Secrecy Rate Maximization via Radio Resource Allocation in Cellular Underlaying V2V Communications

Yiliang Liu, *Student Member, IEEE*, Wei Wang, *Member, IEEE*, Hsiao-Hwa Chen, *Fellow, IEEE*, Liangmin Wang, *Member, IEEE*, Nan Cheng, *Member, IEEE*, Weixiao Meng, *Senior Member, IEEE*, and Xuemin Shen, *Fellow, IEEE*

***Abstract*—In device-to-device (D2D) underlaying vehicle-to-vehicle (V2V) communications, radio resource blocks (RBs) are allocated to primary cellular users, which yields sub-optimal rates and a long access latency for secondary D2D-enabled vehicles. This work investigates a joint radio resource and power management (RRPM) problem for secure cellular underlaying V2V communications, where cellular users and vehicles have the same priority, giving vehicles more opportunities to access the RBs. Specifically, we aim to maximize secrecy rates of V2V channels under the condition that eavesdropper has an adaptive receiving detection vector to maximize the received signal-to-interference-plus-noise ratio (SINR) from vehicles. For a single pair of a vehicle and a cellular user, the closed-form optimal power allocation expressions are derived for the interference-limited scenario and the noise-limited scenario, respectively. Moreover, for multiple pairs of vehicles and cellular users, a 3-partite hypergraph based 3-dimensional matching approach is proposed to solve a mixed-integer and non-convex problem, which achieves a near-optimal result with an $O(n^4)$ time complexity. Simulations in different scenarios show that the secrecy rate of the proposed scheme can be improved by 50% if compared to existing schemes.**

***Index Terms*—Cellular underlaying V2V communications, physical layer security, resource allocation, intelligently connected vehicle.**

Manuscript received October 26, 2019; revised February 21, 2020; accepted April 2, 2020. Date of publication April 8, 2020; date of current version July 16, 2020. This work was supported in part by the National Natural Science Foundation of China under Grants U1764263 and 61671186, in part by the Taiwan Ministry of Science and Technology under Grants 106-2221-E-006-028-MY3 and 106-2221-E-006-021-MY3, and in part by the Natural Sciences and Engineering Research Council (NSERC) of Canada. The review of this article was coordinated by Dr. J. Liu. *(Corresponding author: Hsiao-Hwa Chen.)*

Yiliang Liu and Weixiao Meng are with the School of Electronics and Information Engineering, Harbin Institute of Technology, Harbin 150001, China (e-mail: alanliuyiliang@gmail.com; wxmeng@hit.edu.cn).

Wei Wang, Nan Cheng, and Xuemin Shen are with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: wei.wang1@uwaterloo.ca; n5cheng@uwaterloo.ca; sshen@uwaterloo.ca).

Hsiao-Hwa Chen is with the Department of Engineering Science, National Cheng Kung University, Tainan City 70101, Taiwan (e-mail: hshwchen@mail.ncku.edu.tw).

Liangmin Wang is with the School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212000, China (e-mail: wanglm@ujs.edu.cn).

Digital Object Identifier 10.1109/TVT.2020.2986088

I. Introduction

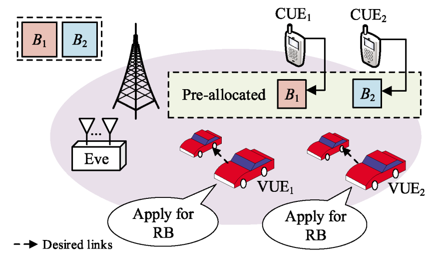
With the technological advancement in connected and autonomous vehicles, intelligently connected vehicles (ICVs) are expected to be equipped with sensors, automotive controllers and actuators, and use advanced network and communication technologies to exchange driving, sensing, and cooperative information among vehicles for autonomous driving [1]–[3].

Legacy solutions for V2V communications are based on ad-hoc technologies such as IEEE 802.11p standard, where a total 75 MHz bandwidth with seven sub-carriers in 5.85–5.925 GHz bands is allocated on physical layer. Each sub-carrier is medium-access-controlled by carrier-sense multiple access (CSMA) [4], and thus the V2V devices should wait for idle channels, which may be rare in rush hours. In order to satisfy the quality of service (QoS) requirements of massive access and different services in ICV networks, 3GPP Release 15 presents a baseline mode for V2V communications [5]. Specifically, the underlaying device-to-device (D2D) technologies are the enablers for the V2V physical layer architecture, in which the uplink spectrum of cellular networks allocated to cellular user equipments (CUEs) is shared with vehicle user equipments (VUEs) [6]. Benefited from the global deployment and wide spectrum band of 5 G systems, the coverages and physical layer resources of vehicular communications will be expanded dramatically. Following the 3GPP standard, plenty of researches have been conducted to investigate D2D-based V2V communications with radio resource allocation to address the issues on underlay-induced interference and performance improvement. The radio resource allocation schemes usually include RB assignment and power allocation [6]–[11].

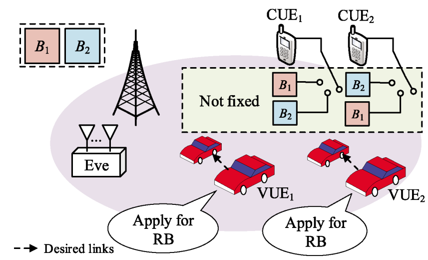
In V2V communications, confidentiality of transmitted information should be guaranteed as the leakage of driving information may cause serious consequences, such as malicious tracing, property loss, and driver casualties [12]–[15]. In IEEE 802.11p based V2V communications, message confidentiality is guaranteed via symmetric key agreement after time-consuming vehicle authentication processes [4]. In the 3GPP standard, the upper layer cryptographic protocols and complicated secret key managements are centrally controlled by the authentication, authorization, and accounting (AAA) servers, which require certificate managements, deployment of trusted third-parties and tamper-proof devices, and complex cryptographic computations [16]–[18]. In addition, cryptographic schemes cause extra latency due to centralized cryptography managements and complex cryptographic computing, and therefore they are not suitable for latency-critical ICV networks. As an important security mechanism, physical layer security achieves confidentiality via random characteristics of wireless medium, and can be implemented in a relatively efficient manner without cryptographic methods, which has received intensive research interests in ICV networks [19]–[21].

Recently, physical layer security based D2D communications has been studied in a large-scale cellular network. If underlaying D2D is used for secure communications without sophisticated resource managements, cellular system performance may be severely degraded because of underlay-induced interference. Power and RB allocation schemes were proposed for secrecy rate maximization of D2D links, where interference between cellular devices and D2D devices is limited at a low level [22]. On the contrary, underlay-induced interference with some delicate interference management can work as cooperative jamming to prevent eavesdroppers from wiretapping cellular links. Thus, Wang *et al.* improved channel capacities of D2D links and provided secure transmission for cellular users with the help of the interferences from D2D users [23]. Shen *et al.* designed a mode selection scheme, where each D2D pair can switch between the underlay and overlay modes according to different communication and security requirements [24]. Zhang *et al.* used a coalition algorithm to solve an RB sharing problem between D2D devices and cellular users to improve the sum secrecy rate in D2D links [25]. Zhang *et al.* made an effort to safeguard D2D-based V2V communications via physical layer security, where a Kuhn-Munkres (KM) algorithm was proposed to establish RB reuse pair of CUE and VUEs [26]. However, these physical layer security-aimed D2D technologies [22]–[26] are not suitable for secure ICV networks. That is because in traditional D2D-underlaying cellular networks, D2D transmissions are secondary with respect to cellular transmissions, where RBs are pre-allocated to CUEs and the resource allocation to D2D users that causes excessive interference to the CUEs is not allowed. Such a secondary D2D resource allocation may lead to two consequences. First, V2V pairs should wait for extra time if RBs are not free, leading to an extra delay, which is critical in delay-sensitive ICV applications. Second, the RB allocation is managed for CUEs and cannot achieve a global optimization on the tripartite allocation among CUEs, VUEs, and RBs. Therefore, we want to transform the traditional "primary" and "secondary" D2D mode to a new "primary" and "primary" D2D-V2V mode, in which RBs are not pre-allocated to CUEs, and thus RB allocation can be globally optimized based on the requirements of CUE rates and VUE secrecy rates, as shown in Fig. 1. This new concept is heuristic and has been accepted for cache optimization in D2D data dissemination [27], [28].

In this article, we propose a joint radio resource and power management (RRPM) scheme for secure ICV networks under strict latency and secrecy rate requirements. Specifically, the contributions of this article are summarized as follows.



(a) Primary CUEs and secondary VUEs mode



(b) Primary CUEs and primary VUEs mode

Fig. 1. Traditional "primary CUEs and secondary VUEs" mode and the proposed "primary CUEs and primary VUEs" mode, where RBs, i.e., B_1 and B_2 are per-allocated to CUEs in "primary CUEs and secondary VUEs" mode, whereas resource allocation in "primary CUEs and primary VUEs" mode treats both CUEs and VUEs equally.

1) We formulate an optimization problem for maximizing CUEs' capacities and VUEs' secrecy rates in Rician channels, which is the first work to treat CUEs and VUEs with the same RB priority for secure ICV networks. The joint RB allocation and transmission power optimization problem is a mixed-integer nonlinear optimization problem and is non-convex.
2) We use a 2-step strategy to transform the original problem to power allocation for a single CUE-VUE pair and RB allocation for multiple CUE-VUE pairs. The first step solves the power allocation problem in the interference-limited scenario and the noise-limited scenario, respectively, where closed-form power allocation expressions are deduced. In the general scenario, we use convex optimization and a one-dimensional searching algorithm to solve the power allocation problem. Then, we generate a 3-partite hypergraph based on the results of the first step, and propose a 3-dimensional matching algorithm on the 3-partite hypergraph to allocate RBs for multiple CUEs and VUEs.
3) We consider a scenario, where a multiple-antenna eavesdropper uses an adaptive receiving detection (ARD) vector for signal reception, with which the eavesdropper aims to maximize wiretap SINR from vehicles to impair the secrecy rates of V2V channels. The solution obtained from the optimization problem helps to avoid the secrecy outage if the eavesdropper uses the multiple antennas.

The notations used in this article are defined in the sequel. Bold uppercase letters denote matrices and bold lowercase letters denote column vectors. $\mathbf{A}^\dagger$ represents the Hermitian transpose of $\mathbf{A}$. $\mathbf{I}_a$ is an identity matrix with its rank a. $\mathcal{CN}(\mu, \Gamma)$ is a complex normal (or Gaussian) variable with its mean μ and

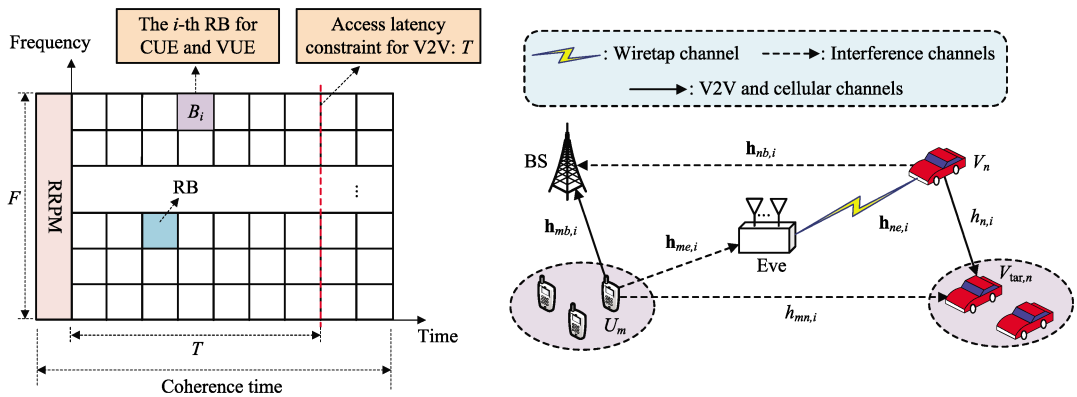


Fig. 2. A wiretap channel model in D2D-based V2V communications with 2-D structured RBs.

variance Γ. $(\mathbf{x})^{-1}$ is an inverse function of $\mathbf{x}$. $|\mathbf{x}|$ is the Euclidean norm of $\mathbf{x}$. $\mathrm{E}[\cdot]$ is an expectation operator. $\ln(\cdot)$ is the natural logarithm with the base e.

