C. Cooper, D. Franklin, M. Ros, F. Safaei, and M. Abolhasan, "A comparative survey of VANET clustering techniques," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 657–681, 2017.

[14] M. Segata, F. Dressler, and R. L. Cigno, "Let's talk in groups: A distributed bursting scheme for cluster-based vehicular applications," *Vehicular Communications*, vol. 8, pp. 2–12, 2017.

[15] C. D. T. Thai, J. Lee, and T. Q. Quek, "Physical-layer secret key generation with colluding untrusted relays," *IEEE Transactions on Wireless Communications*, vol. 15, no. 2, pp. 1517–1530, 2016.

[16] N. Wang, N. Zhang, and T. A. Gulliver, "Cooperative key agreement for wireless networking: Key rates and practical protocol design," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 2, pp. 272–284, 2014.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2019.2926313, IEEE Transactions on Vehicular Technology

$$\Pr\left\{\xi^{v_1},\xi^{v_2},\xi^{v_3}\in[\xi_l,\xi_{l+1}]\right\} = \Pr(\xi_l \le x_3-x_2 | x_1 \ge x_3-x_2)\Pr(\xi_{l+1}\ge x_1 | x_1\ge x_3-x_2)\Pr(x_1\ge x_3-x_2)+ \Pr(\xi_l \le x_1 | x_1 < x_3-x_2)\Pr(\xi_{l+1}\ge x_3-x_2 | x_1 < x_3-x_2)\Pr(x_1 < x_3-x_2) \quad (18)$$

$$= \Pr(\xi_l \le x_3-x_2 \cap x_1\ge x_3-x_2)\Pr(\xi_{l+1}\ge x_1 | x_1\ge x_3-x_2)+ \Pr(\xi_l \le x_1 \cap x_1 < x_3-x_2)\Pr(\xi_{l+1}\ge x_3-x_2 | x_1 < x_3-x_2) \quad (19)$$

$$= \frac{\Pr(\xi_l \le x_3-x_2 \cap x_1\ge x_3-x_2)\Pr(\xi_{l+1}\ge x_1 \cap x_1\ge x_3-x_2)}{\Pr(x_1\ge x_3-x_2)}+ \frac{\Pr(\xi_l \le x_1 \cap x_1 < x_3-x_2)\Pr(\xi_{l+1}\ge x_3-x_2 \cap x_1 < x_3-x_2)}{\Pr(x_1 < x_3-x_2)} \quad (20)$$

$$= \frac{\Pr(\xi_l \le x_3-x_2 \le x_1 \le \xi_{l+1})}{\Pr(x_1\ge x_3-x_2)} + \frac{\Pr(\xi_l \le x_1 < x_3-x_2 \le \xi_{l+1})}{\Pr(x_1 < x_3-x_2)}. \quad (21)$$

[17] D. Chen, Z. Qin, X. Mao, P. Yang, Z. Qin, and R. Wang, "Smokegrenade: An efficient key generation protocol with artificial interference," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 11, pp. 1731–1745, 2013.

[18] Q. Wang, K. Xu, and K. Ren, "Cooperative secret key generation from phase estimation in narrowband fading channels," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 9, pp. 1666–1674, 2012.

[19] 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.

[20] P. Xu, K. Cumanan, Z. Ding, X. Dai, and K. K. Leung, "Group secret key generation in wireless networks: algorithms and rate optimization," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1831–1846, 2016.

[21] R. Jin, X. Du, Z. Deng, K. Zeng, and J. Xu, "Practical secret key agreement for full-duplex near field communications," *IEEE Transactions on Mobile Computing*, vol. 15, no. 4, pp. 938–951, 2016.

[22] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *INFOCOM*. IEEE, 2013, pp. 3048–3056.

[23] P. Huang and X. Wang, "Fast secret key generation in static wireless networks: A virtual channel approach," in *INFOCOM*. IEEE, 2013, pp. 2292–2300.

[24] S. Im, H. Jeon, J. Choi, and J. Ha, "Secret key agreement with large antenna arrays under the pilot contamination attack," *IEEE Transactions on Wireless Communications*, vol. 14, no. 12, pp. 6579–6594, 2015.

[25] K. Li, H. Kurunathan, R. Severino, and E. Tovar, "Cooperative key generation for data dissemination in cyber-physical systems," in *Proceedings of the 9th ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*. IEEE Press, 2018, pp. 331–332.

[26] K. Li, Y. Emami, and E. Tovar, "Privacy-preserving control message dissemination for PVCPS," in *Proceedings of the 18th International Conference on Information Processing in Sensor Networks (IPSN)*. ACM, 2019, pp. 301–302.

