CISTER
Research Centre in
Real-Time & Embedded
Computing Systems

Conference Paper

Cooperative Secret Key Generation for Platoon-based Vehicular Communications

Kai Li
Lingyun Luy
Wei Niz
Eduardo Tovar
Mohsen Guizani

CISTER-TR-190206

Cooperative Secret Key Generation for Platoon-based Vehicular Communications

Kai Li, Lingyun Luy, Wei Niz, 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:

https://www.cister-labs.pt

Abstract

In a vehicular platoon, the lead vehicle that isresponsible for managing the platoon 19s moving directionsand velocity periodically disseminates messages to the followingautomated vehicles in a multi-hop vehicular network.However, due to the broadcast nature of wireless channels,vehicle-to-vehicle (V2V) communications are vulnerable toeavesdropping and message modification. Generating secretkeys by extracting the shared randomness in a wireless fadingchannel is a promising way for V2V communication security.We study a security scheme for platoon-based V2V communications,where the platooning vehicles generate a shared secretkey based on the quantized fading channel randomness. Toimprove conformity of the generated key, the probability ofsecret key agreement is formulated, and a novel secret keyagreement algorithm is proposed to recursively optimize thechannel quantization intervals, maximizing the key agreementprobability. Numerical evaluations demonstrate that the keyagreement probability achieved by our security protocolgiven different platoon size, channel quality, and number ofquantization intervals. Furthermore, by applying our securityprotocol, it is shown that the probability that the encrypteddata being cracked by an eavesdropper is less than 5%.

Cooperative Secret Key Generation for Platoon-based Vehicular Communications

Kai Li*, Lingyun Lu†, Wei Ni‡, Eduardo Tovar*, and Mohsen Guizani§
*Real-Time and Embedded Computing Systems Research Centre (CISTER), Porto, Portugal.
Email: {kai_li, emt}@isep.ipp.pt.
†College of Computer Science, Beijing Jiaotong University, Beijing, P.R. China.
Email: lylu@bjtu.edu.cn.
‡Commonwealth Scientific and Industrial Research Organization (CSIRO), Sydney, Australia.
Email: wei.ni@csiro.au.
§Department of Electrical and Computer Engineering, University of Idaho, Moscow, USA.
Email: mguizani@ieee.org.

***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, vehicle-to-vehicle (V2V) communications are vulnerable to eavesdropping and message modification. Generating secret keys by extracting the shared randomness in a wireless fading channel is a promising way for V2V communication security. We study a security scheme for platoon-based V2V communications, where the platooning vehicles 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, it is shown that the probability that the encrypted data being cracked by an eavesdropper is less than 5%.**

***Index Terms*—Autonomous vehicles, Data dissemination, Wireless communication, Physical layer security**

I. Introduction

Recent advances in vehicle-to-vehicle (V2V) 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]. Forming a vehicular platoon 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 others [4].

The platoon's driving status indicates emergent road conditions, such as traffic jams, crossroads, obstacles or car accidents [5], which affect mobility patterns of the platoon, e.g., decelerating, changing heading directions, and braking. However, due to the broadcast nature of radio channels, V2V communications in order to update the driving status in the platoon are vulnerable to eavesdropping and replay attacks [6], [7]. 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 [8], 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 of the secret key agreement arise in platoon-based V2V communications. 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 one 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 this paper, we propose a PlatoonKey scheme for secure platoon-based V2V communications to address both of the above challenges. Specifically, PlatoonKey quantizes the channel gains between the vehicles, and cooperatively generate a unanimous secret key in the platoon, which is used for encrypting/decrypting the V2V communication.

In particular, PlatoonKey utilizes the phase reciprocity of V2V communications: the underlying channel response between two vehicles is unique and location-specific, and the transmitted signals from each other experience almost the same fading in the phase. In PlatoonKey, the channel quality indicator (CQI) quantization intervals are optimized to maximize the key agreement probability by using a new recursive method, which recursively characterizes all the quantization intervals based on one of them. Note that the secret key is generated by each 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 one secret key, leading to a poor key agreement probability. In addition, since the secret key generated by PlatoonKey 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.

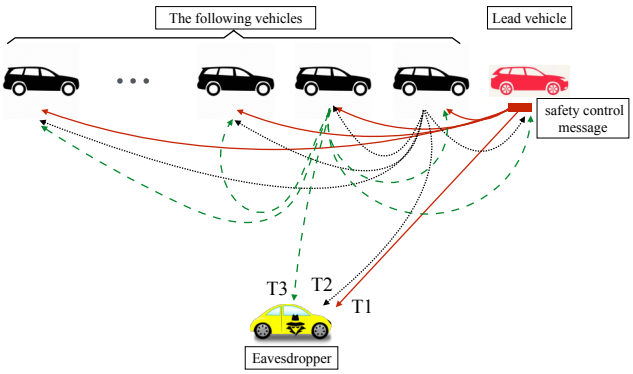

Fig. 1: In a platoon of vehicles, vehicular information is disseminated from the lead vehicle to the tail, by broadcasting over the insecure public channel.