II. System Model

A. System and Channel Models

Let us consider a single cell network, which includes M CUEs, denoted by $\mathcal{M} = \{1, 2, \ldots, M\}$, and N VUEs, denoted by $\mathcal{N} = \{1, 2, \ldots, N\}$, where CUEs and VUEs share uplink radio resources. Both CUEs and VUEs are equipped with single antenna, while BS has N_r antennas and an eavesdropper (Eve) has N_e antennas. In this scenario, the available resources have a 2-D structure in frequency and time domains, as shown in Fig. 2, where the whole uplink spectrum is partitioned into F sub-carriers, defined as $\mathcal{F} = \{1, 2, \ldots, F\}$. A similar D2D scenario was assumed in [6], [30]. Investigations in [31], [32] showed that both vehicular and cellular channels are assumed to be Rician slow-fading channels, whose channel state information (CSI) is constant within the coherence time. The Rician channel model is a probabilistic model based on the assumption that there are a large number of statistically independent reflected and scattered paths. Also, a fixed line-of-sight path exists in addition to reflected and scattered paths. We define $\mathcal{T} = \{1, 2, \ldots, T\}$ as a set of time domain RB indices, where T is an access latency constraint for V2V communications, which should be smaller than the coherence time. Hence, the set of RB indices is denoted as $\mathcal{R} = \mathcal{F} \times \mathcal{T} = \{1, 2, \ldots, R\}$, where $R = F \times T$. Assume that each CUE uses one of the RBs to communicate with BS. Similarly, each VUE uses one of the RBs to communicate with another vehicle. However, an RB can be reused by a pair of CUE and VUE. The reuse will bring in interferences between vehicular and cellular links.

Assume that the mth CUE, i.e., U_m, and the nth VUE, i.e., V_n, share the ith RB, i.e., B_i. U_m communicates with BS while V_n communicates with its destination vehicle $V_{\text{tar},n}$, and thus intra-cell interference occurs in these reused RBs. In general, the interference channel between U_m and $V_{\text{tar},n}$ is defined as $h_{mn,i}$, and the interference channel between V_n and BS is denoted by an $N_r \times 1$ vector, i.e., $\mathbf{h}_{nb,i}$. In cellular communications, an $N_r \times 1$ vector, i.e., $\mathbf{h}_{mb,i}$, represents the cellular channel between U_m and BS. In vehicular communications, vehicular channel between V_n and $V_{\text{tar},n}$ is defined as $h_{n,i}$. Eve creates two channels, including an interference channel between U_m and Eve, defined by an $N_e \times 1$ vector, i.e., $\mathbf{h}_{me,i}$, and a wiretap channel between V_n and Eve, defined by an $N_e \times 1$ vector, i.e., $\mathbf{h}_{ne,i}$.

Here, assume all CSIs are available to BS and Eve, and the channels between CUEs and BS have been protected by AAA servers. We focus only on the V2V confidential transmission.

Within a given time period, B_i is shared by V_n and U_m. V_n transmits signal v_i to its receiving vehicle $V_{\text{tar},n}$, while U_m uses the same RB to send signal x_i to BS. The received signals at $V_{\text{tar},n}$ and BS, i.e., $y_{n,i}$ and $\mathbf{y}_{b,i}$ are

$$y_{n,i} = h_{n,i} v_i + h_{mn,i} x_i + n_{n,i}, \tag{1}$$

$$\mathbf{y}_{b,i} = \mathbf{h}_{mb,i} x_i + \mathbf{h}_{nb,i} v_i + \mathbf{n}_{mb,i}, \tag{2}$$

where

$$h_{n,i} = a_{n,i}\sqrt{\frac{k_{n,i}}{1+k_{n,i}}} + \hat{h}_{n,i}\sqrt{\frac{1}{1+k_{n,i}}}, \tag{3}$$

$$h_{mn,i} = a_{mn,i}\sqrt{\frac{k_{mn,i}}{1+k_{mn,i}}} + \hat{h}_{mn,i}\sqrt{\frac{1}{1+k_{mn,i}}}, \tag{4}$$

$$\mathbf{h}_{mb,i} = \alpha_{mb,i}\left(\mathbf{a}_{mb,i}\sqrt{\frac{k_{mb,i}}{1+k_{mb,i}}} + \hat{\mathbf{h}}_{mb,i}\sqrt{\frac{1}{1+k_{mb,i}}}\right), \tag{5}$$

$$\mathbf{h}_{nb,i} = \alpha_{nb,i}\left(\mathbf{a}_{nb,i}\sqrt{\frac{k_{nb,i}}{1+k_{nb,i}}} + \hat{\mathbf{h}}_{nb,i}\sqrt{\frac{1}{1+k_{nb,i}}}\right). \tag{6}$$

Here, $\hat{h}_{n,i}$ and $\hat{h}_{mn,i}$ are independent and identically distributed (i.i.d.) circular complex Gaussian random variables obeying $\mathcal{CN}(0,1)$. $\hat{\mathbf{h}}_{mb,i}$ and $\hat{\mathbf{h}}_{nb,i}$ are $N_r \times 1$ i.i.d. circular symmetric complex Gaussian random vectors obeying $\mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_r})$. $k_{n,i}$, $k_{mn,i}$, $k_{mb,i}$, and $k_{nb,i}$ are Rician fading factors. $a_{n,i}$ and $a_{mn,i}$ are deterministic complex constants containing the line-of-sight components of $h_{n,i}$ and $h_{mn,i}$. $\mathbf{a}_{mb,i}$ and $\mathbf{a}_{nb,i}$ are deterministic $N_r \times 1$ complex vectors containing the line-of-sight components of $\mathbf{h}_{mb,i}$ and $\mathbf{h}_{nb,i}$ [33]. v_i is the confidential signal from V_n encoded by Wyner coding [34], and x_i is the common signal from U_m, which satisfy the total power constraints as

$$\mathrm{E}\left[|v_i|^2\right] \le P_n^{sum}, \quad \mathrm{E}\left[|x_i|^2\right] \le P_m^{sum}, \tag{7}$$

where P_n^{sum} and P_m^{sum} are the powers of V_n and U_m. $n_{n,i}$ is an additive white Gaussian noise (AWGN) variable with $\mathcal{CN}(0,1)$, and $\mathbf{n}_{mb,i}$ is an AWGN vector obeying $\mathcal{CN}(\mathbf{0},\mathbf{I}_{N_r})$. We consider the large-scale fading effect in cellular channels by setting the large-scale fading factor of $\mathbf{h}_{mb,i}$ as $\alpha_{mb,i}$, and the large-scale fading factor of $\mathbf{h}_{nb,i}$ as $\alpha_{nb,i}$, respectively.

At the same time, Eve with N_e antennas wiretaps the signals from V_n, such that the received signal at V_e, i.e., $\mathbf{y}_{e,i}$, can be expressed as

$$\mathbf{y}_{e,i} = \mathbf{h}_{ne,i} v_i + \mathbf{h}_{me,i} x_i + \mathbf{n}_{ne,i}, \tag{8}$$

where

$$\mathbf{h}_{ne,i} = \mathbf{a}_{ne,i}\sqrt{\frac{k_{ne,i}}{1+k_{ne,i}}} + \hat{\mathbf{h}}_{ne,i}\sqrt{\frac{1}{1+k_{ne,i}}}, \tag{9}$$

$$\mathbf{h}_{me,i} = \mathbf{a}_{me,i}\sqrt{\frac{k_{me,i}}{1+k_{me,i}}} + \hat{\mathbf{h}}_{me,i}\sqrt{\frac{1}{1+k_{me,i}}}. \tag{10}$$

Here $\hat{\mathbf{h}}_{ne,i}$ and $\hat{\mathbf{h}}_{me,i}$ are $N_e \times 1$ i.i.d. circular symmetric complex Gaussian random vectors with the distribution $\mathcal{CN}(\mathbf{0},\mathbf{I}_{N_e})$. $\mathbf{a}_{ne,i}$ and $\mathbf{a}_{me,i}$ are deterministic complex constants containing the line-of-sight components of $\mathbf{h}_{ne,i}$ and $\mathbf{h}_{me,i}$, respectively. $\mathbf{n}_{ne,i}$ is an AWGN vector obeying $\mathcal{CN}(\mathbf{0},\mathbf{I}_{N_e})$.

B. ARD Vector Used by Eve

Assume that Eve knows the indices of the RBs and powers allocated to vehicles. Also assume that Eve has an ARD vector, i.e., a $1 \times N_e$ vector $\mathbf{w}_{ne,i}$, to maximize wiretap SNR, and thus Eve can find $\mathbf{w}_{ne,i}$, which is formulated as

$$\max_{\mathbf{w}_{ne,i}} \left(\frac{q_{n,i} P_{n,i} |\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2}{\mathbf{w}_{ne,i}(\mathbf{I}_{N_e} + q_{m,i} P_m^{sum} \mathbf{h}_{me,i}\mathbf{h}_{me,i}^{\dagger})\mathbf{w}_{ne,i}^{\dagger}} \right), \tag{11}$$

where $P_{n,i}$ is a fixed value, $q_{m,i}$ is a binary variable taking 1 when B_i is assigned to the mth CUE, and 0 otherwise, and so is $q_{n,i}$. From the knowledge of Rayleigh quotient, the optimal $\mathbf{w}_{ne,i}$ is the eigenvector of the largest eigenvalue of $(\mathbf{I}_{N_e} + q_{m,i}P_m^{sum}\mathbf{h}_{me,i}\mathbf{h}_{me,i}^{\dagger})^{-1}\mathbf{h}_{ne,i}\mathbf{h}_{ne,i}^{\dagger}$. With $\mathbf{w}_{ne,i}$, the estimated signal at Eve, i.e., $\hat{y}_{e,i}$, is

$$\hat{y}_{e,i} = \mathbf{w}_{ne,i}\mathbf{h}_{ne,i} v_i + \mathbf{w}_{ne,i}\mathbf{h}_{me,i} x_i + \mathbf{w}_{ne,i}\mathbf{n}_{ne,i}. \tag{12}$$

It is hard for Eve to obtain the information of transmission power of U_m because of the protection of AAA severs, such that Eve has to use the total power of U_m, i.e., P_m^{sum}, in the detection algorithm.