[27] X. Zhu, F. Xu, E. Novak, C. C. Tan, Q. Li, and G. Chen, "Using wireless link dynamics to extract a secret key in vehicular scenarios," *IEEE Transactions on Mobile Computing*, vol. 16, no. 7, pp. 2065–2078, 2017.

[28] A. B. Lopez, "Physical layer key generation for wireless communication security in automotive cyber-physical systems," Ph.D. dissertation, UC Irvine, 2017.

[29] S. Guo, D. Zeng, and Y. Xiang, "Chameleon hashing for secure and privacy-preserving vehicular communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 11, pp. 2794–2803, 2014.

[30] R. Jin, X. Du, K. Zeng, L. Huang, L. Xiao, and J. Xu, "Delay analysis of physical-layer key generation in dynamic roadside-to-vehicle networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2526–2535, 2017.

[31] S.-F. Tzeng, S.-J. Horng, T. Li, X. Wang, P.-H. Huang, and M. K. Khan, "Enhancing security and privacy for identity-based batch verification scheme in VANETs," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 4, pp. 3235–3248, 2017.

[32] Y. Liu, L. Wang, and H.-H. Chen, "Message authentication using proxy vehicles in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 8, pp. 3697–3710, 2015.

[33] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *INFOCOM*. IEEE, 2008, pp. 1229–1237.

[34] K. Li, R. C. Voicu, S. S. Kanhere, W. Ni, and E. Tovar, "Energy efficient legitimate wireless surveillance of UAV communications," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2283–2293, 2019.

[35] X. Wang, D. Li, C. Guo, X. Zhang, S. S. Kanhere, K. Li, and E. Tovar, "Eavesdropping and jamming selection policy for suspicious UAVs based on low power consumption over fading channels," *Sensors*, vol. 19, no. 5, p. 1126, 2019.

[36] X. Wang, K. Li, S. S. Kanhere, D. Li, X. Zhang, and E. Tovar, "PELE: Power efficient legitimate eavesdropping via jamming in UAV communications," in *International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, 2017, pp. 402–408.

[37] R. Liu, C. Yuen, T.-N. Do, D. Jiao, X. Liu, and U.-X. Tan, "Cooperative relative positioning of mobile users by fusing IMU inertial and UWB ranging information," in *2017 IEEE International Conference on Robotics and Automation (ICRA)*. IEEE, 2017, pp. 5623–5629.

[38] A. Yassin, Y. Nasser, M. Awad, A. Al-Dubai, R. Liu, C. Yuen, R. Raulefs, and E. Aboutanios, "Recent advances in indoor localization: A survey on theoretical approaches and applications," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1327–1346, 2016.

[39] K. Li, C. Yuen, B. Kusy, R. Jurdak, A. Ignatovic, S. Kanhere, and S. K. Jha, "Fair scheduling for data collection in mobile sensor networks with energy harvesting," *IEEE Transactions on Mobile Computing*, 2018.

[40] K. Li, W. Ni, X. Wang, R. P. Liu, S. S. Kanhere, and S. Jha, "Energy-efficient cooperative relaying for unmanned aerial vehicles," *IEEE Transactions on Mobile Computing*, vol. 15, no. 6, pp. 1377–1386, 2016.

[41] Y. L. Morgan, "Notes on DSRC & WAVE standards suite: Its architecture, design, and characteristics," *IEEE Communications Surveys & Tutorials*, vol. 12, no. 4, pp. 504–518, 2010.

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

[43] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Communications*, vol. 18, no. 4, 2011.

[44] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *International journal of information security*, vol. 1, no. 1, pp. 36–63, 2001.

[45] Y. Wei, K. Zeng, and P. Mohapatra, "Adaptive wireless channel probing for shared key generation based on PID controller," *IEEE Transactions on Mobile Computing*, vol. 12, no. 9, pp. 1842–1852, 2013.

[46] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," *IEEE Transactions on information forensics and security*, vol. 7, no. 5, pp. 1484–1497, 2012.

[47] 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, 2018.
[48] 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, p. 17, 2010.
[49] G. D. Durgin, *Space-time wireless channels*. Prentice Hall Professional, 2003.
[50] (2018, 01) Two-second rule. [Online]. Available: https://en.wikipedia.org/wiki/Two-second_rule
[51] S. Ucar, S. C. Ergen, and O. Ozkasap, "Multihop-cluster-based IEEE 802.11 p and LTE hybrid architecture for VANET safety message dissemination," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 4, pp. 2621–2636, 2016.