The rest of the paper is organized as follows. Section II presents related work on link-based secret key generation. Section III presents channel model of the platoon-based V2V communication. Section IV investigates PlatoonKey that incorporates the secret key agreement. In Section V, optimization of CQI quantization intervals is studied for secret key agreement. Simulation results are shown in Section VI, followed by conclusions in Section VII.

II. Related Work

In this section, we review the literature on the secret key generation that exploits randomness of wireless fading channels. In [9], 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 algorithms for two scenarios in terms of network size, i.e., the three-node network and the multi-node network [10]. 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 [11], 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 [12], 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 [13], 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 [14]. 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.

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.

III. Channel Model in Vehicular Platoons

In vehicular platoons, Line of Sight (LOS) V2V communication 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 V2V communication channel. Let P_i^{tx} denote the transmit power (in dB) of 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

TABLE I: Channel quality obtained at v_j after the channel probing.

Channel probes	$H_{i,j}$ obtained at v_j						
Probe$_1$	—	$H_{1,2}$	$H_{1,3}$	$H_{1,4}$	...	$H_{1,j}$	...
Probe$_2$	$H_{2,1}$	—	$H_{2,3}$	$H_{2,4}$	...	$H_{2,j}$	...
Probe$_3$	$H_{3,1}$	$H_{3,2}$	—	$H_{3,4}$	...	$H_{3.j}$	...
Probe$_4$	$H_{4,1}$	$H_{4,2}$	$H_{4,3}$	—	...	$H_{4,j}$	...
...	...	...	...	...	...	...	...
Probe$_i$	$H_{i,1}$	$H_{i,2}$	$H_{i,3}$	$H_{i,4}$	...	—	...
...	...	...	...	...	...	...	...

further written as

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

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. $d_{i,j}$ is predetermined before forming the platoon since the non-leading vehicle in the platoon is required to maintain a certain distance with the preceding one.

Table I shows $H_{i,j}$ which is obtained after channel probing. However, v_j is not aware of the channels between the other vehicles, 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 has been known before forming the platoon, the channel gain between any other two vehicles in the platoon can be estimated by v_j based on their distance gap, i.e., $d_{i,j-1} = d_{i,j} - d_{j-1,j}$. 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

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

IV. Platooning secret key agreement

The steps that incorporate the secret key agreement in the proposed PlatoonKey mainly include: channel probing, CQI quantization, and platooning secret key generation.

Step 1: Channel probing. v_1 and v_2 broadcast the probing packet in turn. The following vehicle v_i ($i \in [3, n]$) measures Signal-to-Noise ratio (SNR) of the links with v_1 and v_2 according to the reception of the probing packet. For illustration convenience, in this paper, the first two vehicles, i.e., v_1 and v_2 are considered for the channel probing. v_i ($i \in [3, n]$) estimates the channel gain between v_1 and v_2, i.e., $H_{1,2}$, based on Probe$_1$ and Probe$_2$, using (3).

Step 2: CQI quantization. v_1 and v_2 quantize $H_{1,2}$, while the following vehicle v_i ($i \in [3, n]$) 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 $l \in [1, L]$. We propose to optimize the CQI quantization intervals (denoted by $\xi_l^\star$) to maximize the key agreement probability, as described in Section V.

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., $[\xi_l^\star, \xi_{l+1}^\star]$ ($l \in [1, L]$). 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 the V2V communication at every hop.

Actually, it can be known that the more vehicles perform channel probing, the higher key agreement probability can be achieved. Thus, reducing the number of channel probing vehicles explores the key agreement performance in the worst case, though the proposed PlatoonKey can also be applied to the platoon that more than two channel probing vehicles. Moreover, 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.

V. Optimization Of CQI Quantization Intervals

In this section, we first formulate the CQI quantization intervals optimization problem. Next, we demonstrate PlatoonKey to generate the unanimous secret key with the optimal CQI quantization intervals.