C. BS Detection Vector Design

To improve the cellular network performance, BS uses a zero-forcing (ZF) detection vector [35]. BS generates a $1 \times N_r$ detection vector $\mathbf{w}_{mb,i}$ to eliminate the interference from $\mathbf{h}_{nb,i}$ and gather the signals from $\mathbf{h}_{mb,i}$. The detection vector $\mathbf{w}_{mb,i}$ is

$$\mathbf{w}_{mb,i} = \frac{\mathbf{h}_{mb}^{\dagger}\mathbf{G}_{nb,i}^{\dagger}}{|\mathbf{G}_{nb,i}\mathbf{h}_{mb}|}, \tag{13}$$

where

$$\mathbf{G}_{nb,i} = \mathbf{I}_{N_r} - \mathbf{h}_{nb,i}(\mathbf{h}_{nb,i}^{\dagger}\mathbf{h}_{nb,i})^{-1}\mathbf{h}_{nb,i}^{\dagger}. \tag{14}$$

With $\mathbf{w}_{mb,i}$, the estimated signal at BS, i.e., $\hat{y}_{b,i}$, is

$$\hat{y}_{b,i} = \mathbf{w}_{mb,i}\mathbf{h}_{mb,i} x_i + \mathbf{w}_{mb,i}\mathbf{n}_{mb,i}. \tag{15}$$

In this case, the channel capacity between BS and U_m is a function of $P_{m,i}$ and $q_{m,i}$, i.e., $C_{m,BS,i}(P_{m,i}, q_{m,i})$, which is expressed as

$$C_{m,BS,i}(P_{m,i}, q_{m,i}) = \log_2(1 + \gamma_{m,BS,i}), \tag{16}$$

where

$$\gamma_{m,BS,i} = q_{m,i} P_{m,i} |\mathbf{w}_{mb,i}\mathbf{h}_{mb,i}|^2, \tag{17}$$

and $P_{m,i}$ is the transmission power of U_m on B_i. $q_{m,i}$ is a binary variable that is one when B_i is assigned to the mth CUE, and 0 otherwise.

D. Secrecy Rate Expression

Under the assumption that Eve uses the ARD vector i.e., $\mathbf{w}_{ne,i}$, the secrecy rate between V_n and $V_{\text{tar},n}$ is a function of $P_{m,i}$, $P_{n,i}$, $q_{m,i}$, and $q_{n,i}$, i.e., $R_{n,m,i}(P_{m,i}, P_{n,i}, q_{m,i}, q_{n,i})$, which is expressed as

$$\begin{aligned} &R_{n,m,i}(P_{m,i}, P_{n,i}, q_{m,i}, q_{n,i}) \\ &= [C_{n,i} - C_{n,e,i}]^+ \\ &= [\log_2(1+\gamma_{n,i}) - \log_2(1+\gamma_{n,e,i})]^+, \end{aligned} \tag{18}$$

where

$$\gamma_{n,i} = \frac{q_{n,i}P_{n,i}|h_{n,i}|^2}{1 + q_{m,i}P_{m,i}|h_{mn,i}|^2}, \tag{19}$$

$$\gamma_{n,e,i} = \frac{q_{n,i}P_{n,i}|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2}{1 + q_{m,i}P_{m,i}|\mathbf{w}_{ne,i}\mathbf{h}_{me,i}|^2}, \tag{20}$$

where $[x]^+ = \max(x, 0)$, and $C_{n,i}$ and $C_{n,e,i}$ are channel capacities of V2V and wiretap channels, respectively.

E. Problem Formulation

According to the earlier discussions, the problem is mathematically expressed as maximizing vehicles' sum secrecy rate in the cell. We can obtain vehicles' sum secrecy rate as

$$\begin{aligned} &R_{\text{sum}}(P_{m,i}, P_{n,i}, q_{m,i}, q_{n,i}, \forall n, m, i) \\ &= \sum_{i=1}^{R}\sum_{m=1}^{M}\sum_{n=1}^{N} R_{n,m,i}(P_{m,i}, P_{n,i}, q_{m,i}, q_{n,i}). \end{aligned} \tag{21}$$

Then, the sum secrecy rate maximization problem can be formulated as

$$\text{P1:} \max_{\left\{\substack{P_{m,i},P_{n,i}\\ q_{m,i},q_{n,i}\\ \forall n,m,i}\right\}} \left[R_{\text{sum}}(P_{m,i}, P_{n,i}, q_{m,i}, q_{n,i}, \forall n, m, i)\right], \tag{22}$$

$$\text{s.t. } q_{m,i} \in (0,1), q_{n,i} \in (0,1), \forall n, m, i, \tag{23}$$

$$0 \leq \sum_{i=1}^{R} q_{n,i} P_{n,i} \leq P_n^{sum}, \forall n, \tag{24}$$

$$0 \leq \sum_{i=1}^{R} q_{m,i} P_{m,i} \leq P_m^{sum}, \forall m, \tag{25}$$

$$\sum_{i=1}^{R} q_{n,i} \leq 1, \sum_{i=1}^{R} q_{m,i} \leq 1, \forall m, n, \tag{26}$$

$$\sum_{n=1}^{N} q_{n,i} \leq 1, \sum_{m=1}^{M} q_{m,i} \leq 1, \forall i, \tag{27}$$

$$C_{m,BS,i}(P_{m,i}, q_{m,i}) \geq \varepsilon_{m,i}, \forall m, \tag{28}$$

where $i \in \mathcal{R}$, $m \in \mathcal{M}$, $n \in \mathcal{N}$, and $q_{m,i}$ is equal to 1 if the mth CUE is assigned to the ith RB, and 0 otherwise. A similar definition applies to $q_{n,i}$. Eqns. (24) and (25) give transmission power constraints of V_n and U_m, respectively. Eqn. (26) reveals that each VUE or CUE can be allocated with only one RB. Eqn. (27) guarantees orthogonal RB allocation, i.e., each RB is only assigned to one CUE-VUE pair. Finally, Eqn. (28) specifies a channel capacity constraint for each CUE.

Obviously, P1 is a mixed-integer nonlinear problem and is non-convex. We transform this non-convex problem into two subproblems, i.e., a power allocation problem and an RB allocation problem, and address these problems via RRPM. Note that the CSI is constant within the coherence time, such that the results of the power allocation and RBs management are valid within the coherence time. Hence, the proposed algorithm should be executed within the coherence time. Here, we use a centralized resource allocation mechanism, where the BS is responsible for the RRPM process and informing vehicles their allocated RBs and transmission power parameters.

F. Workflow

The schedule of RRPM and secure transmissions is sketched as follows.

1) *Power allocation in the BS RRPM server:* The server determines optimal transmit power for all CUE-VUE-RB combinations, i.e., $P_{n.i}^*$ and $P_{m.i}^*$ for V_n and $U_m, \forall n, m, i$, then calculates the corresponding optimal secrecy rates, i.e., $R_{n,m,i}^*, \forall n, m, i$. The detail in the power optimization process is shown in Section IV. The parameters $P_{n.i}^*$ and $R_{n,m,i}^*$, $\forall n, m, i$ are delivered to the RB allocation process.
2) *RB allocation in the BS RRPM server:* The data set $R_{n,m,i}^*$, $\forall n, m, i$ records optimal results of all CUE-VUE-RB combinations. For any RB, such as B_i, RB allocation is used to find the optimal RB-reused combination, i.e., $q_{n,i}$ and $q_{m,i}$, to maximize the vehicles' sum secrecy rate.
3) *Transmission of vehicles:* The RB license, i.e., $q_{n,i}$, the corresponding transmission power of V_n, i.e., $P_{n,i}^*$, and the corresponding secrecy rate, i.e., $R_{n,m,i}^*$, are sent to V_n from BS. $R_{n,m,i}^*$ is set as the Wyner coding rate to encode the confidential message. Finally, V_n uses $P_{n,i}^*$ to transmit the message to its targeted vehicle via B_i.

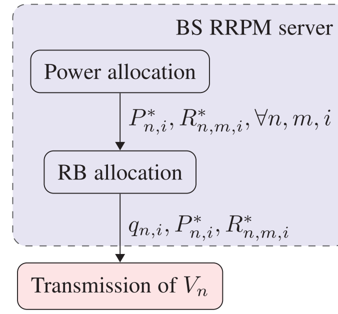


Fig. 3. The workflow includes the power allocation and RB allocation in the BS RRPM server (in the blue frame) and vehicular transmissions (in the red frame).

The workflow of the RRPM scheme including three aforementioned steps is shown in Fig. 3. The RRPM scheme focuses on establishing secure V2V communications. For any CUE, such as U_m, the RB license $q_{m,i}$ and the power parameter $P_{m.i}^*$ are delivered to U_m via independent cellular control links [16].

III. Optimal Power Allocation for Single CUE-VUE Pair

In this section, we will design an optimal power allocation scheme based on each possible CUE-VUE reuse pair. Given that V_n shares B_i with U_m, the power allocation problem of this single CUE-VUE pair can be formulated as

$$\text{P2:} \max_{P_{m,i}, P_{n,i}} \left[R_{n,m,i}(P_{m,i}, P_{n,i}, 1, 1) \right], \tag{29}$$

$$\text{s.t. } 0 \leq P_{n,i} \leq P_n^{sum}, \tag{30}$$

$$0 \leq P_{m,i} \leq P_m^{sum}, \tag{31}$$

$$C_{m,BS,i}(P_{m,i}, 1) \geq \varepsilon_{m,i}. \tag{32}$$

We can observe that $R_{n,m,i}(P_{m,i}, P_{n,i}, 1, 1)$ is a non-convex function of $P_{m,i}$ and $P_{n,i}$. Therefore, first we transform this non-convex problem into two convex problems in interference-limited and noise-limited scenarios, and derive closed-form expressions for $P_{m,i}$ and $P_{n,i}$. Then, we consider a general case and present a one-dimensional search algorithm for the secrecy rate maximization problem.

A. Approximate Power Allocation

1) Noise-Limited Scenarios: In a noise-limited scenario, we have $P_{m,i}|h_{mn,i}|^2 \gg 1$ and $P_{m,i}|\mathbf{w}_{ne,i}\mathbf{h}_{me,i}|^2 \gg 1$. Ignoring AWGN in Eqns. (19) and (20), we can simplify $R_{n,m,i}(P_{m,i}, P_{n,i}, 1, 1)$ as

$$R_{n,m,i}(P_{m,i}, P_{n,i}, 1, 1) = \left[\log_2 \left(\frac{P_{n,i}|h_{n,i}|^2 + P_{m,i}|h_{mn,i}|^2}{P_{n,i}|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2 + P_{m,i}|\mathbf{w}_{ne,i}\mathbf{h}_{me,i}|^2} \rho \right) \right]^+, \tag{33}$$

where

$$\rho = \frac{|\mathbf{w}_{ne,i}\mathbf{h}_{me,i}|^2}{|h_{mn,i}|^2}. \tag{34}$$

Eqn. (33) is the secrecy rate of a V2V channel with a single pair (U_m and V_n) when $q_{n,i} = q_{m,i} = 1$ in a noise-limited scenario.

2) Interference-Limited Scenarios: In an interference-limited scenario, we have $P_{m,i}|h_{mn,i}|^2 \ll 1$ and $P_{m,i}|\mathbf{w}_{ne,i}\mathbf{h}_{me,i}|^2 \ll 1$. Ignoring interference terms in Eqns. (19) and (20), we can simplify $R_{n,m,i}(P_{m,i}, P_{n,i}, 1, 1)$ as

$$R_{n,m,i}(P_{m,i}, P_{n,i}, 1, 1) = \left[\log_2\left(\frac{1 + P_{n,i}|h_{n,i}|^2}{1 + P_{n,i}|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2}\right)\right]^+. \tag{35}$$

Eq. (35) is the secrecy rate of a V2V channel with a single pair (U_m and V_n) when $q_{n,i} = q_{m,i} = 1$ in an interference-limited scenario.