Kai Li (S'09–M'14) received the B.E. degree from Shandong University, China, in 2009, the M.S. degree from The Hong Kong University of Science and Technology, Hong Kong, in 2010, and the Ph.D. degree in Computer Science from The University of New South Wales, Sydney, Australia, in 2014. Currently he is a senior research scientist and project leader at Real-Time and Embedded Computing Systems Research Centre (CISTER), Portugal. Prior to this, Dr. Li was a postdoctoral research fellow at The SUTD-MIT International Design Centre, The Singapore University of Technology and Design, Singapore (2014-2016). He was a visiting research assistant at ICT Centre, CSIRO, Australia (2012-2013). From 2010 to 2011, he was a research assistant at Mobile Technologies Centre with The Chinese University of Hong Kong. His research interests include vehicular communications and security, resource allocation optimization, Cyber-Physical Systems, Internet of Things (IoT), human sensing systems, sensor networks and UAV networks.

Lingyun Lu received the M.E. degrees from Shenyang Institute of technology, Shenyang, China, and Ph.D. degrees from Beijing Jiaotong University, Beijing, China. She is an Associate Professor with Beijing Jiaotong University, Beijing, China. Her research interests include cross-layer network performance, heterogeneous networks, and multiuser signal processing. She has been involved with and led projects for the National Natural Science Foundation of China and other commercial projects ranging from OpenFlow and congestion control.

Wei Ni (M'09–SM'15) received the B.E. and Ph.D. degrees in Electronic Engineering from Fudan University, Shanghai, China, in 2000 and 2005, respectively. Currently he is a Team Leader at CSIRO, Sydney, Australia, and an adjunct professor at the University of Technology Sydney (UTS). He also holds adjunct positions at the University of New South Wales (UNSW) and Macquarie University (MQ). Prior to this, he was a postdoctoral research fellow at Shanghai Jiaotong University from 2005-2008; Deputy Project Manager at the Bell Labs R&I Center, Alcatel/Alcatel-Lucent from 2005-2008; and Senior Researcher at Devices R&D, Nokia from 2008-2009. His research interests include stochastic optimization, game theory, graph theory, as well as their applications to network and security.

Eduardo Tovar was born in 1967 and has received the Licentiate, MSc and PhD degrees in electrical and computer engineering from the University of Porto, Porto, Portugal, in 1990, 1995 and 1999, respectively. Currently he is Professor in the Computer Engineering Department at the School of Engineering (ISEP) of Polytechnic Institute of Porto (IPP), where he is also engaged in research on real-time distributed systems, wireless sensor networks, multiprocessor systems, cyber-physical systems and industrial communication systems. He heads the CISTER Research Unit, an internationally renowned research centre focusing on RTD in real-time and embedded computing systems. He is deeply engaged in research on real-time distributed systems, multiprocessor systems, cyber-physical systems and industrial communication systems. He is currently the Vice-chair of ACM SIGBED (ACM Special Interest Group on Embedded Computing Systems) and was for 5 years, until December 2015, member of the Executive Committee of the IEEE Technical Committee on Real-Time Systems (TC-RTS). Since 1991 he authored or co-authored more than 150 scientific and technical papers in the area of real-time and embedded computing systems, with emphasis on multiprocessor systems and distributed embedded systems. Eduardo Tovar has been consistently participating in top-rated scientific events as member of the Program Committee, as Program Chair or as General Chair. Notably he has been program chair/co-chair for ECRTS 2005, IEEE RTCSA 2010, IEEE RTAS 2013 or IEEE RTCSA 2016, all in the area of real-time computing systems. He has also been program chair/co-chair of other key scientific events in the area of architectures for computing systems and cyber-physical systems as is the case of ARCS 2014 or the ACM/IEEE ICCPS 2016 or in the area of industrial communications (IEEE WFCS 2014).

Mohsen Guizani (S'85–M'89–SM'99–F'09) received the B.S. (with distinction) and M.S. degrees in electrical engineering, 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 and the ECE Department Chair at the University of Idaho, USA. Previously, he served as the Associate Vice President of Graduate Studies, Qatar University, Chair of the Computer Science Department, Western Michigan University, and Chair of the Computer Science Department, University of West Florida. He also served in academic positions at the University of Missouri-Kansas City, University of Colorado-Boulder, Syracuse University, and Kuwait University. His research interests include wireless communications and mobile computing, computer networks, mobile cloud computing, security, and smart grid. He currently serves on the editorial boards of several international technical journals and the Founder and the Editor-in-Chief of Wireless Communications and Mobile Computing journal (Wiley). He is the author of 9 books and more than 500 publications in refereed journals and conferences. He guest edited a number of special issues in IEEE journals and magazines. He also served as a member, Chair, and General Chair of a number of international conferences. He received the teaching award multiple times from different institutions as well as the best Research Award from three institutions. He received the 2017 IEEE ComSoc Recognition Award for his contribution to Wireless Communications. He was the Chair of the IEEE Communications Society Wireless Technical Committee and the Chair of the TAOS Technical Committee. He served as the IEEE Computer Society Distinguished Speaker from 2003 to 2005. He is a Fellow of IEEE and a Senior Member of ACM.