A. Problem formulation

We consider n vehicles in the platoon, where $n \geq 3$. The first two platooning vehicles, i.e., v_1 and v_2, are the channel probing vehicles. Note that our formulation can be extended to any number of channel probing vehicles given the channel gains in Table I. Moreover, the distribution of the channel between vehicles v_1 and v_2 is estimated by the following vehicle v_i ($i \in [3, n]$) when it receives Probe$_1$ and Probe$_2$, which follows $x_i' = (x_i - x_{i-1}) \backsim \mathcal{N}(0, \sigma_{1,i}^2 + \sigma_{2,i}^2)$. 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 the channel distribution observation at the vehicles is

$$\Phi(x_1, \ ... \ x_n') = \frac{e^{-\frac{x_1^2}{2\sigma_{1,2}^2} - \frac{(x_3')^2}{2(\sigma_{1,3}^2+\sigma_{2,3}^2)} - ... - \frac{(x_n')^2}{2(\sigma_{1,n}^2+\sigma_{2,n}^2)}}}{\sqrt{(2\pi)^n \sigma_{1,2}^2(\sigma_{1,3}^2+\sigma_{2,3}^2)...(\sigma_{1,n}^2+\sigma_{2,n}^2)}}. \tag{4}$$

Given $n \geq 3$, the desired probability that the channel quantization at all vehicles fall into the same interval is given by (5).

$$\Pr\Big\{\xi^{v_1},\xi^{v_2},...,\xi^{v_n}\in[\xi_l,\xi_{l+1}]\Big\}=\int\cdots\int_{[\xi_l,\xi_{l+1}]}\Phi(x_1,\ ...\ x_n')dx_1...dx_n'$$
$$=\frac{\pi\Big(\text{erf}(\sqrt{\frac{1}{2\sigma_{1,2}^2}}\xi_{l+1})-\text{erf}(\sqrt{\frac{1}{2\sigma_{1,2}^2}}\xi_l)\Big)}{2\sqrt{(2\pi)^n(\sigma_{1,3}^2+\sigma_{2,3}^2)...(\sigma_{1,n}^2+\sigma_{2,n}^2)}}\prod_{n\geq 3}\sqrt{\frac{\pi(\sigma_{1,n}^2+\sigma_{2,n}^2)}{2}}\Big(\text{erf}(\sqrt{\frac{1}{2(\sigma_{1,n}^2+\sigma_{2,n}^2)}}\xi_{l+1})-\text{erf}(\sqrt{\frac{1}{2(\sigma_{1,n}^2+\sigma_{2,n}^2)}}\xi_l)\Big) \quad (5)$$

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

$$\max_{\{\xi_l\}}\Big\{P_L\Big\} \quad (6)$$

where $P_L=\sum_{l=1}^{L}\Pr\Big\{\xi^{v_1},\xi^{v_2},...,\xi^{v_n}\in[\xi_l,\xi_{l+1}]\Big\}$.

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 $l=L$, only ξ_l, and itself, ξ_{l+1}). Since $\xi_L=+\infty$ and $\text{erf}(+\infty)=1$, the partial derivative can be given by (7), where $l\in[1,L]$. By exploiting the first-order necessary condition of a maximum on (7), $\partial P_L/\partial\xi_l=0$ can be rewritten as (8). The optimal solution can be given by $\xi_l^*=\arg(G(\xi_l^*))$, where $G(\xi_l^*)$ denotes the LHS of (8). 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 (7), 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, $\xi_l^\star$ ($l\in[1,L]$) can be recursively optimized.

B. Secret key generation

Next, we demonstrate PlatoonKey to reconcile the generated secret key with the optimal channel quantization intervals, as shown in Algorithm 1. Specifically, $\xi_l^\star$ ($1\leq l\leq L$) is obtained by conducting **Steps 1 and 2** to derive (8). Note that any two vehicles in the platoon using the same channel quantization intervals generate the same secret key. In the case that the V2V communication channels experience a large variation of random noise and significant estimation errors, $\xi_l^\star$ and $\xi_{l+1}^\star$ in (6) 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**, an encoding scheme $f_{\text{encoding}}^{v_i}(l,l+1)$ 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. 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 V2V communication 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 PlatoonKey, 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 [15]. Note that complexity of Algorithm 1 increases linearly with the number of quantization intervals.

Algorithm 1 PlatoonKey with the Optimal CQI Quantization Intervals

1: **Initialize:** n, L, Probe$_1$, Probe$_2$, $\{\xi^{v_1},\xi^{v_2},...,\xi^{v_n}\}=0$, $\xi_1=0$, $\xi_L=+\infty$.
2: **Optimal channel quantization:**
3: Probe$_1$ and Probe$_2$ 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: $\quad\xi_{l+1}^\star\leftarrow$ (8).
7: $\quad l\leftarrow l+1$.
8: **end while**
9: **Output:** $\{\xi_1^*,...,\xi_L^*\}$.
10: **Generate platooning secret key:**
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.