Proposition 1: In both interference-limited and noise-limited scenarios, an optimal solution of $P_{n,i}$ and $P_{m,i}$ in P2 always exists on the boundary of the constraint (32).

Moreover, the optimal solution of $P_{n,i}$ and $P_{m,i}$ in P2 admits a closed-form expression, which is given in the following two cases.

- *Case 1:* In a noise-limited scenario, if $|h_{mn,i}|^2 |\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2 \geq |h_{n,i}|^2|\mathbf{w}_{ne,i}\mathbf{h}_{me,i}|^2$, we have

$$P^*_{n,i} = 0, \quad P^*_{m,i} = c_i, \tag{36}$$

where

$$c_i = \frac{2^{\varepsilon_{m,i}} - 1}{|\mathbf{w}_{mb,i}\mathbf{h}_{mb,i}|^2}. \tag{37}$$

If $|h_{mn,i}|^2|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2 < |h_{n,i}|^2|\mathbf{w}_{ne,i}\mathbf{h}_{me,i}|^2$, the optimal solution is given by

$$P^*_{n,i} = P^{sum}_n, \quad P^*_{m,i} = c_i. \tag{38}$$

- *Case 2:* In an interference-limited scenario, if $|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2 \geq |h_{n,i}|^2$, we have

$$P^*_{n,i} = 0, \quad P^*_{m,i} = c_i. \tag{39}$$

If $|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2 < |h_{n,i}|^2$, we have

$$P^*_{n,i} = P^{sum}_n, \quad P^*_{m,i} = c_i. \tag{40}$$

Proof: See Appendix A. ∎

Remark 1: It is deduced from Case 1 that when the combined gain of wiretap channels and interference channels between U_m and V_n is larger than the combined gain of the main channel and interference channels between U_m and Eve, there is no positive secrecy rate. Hence, the optimal choice is to set $P_{n,i} = 0$, and let SINR from U_m to BS approach to the threshold. In the situation that the combined gain of the main channel and interference channels between U_m and Eve is relatively high, a positive secrecy rate always exists. VUEs prefer to use their total power to send signals, while CUEs use the pre-defined thresholds for BS. In addition, based on $\mathbf{w}_{ne,i}$, increasing P^{sum}_m will increase $|\mathbf{w}_{ne,i}\mathbf{h}_{me,i}|^2$, and thus allows a vehicle to have $|h_{mn,i}|^2|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2 < |h_{n,i}|^2|\mathbf{w}_{ne,i}\mathbf{h}_{me,i}|^2$ to achieve a positive secrecy rate.

Remark 2: Case 2 is relevant to an interference-limited scenario, where the interference channels of CUE are ignored. Hence, if the gain of wiretap channels is larger than the main channel, the secrecy rate is always zero. If the main channel becomes better, secrecy rates increase with an increasing $P_{n,i}$, such that VUEs try their best to send signals with a pre-defined threshold for BS. In addition, increasing P^{sum}_m will decrease $|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2$, and thus more likely a vehicle has $|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2 < |h_{n,i}|^2$ to achieve a positive secrecy rate.

In conclusion, the secrecy rate will be improved by increasing P^{sum}_n and P^{sum}_m.

B. General Case

Since $R_{n,m,i}(P_{m,i}, P_{n,i}, 1, 1)$ is a non-convex function with $P_{m,i}$ and $P_{n,i}$, we transform P2 into a convex optimization problem by introducing an auxiliary variable θ as

$$\text{P3: } \max_{\theta}[\chi(\theta)], \tag{41}$$

where $\chi(\theta)$ is defined as

$$\chi(\theta) = \max_{P_{m,i}, P_{n,i}} \left[\log_2(1 + \gamma_{n,i}) - \log_2(1 + \theta)\right], \tag{42}$$

$$\text{s.t. } \log_2(1 + \gamma_{n,e,i}) \leq \log_2(1 + \theta), \tag{43}$$

$$\text{Constraints (30), (31), and (32).} \tag{44}$$

Here, $\chi(\theta)$ is still non-convex. We use Charnes-Cooper transform to transform this non-convex optimization into a convex one via changing transmission power variables to

$$Q_{n,i} = \varphi P_{n,i}, \quad Q_{m,i} = \varphi P_{m,i}, \quad \varphi > 0, \tag{45}$$

and thus $\chi(\theta)$ can be transformed to

$$\chi'(\theta) = \max_{Q_{m,i}, Q_{n,i}, \varphi} \left(\varphi + Q_{n,i}|h_{n,i}|^2 + Q_{m,i}|h_{mn,i}|^2\right), \tag{46}$$

$$\text{s.t. } (\varphi + Q_{m,i}|h_{mn,i}|^2)(1 + \theta) = 1, \tag{47}$$

$$Q_{n,i}|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2 - \varphi\theta - \theta Q_{m,i}|\mathbf{w}_{ne,i}\mathbf{h}_{me,i}|^2 \leq 0, \tag{48}$$

$$Q_{n,i} - \varphi P^{sum}_n \leq 0, \tag{49}$$

$$Q_{m,i} - \varphi P^{sum}_m \leq 0, \tag{50}$$

$$Q_{m,i}|\mathbf{w}_{mb,i}\mathbf{h}_{mb,i}|^2 - \varphi\eta_{m,i} \geq 0, \tag{51}$$

$$Q_{n,i} \geq 0, \quad Q_{m,i} \geq 0, \quad \varphi > 0, \tag{52}$$

where $\eta_{m,i} = 2^{\varepsilon_{m,i}} - 1$. The objective function in Eqn. (46) is an affine function with $Q_{n,i}$, $Q_{m,i}$, and φ. Eqn. (47) is a hyperplanes with $Q_{m,i}$ and φ. The inequality (48) is a convex function with $Q_{n,i}$, $Q_{m,i}$, and φ. The inequality (49) is a convex function with $Q_{n,i}$ and φ. The inequalities (50) and (51) are convex with $Q_{m,i}$ and φ. Hence, $\chi'(\theta)$ is a convex problem that can be solved by CVX package. Note that $\chi'(\theta)$ has no valid solution in some CSI cases. For example, if the main CSI $h_{n,i}$ is very small, there is no valid solution and the secrecy rate is zero. In this case, the vehicular transmission stops to avoid the information leakage.

The maximum of $\chi(\theta)$ in P3 can be obtained through one-dimensional search, while Algorithm 1 is to solve the maximum of $\chi(\theta)$ for each trial $\theta \in [\theta_{\min}, \theta_{\max}]$, where

$$\theta_{\min} = 0, \quad \theta_{\max} = P^{sum}_n|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2. \tag{53}$$

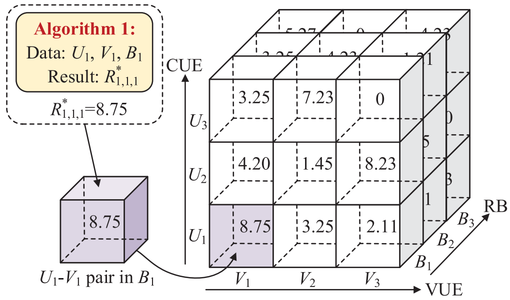


Fig. 4. A 3-D matrix for formulating a 3-partite hypergraph, where each nest stores the optimal secrecy rate for a given CUE-VUE-RB combination. Given 3 CUEs, 3 VUEs and 3 RBs, the 3-D matrix needs 27 nests to store the results of these combinations.

Algorithm 1: One-Dimensional Power Allocation Search Algorithm for a Single CUE-VUE Pair.

Data: U_m, V_n, B_i
Result: $P^*_{m,i}$, $P^*_{n,i}$, and $R^*_{n,m,i}$
1: **Initialization**;
2: Initial: P_n^{sum}, P_m^{sum}, and CUE channel capacity threshold $\varepsilon_{m,i}$;
3: Channel estimation: $h_{n,i}$, $\mathbf{h}_{nb,i}$, $h_{mn,i}$, $\mathbf{h}_{mb,i}$, $\mathbf{h}_{me,i}$, $\mathbf{h}_{ne,i}$;
4: Calculate $\theta_{\max} = P_n^{sum}|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2$, and $\theta_{\min} = 0$;
5: Find θ^* to maximize $\chi'(\theta)$ in $\{\theta_{\min}, \theta_{\max}\}$ via one-dimensional search;
6: Calculate $P^*_{m,i} = Q^*_{m,i}/\varphi^*$, $P^*_{n,i} = Q^*_{n,i}/\varphi^*$, and $R^*_{n,m,i} = R_{n,m,i}(P^*_{m,i}, P^*_{n,i}, 1, 1)$ for given θ^*;
7: **Procedure End**

We do not know how many peaks in $\chi(\theta)$ within $[\theta_{\min}, \theta_{\max}]$, and thus one-dimensional searching algorithms, such as genetic algorithm, simulated annealing, and interval arithmetic-based technique, can be used in one-dimensional searching [37]. In this work, we used interval-based technique.

IV. Radio Resource Management for Multiple CUES, VUES, and RBS

In this section, we introduce a global radio resource management (RRM) algorithm for multiple CUEs, VUEs, and RBs. Given that each CUE-VUE pair has been allocated an RB, we use Algorithm 1 to calculate the optimal $R^*_{n,m,i}$ for each RB via adjusting transmission power, and then generate a 3-partite hypergraph to record all CUE-VUE-RB combinations, as shown in Fig. 4. Then, the BS allocates RBs to both VUEs and CUEs based on the 3-partite hypergraph. Since the CSI is constant within the coherence time, if RBs belong to the same spectrum, these RBs have the same optimal secrecy rate for a given CUE-VUE pair.

A. 3-Partite Hypergraph Generation via Extending Virtual VUEs, CUEs, and RBs

The hypergraph theory has been recognized as a useful mathematical tool in 5 G research [28]. We first introduce the definition of the 3-partite hypergraph as follows.

Definition 1 (3-partite hypergraph [38]): $\mathcal{H} = (\mathcal{V}, \mathcal{E})$ is regarded as a 3-partite hypergraph if a vertex set $\mathcal{V}$ can be divided into 3 sub-sets $\mathcal{V}_1$, $\mathcal{V}_2$, and $\mathcal{V}_3$, in which every hyperedge contains only one vertex from every vertex subset. The 3-dimensional matching on a 3-partite hypergraph means a subset of hyperedges of hypergraph and any two hyperedges do not share a vertex.

Let us transform the RB allocation problem into an iterative Kuhn and Munkres (KM) algorithm on a 3-partite hypergraph, where optimal secrecy rate and power allocation have been efficiently computed in Section IV. The 3-partite hypergraph generation requires that the numbers of CUEs, VUEs, and RBs are the same. Hence, we use a concept of virtual CUEs, VUEs, and RBs to handle the 3-partite hypergraph generation first.

1) Virtual VUEs, CUEs, and RBs Generation: As described in Section II, the numbers of CUEs, VUEs, and RBs are M, N, and R, respectively. Define $Z = \max(M, N, R)$ in advance. Then, we generate virtual CUEs, VUEs, and RBs using the following rules.

1) If the number of CUEs is smaller than Z, i.e., $M < Z$, we will set $Z - M$ virtual CUEs indexed by $\{M+1, M+2, \ldots, Z\}$, define a CUE set as $\mathcal{M}_Z = \{1, \ldots, M, M+1, \ldots, Z\}$, and then set $R^*_{n,m,i} = -\infty$ for $m \in \{M+1, M+2, \ldots, Z\}$.
2) If the number of VUEs is smaller than Z, i.e., $N < Z$, we will set $Z - N$ virtual VUEs indexed by $\{N+1, N+2, \ldots, Z\}$, define a VUE set as $\mathcal{N}_Z = \{1, \ldots, N, N+1, \ldots, Z\}$, and then set $R^*_{n,m,i} = -\infty$ for $n \in \{N+1, N+2, \ldots, Z\}$.
3) If the number of RBs is smaller than Z, i.e., $R < Z$, we will set $Z - R$ virtual RBs indexed by $\{R+1, R+2, \ldots, Z\}$, define an RB set as $\mathcal{R}_Z = \{1, \ldots, R, R+1, \ldots, Z\}$, and then set $R^*_{n,m,i} = -\infty$ for $i \in \{R+1, R+2, \ldots, Z\}$. For given m and n, $R^*_{n,m,i} = R^*_{n,m,j}$ if $i, j \in f \times \mathcal{T}$ and $f \in \mathcal{F}$.

With the same number of CUEs, VUEs, and RBs, we can generate a 3-partite hypergraph as follows.

2) 3-Partite Hypergraph Generation: First, we establish a scenario as a hypergraph $\mathcal{H} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is a set of vertices divided into three disjoint sub-sets $\mathcal{M}_Z$, $\mathcal{N}_Z$, and $\mathcal{F}_Z$. $\mathcal{E} \subseteq \mathcal{M}_Z \times \mathcal{N}_Z \times \mathcal{F}_Z$ denotes a set of hyperedges in the hypergraph. Vertex $V_n, n \in \{1, \ldots, Z\}$ in subset $\mathcal{N}_Z$ denotes the nth VUE, vertex $U_m, m \in \{1, \ldots, Z\}$ in subset $\mathcal{M}_Z$ denotes the mth CUE, and vertex $B_i, i \in \{1, \ldots, Z\}$ in subset $\mathcal{F}_Z$ denotes the ith RB. For each CUE-VUE-RB combination, we get a hyperedge $e_{n,m,i} = (V_n, U_m, B_i)$ and define its weight $W_{n,m,i} = R^*_{n,m,i}$ from Algorithm 1, which represents the optimal secrecy rate when V_n shares B_i with U_m. Note that when there is no positive secrecy rate, $W_{n,m,i} = 0$, and for virtual CUEs, VUEs and RBs, $W_{n,m,i} = -\infty$. Finally, we use a $Z \times Z \times Z$ 3-D matrix in Fig. 4 to save this weight information as $\mathbf{W}$, with the (m, n, i)th element as $W_{n,m,i}$.

We set a $Z \times Z \times Z$ matching matrix $\mathbf{E}$, whose (m, n, i)-th element represents a hyperedge, i.e., $e_{n,m,i}$. For another hyperedge $e_{n,'m,'i'}$, we have $n \neq n'$, $m \neq m'$, and $i \neq i'$ to satisfy the constraint that any two hyperedges do not share a vertex. $e_{n,m,i} = 1, n \in \mathcal{N}_Z, m \in \mathcal{M}_Z, i \in \mathcal{F}_Z$ when the hyperedge is included in a matching. We aim to find an optimal $\mathbf{E}$ to maximize $\sum_{n=1}^{Z}\sum_{m=1}^{Z}\sum_{i=1}^{Z} e_{n,m,i}W_{n,m,i}$.

B. 3-Dimensional Matching Problem on 3-Partite Hypergraph

1) 3-Dimensional Matching Problem: Solving the optimal $\mathbf{E}$ is an integer programming problem because $e_{n,m,i} = 1$ if V_n shares B_i with U_m, and $e_{n,m,i} = 0$ otherwise. The 3-dimensional matching problem is now formulated as

$$\text{P4:} \max_{e_{n,m,i}} \left(\sum_{n=1}^{Z}\sum_{m=1}^{Z}\sum_{i=1}^{Z} e_{n,m,i}W_{n,m,i} \right), \tag{54}$$

$$\text{s.t. } e_{n,m,i} = (0,1), \forall n,m,i, \tag{55}$$

$$\sum_{n=1}^{Z} e_{n,m,i} \leq 1, \; \sum_{m=1}^{Z} e_{n,m,i} \leq 1,$$

$$\sum_{i=1}^{Z} e_{n,m,i} \leq 1, \forall n,m,i, \tag{56}$$

where Eqn. (56) enforces that each RB can be used by only one pair, and each CUE or VUE has at most one RB. This is a classic 3-dimensional matching problem, and searching for optimal (q_n, q_m) in P1 equals to find optimal $e_{n,m,i}$ for $n \in \mathcal{N}_Z, m \in \mathcal{M}_Z, i \in \mathcal{F}_Z$. $\sum_{n=1}^{Z} e_{n,m,i}$, $\sum_{m=1}^{Z} e_{n,m,i}$, and $\sum_{i=1}^{Z} e_{n,m,i}$ may be smaller than one (equals to zero) because the model has virtual CUEs, VUEs, and RBs.

P4 is a NP-complete problem that can be solved by an exhaustive search algorithm with a complexity $O(Z!)$, and outputs the optimal $\mathbf{E}$. It is desirable to design an algorithm that can solve P4 with an acceptable time complexity to obtain a near optimal performance. We use an iterative method to solve the challenging problem by transforming the 3-dimensional matching problem into three iterative 2-dimensional matching problems, i.e., P4.1, P4.2, and P4.3, each of which can be solved by KM algorithm. The iterative method uses the following rules.

1) P4.1: for an initial allocation of RBs to CUEs, search for an optimal allocation of CUEs to VUEs.
2) P4.2: for the allocation results of CUEs to VUEs in P4.1, search for an optimal allocation of VUEs to RBs.
3) P4.3: for the allocation results of VUEs to RBs in P4.2, search for an optimal allocation of RBs to CUEs.

A similar iterative KM algorithm was used for cache allocation in traditional D2D communications [27].

2) Iterative KM-based RB Allocation: Assume that we have an arbitrary initial allocation for RB-CUE pairs, i.e., $\mathbf{b}^0 = \{e_{n,m,i} = 1 | (m,i), \forall m,n,i\}$ for given (m,i) combinations, which satisfies the constraint $\sum_{m=1}^{Z} e_{n,m,i} \leq 1$ and $\sum_{i=1}^{Z} e_{n,m,i} \leq 1$. The 3-dimensional matching problem will be reduced to a 2-dimensional matching problem as

$$\text{P4.1:} \max_{\mathbf{b}^1} \left(\sum_{n=1}^{Z}\sum_{m=1}^{Z} e_{n,m,i}W_{n,m,i} \right), \tag{57}$$

$$\text{s.t. } e_{n,m,i} = (0,1), \forall n,m, \tag{58}$$

Algorithm 2: Alternating KM Algorithm for Radio Resource Allocation for Multiple CUE-VUE-RB.

Data: $R^*_{n,m,i}, \forall n,m,i$, and $Z = \max(M,N,R)$
Result: $q_{n,i}$, $q_{m,i}$, $\forall n,m,i$

Initialization;
Initial: $\text{iter} = 1$, and the iterating limit $\text{iter}_{\max}$;
Initial: the initial RB and CUE allocation via $\mathbf{b}^0 = \{e_{n,m,i} = 1 | (m,i), \forall m,n,i\}$;
Generate a $Z \times Z \times Z$ 3-D matrix $\mathbf{W}$ based on $R^*_{n,m,i}, \forall n,m,i$, as shown in Fig. 4;
Generate a $Z \times Z$ matrix $\mathbf{T}_1(\text{iter})$ by reducing the RB dimension of $\mathbf{W}$ with $\mathbf{b}^0$, as shown in Fig. 5;
while $\text{iter} < \text{iter}_{\max}$ **do**
  for $k \in \{1,2,3\}$ **do**
    Do KM Algorithm on the matrix $\mathbf{T}_k(\text{iter})$, and output a $Z \times 1$ matching vector $\mathbf{b}^k$, where $b_i^k = \{0,1\}, i \in \{1,\ldots,Z\}$;
    if *k=1* **then**
      $\mathbf{b}^1 = \{e_{n,m,i} = 1 | (m,n), \forall m,n,i\}$, and reduce the CUE dimension of $\mathbf{W}$ to generate a $Z \times Z$ $\mathbf{T}_2(\text{iter})$ based on $\mathbf{b}^1$;
    else if *k=2* **then**
      $\mathbf{b}^2 = \{e_{n,m,i} = 1 | (n,i), \forall m,n,i\}$, and reduce the VUE dimension of $\mathbf{W}$ to generate a $Z \times Z$ $\mathbf{T}_3(\text{iter})$ based on $\mathbf{b}^2$;
    else
      $\mathbf{b}^3 = \{e_{n,m,i} = 1 | (m,i), \forall m,n,i\}$, and reduce the RB dimension of $\mathbf{W}$ to generate a $Z \times Z$ $\mathbf{T}_1(\text{iter})$ based on $\mathbf{b}^3$;
  Generate a $Z \times Z \times Z$ 3-D allocation matrix $\mathbf{E}(\text{iter})$ via $\mathbf{b}^3 = \{e_{n,m,i} = 1 | (m,i), \forall m,n,i\}$ and $\mathbf{b}^2 = \{e_{n,m,i} = 1 | (n,i), \forall m,n,i\}$;
  if $\text{iter} > 2$ *and* $\mathbf{E}(\text{iter}) = \mathbf{E}(\text{iter}-1)$ **then**
    $\{m,n,i\} = \text{find}((e_{n,m,i}) = 1 | \mathbf{E}_{m,n,i}(\text{iter}))$, then, $q_{n,i} = 1$ and $q_{m,i} = 1$, break;
Procedure End

$$\sum_{n=1}^{Z} e_{n,m,i} \leq 1, \; \sum_{m=1}^{Z} e_{n,m,i} \leq 1, \forall n,m, \tag{59}$$

where Eqn. (59) indicates that each RB can be used by only one CUE-VUE pair. This is a 2-dimensional matching problem that is solved by KM algorithm before we obtain optimal $\mathbf{b}^1 = \{e_{n,m,i} = 1 | (m,n), \forall m,n,i\}$. The entire process, including dimension reduction and KM algorithm, is shown in Fig. 5.

The optimal $\mathbf{b}^1 = \{e_{n,m,i} = 1 | (m,n), \forall m,n,i\}$ gives a condition for VUE-RB allocation, which is the second 2-dimensional matching problem expressed as

$$\text{P4.2:} \max_{\mathbf{b}^2} \left(\sum_{n=1}^{Z}\sum_{i=1}^{Z} e_{n,m,i}W_{n,m,i} \right), \tag{60}$$

$$\text{s.t. } e_{n,m,i} = (0,1), \forall n,i, \tag{61}$$

$$\sum_{n=1}^{Z} e_{n,m,i} \leq 1, \; \sum_{i=1}^{Z} e_{n,m,i} \leq 1, \forall n,i, \tag{62}$$

where Eqn. (62) reveals that the allocated CUE in P4.1 can share its RB with only one VUE. This is also a 2-dimensional matching problem, which is solved by KM algorithm and gives optimal $\mathbf{b}^2 = \{e_{n,m,i} = 1 | (n,i), \forall m,n,i\}$.