C. The eavesdropper's vehicle

Note that the eavesdropper's vehicle, wavelengths away from the platoon, can experience an independent radio channel. Despite that, the eavesdropper's vehicle can also quantize the channels from the platooning vehicles in the attempt to recover the secret key for decoding the overheard data packets.

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 PlatoonKey to generate its secret key based on either $\sigma_{1,x}$ or $\sigma_{2,x}$, when it overhears Probe$_1$ and Probe$_2$. The channel estimation error at v_x follows $\mathcal{N}(0,\sigma_{1,x}^2+\sigma_{2,x}^2)$. Consequently, the probability

$$\frac{\partial P_L}{\partial \xi_l} = \frac{\partial \sum_{l=1}^{L} \int \cdots \int_{[\xi_l,\xi_{l+1}]} \frac{e^{-\frac{x_1^2}{2\sigma_{1,2}^2} - \frac{(x_3')^2}{2(\sigma_{1,3}^2+\sigma_{2,3}^2)} - \cdots - \frac{(x_n')^2}{2(\sigma_{1,n}^2+\sigma_{2,n}^2)}}}{\sqrt{(2\pi)^n \sigma_{1,2}^2(\sigma_{1,3}^2+\sigma_{2,3}^2)\ldots(\sigma_{1,n}^2+\sigma_{2,n}^2)}} dx_1 \ldots dx_n'}{\partial \xi_l}$$

$$= \frac{\pi \prod_{n\geq 3} \sqrt{\frac{\pi(\sigma_{1,n}^2+\sigma_{2,n}^2)}{2}}}{2\sqrt{(2\pi)^n(\sigma_{1,3}^2+\sigma_{2,3}^2)\ldots(\sigma_{1,n}^2+\sigma_{2,n}^2)}} \cdot$$

$$\Big(\frac{-2e^{-\frac{1}{2\sigma_{1,2}^2}\xi_l^2}}{\sqrt{\pi}}\Big(\text{erf}(\sqrt{\frac{1}{2\sigma_{1,2}^2}}\xi_{l+1}) - \text{erf}(\sqrt{\frac{1}{2\sigma_{1,2}^2}}\xi_l)\Big) \prod_{n\geq 3}\Big(\text{erf}(\sqrt{\frac{1}{2(\sigma_{1,n}^2+\sigma_{2,n}^2)}}\xi_{l+1}) - \text{erf}(\sqrt{\frac{1}{2(\sigma_{1,n}^2+\sigma_{2,n}^2)}}\xi_l)\Big) +$$

$$\sum_{n\geq 3}\Big(\text{erf}(\sqrt{\frac{1}{2\sigma_{1,2}^2}}\xi_{l+1}) - \text{erf}(\sqrt{\frac{1}{2\sigma_{1,2}^2}}\xi_l)\Big) \prod_{n\geq 3, n'\neq n} \frac{-2e^{-\frac{1}{2(\sigma_{1,n}^2+\sigma_{2,n}^2)}\xi_l^2}}{\sqrt{\pi}}\Big(\text{erf}(\sqrt{\frac{1}{2(\sigma_{1,n'}^2+\sigma_{2,n'}^2)}}\xi_{l+1}) - \text{erf}(\sqrt{\frac{1}{2(\sigma_{1,n'}^2+\sigma_{2,n'}^2)}}\xi_l)\Big)\Big) \tag{7}$$

$$\Big(\frac{-2e^{-\frac{1}{2\sigma_{1,2}^2}\xi_l^2}}{\sqrt{\pi}}\Big(1 - \text{erf}(\sqrt{\frac{1}{2\sigma_{1,2}^2}}\xi_l)\Big) \prod_{n\geq 3}\Big(1 - \text{erf}(\sqrt{\frac{1}{2(\sigma_{1,n}^2+\sigma_{2,n}^2)}}\xi_l)\Big) + \sum_{n\geq 3}\Big(1 - \text{erf}(\sqrt{\frac{1}{2\sigma_{1,2}^2}}\xi_l)\Big) \cdot$$

$$\prod_{n\geq 3, n'\neq n} \frac{-2e^{-\frac{1}{2(\sigma_{1,n}^2+\sigma_{2,n}^2)}\xi_l^2}}{\sqrt{\pi}}\Big(1 - \text{erf}(\sqrt{\frac{1}{2(\sigma_{1,n'}^2+\sigma_{2,n'}^2)}}\xi_l)\Big)\Big) = 0 \tag{8}$$

that the eavesdropper generates the same secret key as the platooning vehicles is given by

$$P_{\text{adv}} = \Pr\Big\{\xi^{v_x} \in [\xi_l^*, \xi_{l+1}^*]\Big\} = \frac{1}{2}\big(\text{erf}(\frac{\xi_{l+1}^*}{\sqrt{2(\sigma_{1,x}^2+\sigma_{2,x}^2)}}) - \text{erf}(\frac{\xi_l^*}{\sqrt{2(\sigma_{1,x}^2+\sigma_{2,x}^2)}})\big), \tag{9}$$

where x_0 defines the random variable of the channel between v_1 and v_x. $l \in [1, L_{\text{adv}}]$. Note that ξ^{v_x} is independent of ξ^{v_i} in (6) 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, as will be numerically demonstrated in Section VI-D.