Similarly, the optimal $\mathbf{b}^2 = \{e_{n,m,i} = 1 | (n,i), \forall m,n,i\}$ is a condition for the RB-CUE allocation, which is the third 2-dimensional matching problem written as

$$\text{P4.3:} \max_{\mathbf{b}^3} \left(\sum_{m=1}^{Z}\sum_{i=1}^{Z} e_{n,m,i}W_{n,m,i} \right), \tag{63}$$

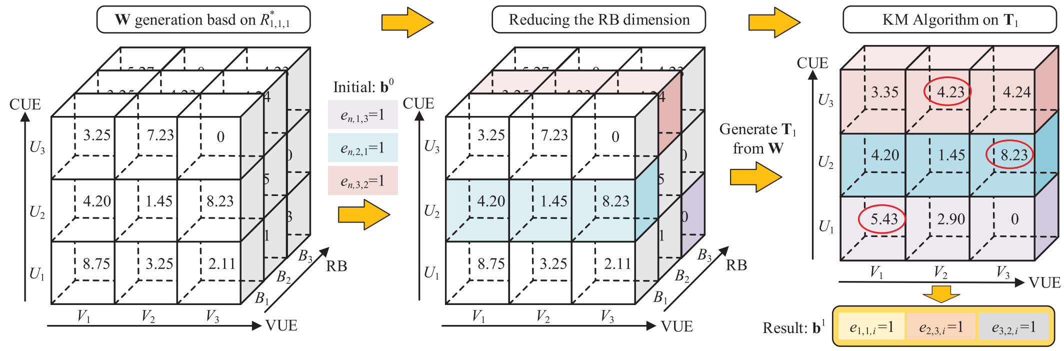


Fig. 5. KM algorithm of matrix $\mathbf{T}_1$ that is a dimension-reduced from of $\mathbf{W}$ via $\mathbf{b}^0$. $\mathbf{T}_1$ includes CUE dimension and VUE dimension. The optimal allocation of P4.1, i.e., $\mathbf{b}^1 = \{e_{n,m,i} = 1|(m,n), \forall m,n,i\}$, is the input of P4.2 for the allocation in VUE dimension and RB dimension.

$$\text{s.t. } e_{n,m,i} = (0,1), \forall m,i, \tag{64}$$

$$\sum_{m=1}^{Z} e_{n,m,i} \leq 1, \ \sum_{i=1}^{Z} e_{n,m,i} \leq 1, \forall m,i, \tag{65}$$

where Eqn. (65) indicates the fact that the allocated VUE in P4.2 can share its RB with only one CUE. The 2-dimensional matching is solved by KM algorithm and yields optimal $\mathbf{b}^3 = \{e_{n,m,i} = 1|(m,i), \forall m,n,i\}$, which is a condition for P4.1 in the next iteration. Hence, we implement the subsequent iteration as

$$\text{P4.1} \rightarrow \text{P4.2} \rightarrow \text{P4.3} \rightarrow \text{P4.1} \rightarrow \ldots, \tag{66}$$

and generate $\mathbf{E}(\text{iter})$ via $\mathbf{b}^3 = \{e_{n,m,i} = 1|(m,i), \forall m,n,i\}$ and $\mathbf{b}^2 = \{e_{n,m,i} = 1|(n,i), \forall m,n,i\}$ of P4.2 and P4.3, at the iter-th iteration. The iteration process continues until $\mathbf{E}(\text{iter}) = \mathbf{E}(\text{iter} - 1)$. The details have been given in Algorithm 2.

Proposition 2: $\sum_{n=1}^{Z} \sum_{m=1}^{Z} \sum_{i=1}^{Z} e_{n,m,i} W_{n,m,i}$ converges when $\mathbf{E}(\text{iter}) = \mathbf{E}(\text{iter} - 1)$.

Proof: See Appendix B. ■

The time complexity of the KM algorithm is $O(Z^4)$ [39], and we perform the KM algorithms for three times in each iterative. The time complexity to generate the 3-partite hypergraph is $O(Z^3)$. The total time complexity of RRPM is $O(Z^4)$ in the worst case, where $Z = \max(M,N,R)$. That is to say the resource allocation problem can be solved in a polynomial time $O(Z^4)$, and thus it is a "P-problem". In a real environment, vehicular speed varies from 10 m/s to 30 m/s, with its corresponding channel coherence time changing approximately from 2 ms to 0.68 ms in 6 GHz bands [40]. It seems that real-time resource allocation is achievable with currently available customized ICs at BS [41].

V. Simulations

In this section, simulation results are presented to verify the analysis. In the simulations, we assume that the Rician channels are constant within the coherence time, and the proposed algorithm independently runs once in the coherence time. Each value in the simulation figures is the average of the results of 1000 independent runs. Specifically, all elements in $\mathbf{a}_{nb,i}$, $\mathbf{a}_{mb,i}$, $\mathbf{a}_{me,i}$, and $\mathbf{a}_{ne,i}$ equal to one, and $a_{n,i} = a_{m,i} = 1$, for all m,n,i. For the large-scale fading factors, $\alpha_{mb,i} = 0.8$, and $\alpha_{nb,i} = 0.8$, for all m,n,i. Assume that all Rician factors are equal to one, i.e., $k_{n,i} = k_{mn,i} = k_{mb,i} = k_{nb,i} = k_{ne,i} = k_{me,i} = 1$ for all m,n,i. Also, we have $N_r = 4$ and $N_e = 2$.

In addition, three different schemes, i.e., Optimum, Greed, and Separate resource block and power allocation (SOLEN), are compared with our proposed scheme. The three compared schemes are briefly introduced as follows.

1) *Optimum:* It is an exhaustive search algorithm that can obtain global optimal results via brute force searching for all allocation schemes. Its time complexity is $O(Z!)$.
2) *Greed:* It is a greed algorithm that finds optimal VUE-CUE reuse pair with the current CUE-RB allocation. Its time complexity equals to that of KM algorithm, i.e., $O(Z^4)$. Note that this algorithm was adopted in many papers for rate or secrecy rate optimization in D2D scenarios [25], [26], [42], [43].
3) *SOLEN:* This algorithm was proposed by Sun for D2D-based V2V communications [6], which uses the KM algorithm for CUE-VUE allocation first with a given power, and then optimizes power allocation with the given CUE-VUE allocation results. A similar idea was used in D2D-based V2V communications in [30]. Its time complexity is $O(Z^4)$.

A. Single CUE-VUE Scenario

To show the impact of VUE transmit SNR threshold in terms of different choices of Eve's detection vectors, we evaluated the secrecy rates in Fig. 6, which shows that the secrecy rates increase with an increasing VUE transmit SNR threshold. Hence, a good strategy to improve secrecy rates is to increase VUE transmit SNR threshold to achieve positive secrecy rates, which is consistent with the approximated power allocation in Section IV. On the other hand, we found that when CUE transmit SNR threshold is high, the ARD and maximum ratio combining (MRC) vectors have a similar performance on the secrecy rates. However, when the CUE transmit SNR threshold is not high enough, for example, $P_m^{sum} = 5$ dB in Fig. 6, Eve's ARD

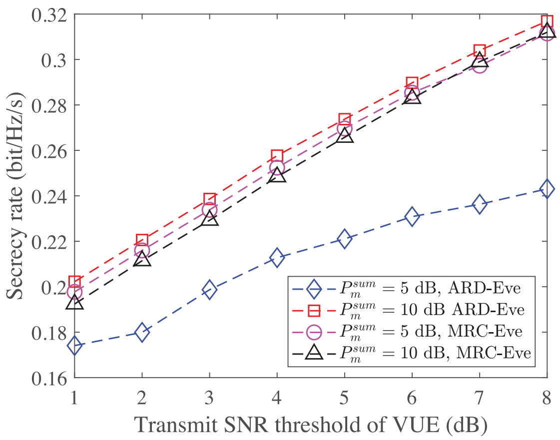


Fig. 6. Optimal secrecy rate of a single CUE-VUE pair with ARD and MRC vectors used by Eve.

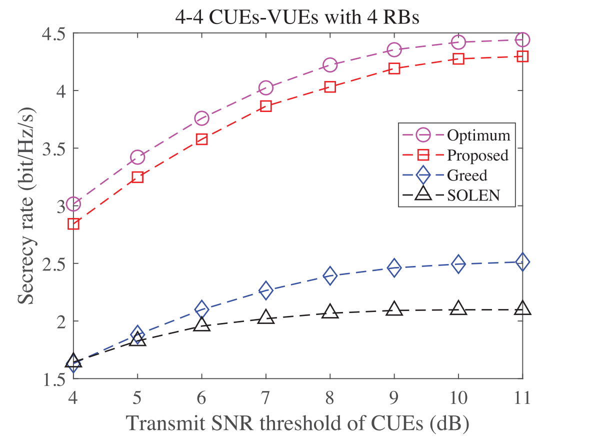


Fig. 8. Optimal sum secrecy rate in multiple CUE-VUE-RB scenarios in terms of CUE transmit SNR, where there are 4 VUEs, 4 CUEs, and 4 RBs.

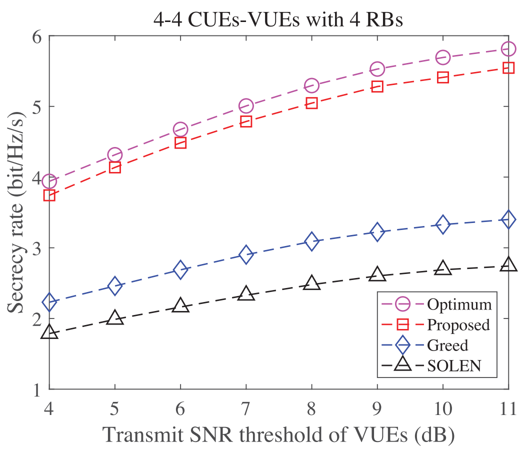


Fig. 7. Optimal sum secrecy rate in multiple CUE-VUE-RB scenarios in terms of VUE transmit SNR, where there are 4 VUEs, 4 CUEs, and 4 RBs.

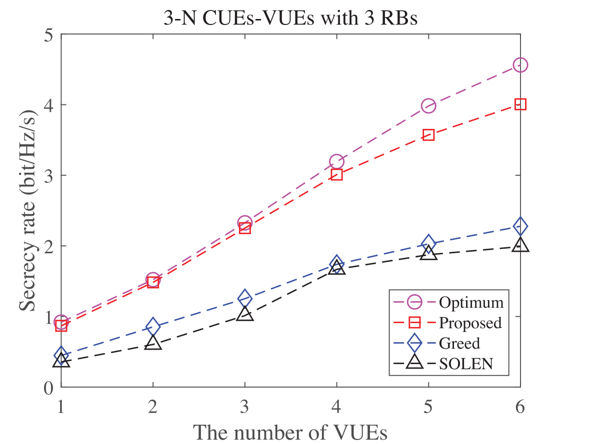


Fig. 9. Optimal sum secrecy rate in terms of the number of VUEs, where there are 3 VUE and 3 RBs.

scheme will degrade the secrecy rates, which is also consistent with the analysis in Section IV. Hence, the consideration of Eve's detection vector is necessary.

B. Multiple CUE-VUE-RB Scenarios

In multiple CUE-VUE-RB scenarios, we assumed that Eve uses an ARD vector.

Sum secrecy rates in terms of VUE transmit SNR threshold are shown in Fig. 7, in which each VUE stays within the coverage of its target VUE. We can see that the sum secrecy rates of VUEs increase with the VUE transmit SNR threshold, which means that VUEs usually transmit total power for secrecy performance improvement, because RB allocation algorithms always assign RBs to VUEs whose main channel gains are larger than the wiretap channels. For evaluation of different schemes, the proposed method achieves a near optimal performance.

The secrecy rates are improved by increasing CUE transmit SNR threshold, as shown in Fig. 8. This is because increasing CUE transmit SNR potentially introduces interference for both VUEs and the eavesdropper in spectrum underlaying D2D. With optimal RB allocation when main channels are better than wiretap channels, CUEs' interference potentially improves secrecy via interfering Eve. It shows that the sum secrecy rate increases slightly when CUEs' SNR is high enough because a higher interference also affects V2V channels. Hence, the power of CUEs should not be set unnecessarily high for power efficiency consideration.

The effect of VUE density on the sum secrecy rates is shown in Fig. 9, which illustrates a common scenario in cellular networks, where the numbers of RBs and CUEs are the same, and vehicles join in the network randomly. Here, the numbers of CUE and RB are set to be three. We can see that the sum secrecy rates increase with the vehicle density, and only three vehicles can obtain their RBs to establish secure channels. More vehicles means more channel allocation choices for a given RB, and RBs will be allocated to these channels that have higher secrecy rates. Hence, with a constrained number of RBs, more vehicles in the network will benefit the sum secrecy performance.

C. Convergence Tests

Finally, we verify the convergence performance of the scheme as proposed in Proposition 2 in Fig. 10, i.e.,

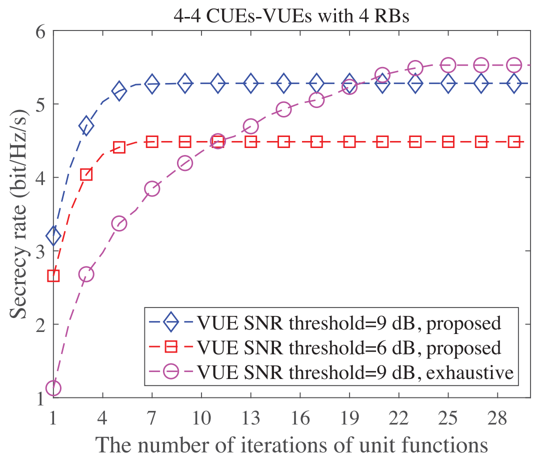


Fig. 10. Convergence test of sum secrecy rates with the number of iterations. In the proposed algorithm, the unit function works in the For Loop in Algorithm 2, 7-14 lines. In exhaustive search, the unit function is a classic maximum value search algorithm for a CUE-VUE-RB combination.

$\sum_{n=1}^{Z}\sum_{m=1}^{Z}\sum_{i=1}^{Z} e_{n,m,i}W_{n,m,i}$ converges as the number of iterations increases. The exhaustive curve shows the performance of an exhaustive search algorithm for a global optimal $\mathbf{E}$, whose number of iterations is $Z!$. In Fig. 10, we have $Z = 4$, such that the exhaustive algorithm needs to search for 4! times. Note that the result of iterative KM algorithm is not optimal.

VI. Conclusions and Future Works

In this article, we investigated resource allocation issues for secrecy rate maximization in cellular underlaying V2V communications. Specifically, we presented a secure and efficient PPRM scheme by granting VUEs the same priority with CUEs to access cellular spectrum. A mixed-integer and non-convex PPRM problem was transformed into a power allocation problem and an RB allocation problem, which have been solved efficiently. The simulations showed that the proposed algorithm can improve secrecy performance by 50% as compared to other schemes, and can achieve near-optimal performance. Moreover, underlay-induced interferences due to a large number of connected vehicles may potentially improve the sum secrecy performance in cellular networks. In the further works, we will study the cases that a multi-antenna based artificial noise technology can be applied to vehicles.

Appendix

A. Proof of Proposition 1

1) Noise-Limited Scenario: According to Eqn. (33), let us introduce an auxiliary function as

$$f(P_{n,i}, P_{m,i}) = \frac{\left(P_{n,i}|h_{n,i}|^2 + P_{m,i}|h_{mn,i}|^2\right)}{\left(P_{n,i}|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2 + P_{m,i}|\mathbf{w}_{ne,i}\mathbf{h}_{me,i}|^2\right)}. \tag{67}$$

The partial derivative functions of $f(P_{n,i}, P_{m,i})$ with respect to $P_{n,i}$ and $P_{m,i}$ are given by

$$\begin{aligned} f_{pn}(P_{n,i}, P_{m,i}) &= \frac{\partial f(P_{n,i}, P_{m,i})}{\partial P_{n,i}} \\ &= \frac{P_{m,i}(|h_{n,i}|^2|\mathbf{w}_{ne,i}\mathbf{h}_{me,i}|^2 - |h_{mn,i}|^2|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2)}{(P_{n,i}|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2 + P_{m,i}|\mathbf{w}_{ne,i}\mathbf{h}_{me,i}|^2)^2}, \end{aligned} \tag{68}$$

$$\begin{aligned} f_{pm}(P_{n,i}, P_{m,i}) &= \frac{\partial f(P_{n,i}, P_{m,i})}{\partial P_{m,i}} \\ &= \frac{P_{n,i}(|h_{mn,i}|^2|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2 - |h_{n,i}|^2|\mathbf{w}_{ne,i}\mathbf{h}_{me,i}|^2)}{(P_{n,i}|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2 + P_{m,i}|\mathbf{w}_{ne,i}\mathbf{h}_{me,i}|^2)^2}. \end{aligned} \tag{69}$$

It is obvious that $f_{pn}(P_{n,i}, P_{m,i}) = 0$ and $f_{pm}(P_{n,i}, P_{m,i}) = 0$ if and only if $|h_{n,i}|^2|\mathbf{w}_{ne,i}\mathbf{h}_{me,i}|^2 = |h_{mn,i}|^2|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2$, which is an unusual condition. Let us check the boundary on Eqn. (32), which is commonly used in power allocation [44]. Since we have $C_{m,BS,i}(P_{m,i}, 1, \mathbf{w}_{mb,i}) = \varepsilon_{m,i}$, we can obtain

$$P_{m,i} = c_i, \tag{70}$$

where

$$c_i = \frac{2^{\varepsilon_{m,i}} - 1}{|\mathbf{w}_{mb,i}\mathbf{h}_{mb,i}|^2}. \tag{71}$$

Substituting Eqn. (70) into Eqn. (67) yields

$$g(P_{n,i}) = \frac{|h_{n,i}|^2 P_{n,i} + |h_{mn,i}|^2 c_i}{|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2 P_{n,i} + |\mathbf{w}_{ne,i}\mathbf{h}_{me,i}|^2 c_i}. \tag{72}$$

The derivative of $g(P_{n,i})$ with respect to $P_{n,i}$ is given by

$$\begin{aligned} g_{pn}(P_{n,i}) &= \frac{\partial g(P_{n,i})}{\partial P_{n,i}} \\ &= \frac{c_i\left(|h_{n,i}|^2|\mathbf{w}_{ne,i}\mathbf{h}_{me,i}|^2 - |h_{mn,i}|^2|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2\right)}{\{|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2 P_{n,i} + |\mathbf{w}_{ne,i}\mathbf{h}_{me,i}|^2 c_i\}^2}. \end{aligned} \tag{73}$$

Then, we can discuss the monotonicity of Eqn. (72) in two cases as follows.

a) If $|h_{n,i}|^2|\mathbf{w}_{ne,i}\mathbf{h}_{me,i}|^2 > |h_{mn,i}|^2|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2$, we have $g_{pn}(P_{n,i}) > 0$, which means that $g(P_{n,i})$ increases monotonously with $P_{n,i}$. Then, we should chose $P^*_{n,i} = P_n^{sum}$ to maximize $g(P_{n,i})$ with

$$P^*_{m,i} = c_i, \tag{74}$$

if $P_m^{sum} > c_i$.

b) If $|h_{n,i}|^2|\mathbf{w}_{ne,i}\mathbf{h}_{me,i}|^2 \le |h_{mn,i}|^2|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2$, we have $g_{pn}(P_{n,i}) \le 0$. We chose $P^*_{n,i} = 0$ to reduce power consumption. In this case, the constraint (32) is also required such that $P^*_{m,i} = c_i$.

2) Interference-Limited Scenario: Next, we prove that in an interference-limited scenario, the optimal solutions of $P_{n,i}$ and $P_{m,i}$ in P2 exist on the boundary of the constraint (32). According to Eqn. (35), we introduce an auxiliary function as

$$f(P_{n,i}) = \frac{1 + P_{n,i}|h_{n,i}|^2}{1 + P_{n,i}|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2}. \tag{75}$$

The partial derivative of $f(P_{n,i})$ with respect to $P_{n,i}$ is given by

$$\frac{\partial f(P_{n,i})}{\partial P_{n,i}} = \frac{|h_{n,i}|^2 - |\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2}{(1 + P_{n,i}|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2)^2}. \tag{76}$$

a) If $|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2 \geq |h_{n,i}|^2$, it is easy to show that the optimal solution is zero with $P^*_{n,i} = 0$, and we get

$$P^*_{m,i} \in [c_i, P^{sum}_m], \tag{77}$$

to satisfy the constraint (32) if $P^{sum}_m > c_i$. Otherwise, we should choose

$$P^*_{m,i} = c_i, \tag{78}$$

to reduce power consumption.

b) If $|\mathbf{w}_{ne,i}\mathbf{h}_{ne,i}|^2 < |h_{n,i}|^2$, we have $\partial f(P_{n,i})/\partial P_{n,i} > 0$. Then, Eqn. (75) is a monotonically increasing function with respect to $P_{n,i}$, and we obtain

$$P^*_{n,i} = P^{sum}_n, \quad P^*_{m,i} = c_i. \tag{79}$$

The proof is completed. ■

B. Proof of Proposition 2

Similar proofs of convergence can be seen in [45, Th. 3], [46, Th. 1], [47, Pr. 3]. Since KM algorithms on $\mathbf{T}_1$, $\mathbf{T}_2$, and $\mathbf{T}_3$ are all convex, we find $\mathbf{b}^1(\text{iter})$, $\mathbf{b}^2(\text{iter})$, and $\mathbf{b}^3(\text{iter})$ are maximal matching for each KM algorithm of the iter-th iteration (iter ≥ 2). We introduce an auxiliary function as

$$f(\mathbf{b}) = \sum_{n=1}^{Z}\sum_{m=1}^{Z} e_{n,m,i}W_{n,m,i}. \tag{80}$$

Then, we have

$$f[\mathbf{b}^3(\text{iter}-1)] \leq \max_{\mathbf{b}^1} f(\mathbf{b}) = f[\mathbf{b}^1(\text{iter})]. \tag{81}$$

Similarly, we have

$$f[\mathbf{b}^1(\text{iter})] \leq \max_{\mathbf{b}^2} f(\mathbf{b}) = f[\mathbf{b}^2(\text{iter})], \tag{82}$$

$$f[\mathbf{b}^2(\text{iter})] \leq \max_{\mathbf{b}^3} f(\mathbf{b}) = f[\mathbf{b}^3(\text{iter})]. \tag{83}$$

Since $\mathbf{E}(\text{iter}) = \mathbf{E}(\text{iter}-1)$, each $\mathbf{E}$ is conducted by $\mathbf{b}^2(\text{iter})$ and $\mathbf{b}^3(\text{iter})$. We have $\mathbf{b}^2(\text{iter}) = \mathbf{b}^2(\text{iter}-1)$ and $\mathbf{b}^3(\text{iter}) = \mathbf{b}^3(\text{iter}-1)$. Combining Eqns. (81) and (82), we have

$$\begin{aligned} &f[\mathbf{b}^2(\text{iter}-1)] = f[\mathbf{b}^3(\text{iter}-1)] \\ &= f[\mathbf{b}^1(\text{iter})] = f[\mathbf{b}^32(\text{iter})] = f[\mathbf{b}^3(\text{iter})]. \end{aligned} \tag{84}$$

The proof is completed. ■

References

[1] Y. Li, Q. Luo, J. Liu, H. Guo, and N. Kato, "TSP security in intelligent and connected vehicles: Challenges and solutions," *IEEE Wireless Commun.*, vol. 26, no. 3, pp. 125–131, Jun. 2019.