VI. Performance Evaluation

In this section, we demonstrate the key agreement probability achieved by the proposed PlatoonKey given different platoon size, channel quality, and number of quantization intervals. Without loss of generality, the block fading is assumed on the V2V communication 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. 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. The average SNR of the V2V communication channel is denoted by $\overline{H_{i,j}}$ ($i \neq j$; $\forall i,j \in [1,n]$), Figure 2 shows the key agreement probability of PlatoonKey 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 platoon sizes, $n = 3$ or $n = 10$. Particularly, PlatoonKey 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, $\Pr\Big\{\xi^{v_1}, \xi^{v_2}, ..., \xi^{v_n} \in [\xi_l, \xi_{l+1}]\Big\}$ in Eq. (5) increases. Additionally, increasing L from 10 to 20 intervals downgrades the key agreement probability of the two platoons by 5% and 40%, respectively, which is further evaluated in the next case.

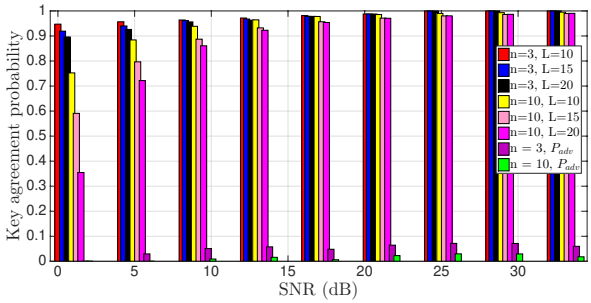

Fig. 2: Key agreement probability achieved by PlatoonKey with an increasing SNR.

As observed, P_{adv} of the eavesdropper also increases when $\overline{H_{i,j}}$ is raised, where L_{adv} is fixed at 20 intervals.

Fortunately, thanks to cooperative key generation of PlatoonKey, 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%.

B. CQI quantization intervals

In this case, we assess the performance of PlatoonKey when it operates on two platoons with either $n = 3$ or $n = 10$, as L increases from 25 intervals to 75 intervals. Figure 3 depicts that the key agreement probability generally decreases with the growth of L. Specifically, the key agreement probability of the 3-vehicle platoon is 29% higher than the 10-vehicle platoon 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 the following vehicles far from the lead one have large channel estimation error due to the poor channel quality. 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 platoon 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, platoon size, and link quality.

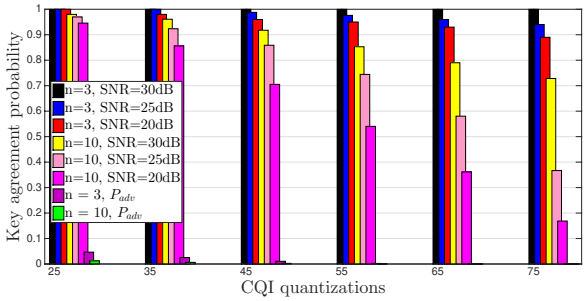

Fig. 3: Key agreement probability achieved by PlatoonKey with regards to the total quantization intervals, i.e., L.

VII. Conclusions and Discussion

In this paper, we study the platoon-based V2V communication security, where the platooning vehicles generate an unanimous secret key based on the quantized fading channel randomness. The problem of CQI quantization intervals optimization is formulated. Furthermore, PlatoonKey is proposed to maximize the key agreement probability by recursively optimizing the CQI quantization intervals, 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 quality of V2V channel and the CQI quantization intervals. We have also shown that the probability that eavesdroppers generate the same secret key, which is far lower than the one using PlatoonKey.

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).

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] 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)*, 2018.

[5] 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.

[6] K. Li, R. C. Voicu, S. S. Kanhere, W. Ni, and E. Tovard, "Energy efficient legitimate wireless surveillance of UAV communications," *IEEE Transactions on Vehicular Technology*, 2019.

[7] 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.

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

[9] 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.

[10] 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.

[11] 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.

[12] 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.

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

[14] 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.

[15] 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.