[2] N. Cheng *et al.*, "Big data driven vehicular networks," *IEEE Netw.*, vol. 32, no. 6, pp. 160–167, Nov. 2018.

[3] J. Liu, H. Guo, J. Xiong, N. Kato, J. Zhang, and Y. Zhang, "Smart and resilient EV charging in SDN-enhanced vehicular edge computing networks," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 1, pp. 217–228, Jan. 2020.

[4] G. Karagiannis *et al.*, "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 584–616, Oct.–Dec. 2011.

[5] "Study on enhancement of 3GPP support for 5G V2X services (v15.0.0, release 15)," 3GPP, Sophia Antipolis Cedex, France, Tech. Rep. 22.886, Sep. 2017.

[6] W. Sun, E. G. Strm, F. Brnnstrm, K. C. Sou, and Y. Sui, "Radio resource management for D2D-based V2V communication," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6636–6650, Aug. 2016.

[7] N. Cheng *et al.*, "Performance analysis of vehicular device-to-device underlay communication," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 5409–5421, Jun. 2017.

[8] X. Cheng, L. Yang, and X. Shen, "D2D for intelligent transportation systems: A feasibility study," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 4, pp. 1784–1793, Aug. 2015.

[9] H. Nishiyama, T. Ngo, S. Oiyama, and N. Kato, "Relay by smart device: Innovative communications for efficient information sharing among vehicles and pedestrians," *IEEE Veh. Technol. Mag.*, vol. 10, no. 4, pp. 54–62, Dec. 2015.

[10] Q. Wei, W. Sun, B. Bai, L. Wang, E. G. Strm, and M. Song, "Resource allocation for V2X communications: A local search based 3D matching approach," in *Proc. IEEE Int. Conf. Commun.*, May 2017, pp. 1–6.

[11] H. Ye, G. Y. Li, and B. F. Juang, "Deep reinforcement learning based resource allocation for V2V communications," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 3163–3173, Apr. 2019.

[12] F. Lyu *et al.*, "Characterizing urban vehicle-to-vehicle communications for reliable safety applications," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 6, pp. 2586–2602, Jun. 2020.

[13] Q. Luo and J. Liu, "Wireless telematics systems in emerging intelligent and connected vehicles: Threats and solutions," *IEEE Wireless Commun.*, vol. 25, no. 6, pp. 113–119, Dec. 2018.

[14] Y. Xun, J. Liu, and Y. Zhang, "Side-channel analysis for intelligent and connected vehicle security: A new perspective," *IEEE Netw.*, vol. 34, no. 2, pp. 150–157, Mar./Apr. 2020.

[15] Q. Luo, Y. Cao, J. Liu, and A. Benslimane, "Localization and navigation in autonomous driving: Threats and countermeasures," *IEEE Wireless Commun.*, vol. 26, no. 4, pp. 38–45, Aug. 2019.

[16] A. N. Bikos and N. Sklavos, "LTE/SAE security issues on 4G wireless networks," *IEEE Security Privacy*, vol. 11, no. 2, pp. 55–62, Mar. 2013.

[17] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[18] J. Chen *et al.*, "Collaborative trust blockchain based unbiased control transfer mechanism for industrial automation," *IEEE Trans. Ind. Appl.*, to be published, doi: 10.1109/TIA.2019.2959550.

[19] X. Wang *et al.*, "Privacy-preserving content dissemination for vehicular social networks: Challenges and solutions," *IEEE Commun. Surv. Tuts.*, vol. 21, no. 2, pp. 1314–1345, Apr.–Jun. 2019.

[20] Y. Xun, J. Liu, N. Kato, Y. Fang, and Y. Zhang, "Automobile driver fingerprinting: A new machine learning based authentication scheme," *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 1417–1426, Feb. 2020.

[21] S. Han, S. Xu, W. Meng, and C. Li, "Dense-device-enabled cooperative networks for efficient and secure transmission," *IEEE Netw.*, vol. 32, no. 2, pp. 100–106, Mar. 2018.

[22] W. Wang, K. C. Teh, and K. H. Li, "Enhanced physical layer security in D2D spectrum sharing networks," *IEEE Wireless Commun. Lett.*, vol. 6, no. 1, pp. 106–109, Feb. 2017.

[23] J. Wang, Y. Huang, S. Jin, R. Schober, X. You, and C. Zhao, "Resource management for device-to-device communication: A physical layer security perspective," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 946–960, Apr. 2018.

[24] Y. Zhang, Y. Shen, X. Jiang, and S. Kasahara, "Mode selection and spectrum partition for D2D inband communications: A physical layer security perspective," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 623–638, Jan. 2019.

[25] R. Zhang, X. Cheng, and L. Yang, "Cooperation via spectrum sharing for physical layer security in device-to-device communications underlaying cellular networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5651–5663, Aug. 2016.

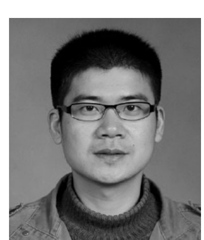
[26] H. Zhang, T. Wang, L. Song, and Z. Han, "Radio resource allocation for physical-layer security in D2D underlay communications," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2014, pp. 2319–2324.

[27] W. Song, Y. Zhao, and W. Zhuang, "Stable device pairing for collaborative data dissemination with device-to-device communications," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1251–1264, Apr. 2018.
[28] L. Wang, H. Wu, Y. Ding, W. Chen, and H. V. Poor, "Hypergraph-based wireless distributed storage optimization for cellular D2D underlays," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 10, pp. 2650–2666, Oct. 2016.
[29] H. Liao *et al.*, "Learning-based context-aware resource allocation for edge computing-empowered industrial IoT," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4260–4277, May 2020.
[30] L. Liang, G. Y. Li, and W. Xu, "Resource allocation for D2D-enabled vehicular communications," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 3186–3197, Jul. 2017.
[31] L. Wang, W. Liu, and Y. Cheng, "Statistical analysis of a mobile-to-mobile Rician fading channel model," *IEEE Trans. Veh. Technol.*, vol. 58, no. 1, pp. 32–38, Jan. 2009.
[32] C. Li, Y. Zhang, T. H. Luan, and Y. Fu, "Building transmission backbone for highway vehicular networks: Framework and analysis," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8709–8722, Sep. 2018.
[33] C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui, and X. Wang, "Interference exploitation in D2D-enabled cellular networks: A secrecy perspective," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 229–242, Jan. 2015.
[34] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[35] S. Han, Y. Zhang, W. Meng, C. Li, and Z. Zhang, "Full-duplex relay-assisted macrocell with millimeter wave backhauls: Framework and prospects," *IEEE Netw.*, vol. 33, no. 5, pp. 190–197, Sep. 2019.
[36] J. F. Sturm, "Using SeDuMi 1.02, a Matlab toolbox for optimization over symmetric cones," *Optim. Method Softw.*, vol. 11, no. 1–4, pp. 625–653, 1999.
[37] P. Xu, "A hybrid global optimization method: The one-dimensional case," *J. Comput. Appl. Math.*, vol. 147, no. 2, pp. 301–314, Oct. 2002.
[38] V. I. Voloshin, *Introduction to Graph and Hypergraph Theory*. Hauppauge, NY, USA: Nova Science, 2009.
[39] R. Duan and H. H. Su, "A scaling algorithm for maximum weight matching in bipartite graphs," in *Proc. 23th Annu. ACM-SIAM Symp. Discrete Algorithms*, Jan. 2012, pp. 1413–1424.
[40] T. L. Marzetta, E. G. Larsson, H. Yang, and H. Q. Ngo, *Fundamentals of Massive MIMO*. Cambridge, U.K.: Cambridge Univ. Press, 2016.
[41] Y. Zhang, C. Li, T. H. Luan, Y. Fu, W. Shi, and L. Zhu, "A mobility-aware vehicular caching scheme in content centric networks: Model and optimization," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 3100–3112, Apr. 2019.
[42] Y. Wang, M. Chen, N. Huang, Z. Yang, and Y. Pan, "Joint power and channel allocation for D2D underlaying cellular networks with Rician fading," *IEEE Commun. Lett.*, vol. 22, no. 12, pp. 2615–2618, Dec. 2018.
[43] D. Feng, L. Lu, Y. Yuan-Wu, G. Y. Li, G. Feng, and S. Li, "Device-to-device communications underlaying cellular networks," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3541–3551, Aug. 2013.
[44] S. Han, Y. Huang, W. Meng, C. Li, N. Xu, and D. Chen, "Optimal power allocation for SCMA downlink systems based on maximum capacity," *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 1480–1489, Feb. 2019.
[45] J. C. Bezdek and R. J. Hathaway, "Convergence of alternating optimization," *Neural, Parallel Scientific Comput.*, vol. 11, no. 4, pp. 351–368, Dec. 2003.
[46] T. Kim and M. Dong, "An iterative Hungarian method to joint relay selection and resource allocation for D2D communications," *IEEE Wireless Commun. Lett.*, vol. 3, no. 6, pp. 625–628, Dec. 2014.
[47] Q. Ye, W. Zhuang, S. Zhang, A. Jin, X. Shen, and X. Li, "Dynamic radio resource slicing for a two-tier heterogeneous wireless network," *IEEE Trans. Veh. Technol.*, vol. 67, no. 10, pp. 9896–9910, Oct. 2018.

Yiliang Liu (Student Member, IEEE) received the B.E. and M.Sc degrees in computer science and communication engineering from Jiangsu University, Zhenjiang, China, in 2012 and 2015, respectively. He is currently working toward the Ph.D. degree in the communication research centre, Harbin Institute of Technology, China. He was a Visiting Research Student with the Department of Engineering Science, National Cheng Kung University, Tainan, Taiwan, from 2014 to 2015. His research interests include security of wireless communications, physical layer security, and intelligent connected vehicles.

Wei Wang (Member, IEEE) received the B.Eng. degree in information countermeasure technology and the M.Eng. degree in signal and information processing from Xidian University, Xi'an, China, in 2011 and 2014, respectively, and the Ph.D. degree in electrical and electronic engineering from Nanyang Technological University (NTU), Singapore, in 2018. From September 2018 to August 2019, he was a Postdoctoral Fellow with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. He is currently a Professor with the Nanjing University of Aeronautics and Astronautics, Nanjing, China. His research interests include wireless communications, space air ground integrated networks, wireless security, and electromagnetic spectrum security. Dr. Wang was awarded the IEEE Student Travel Grants for the IEEE International Conference on Communications in 2017 and the Chinese Government Award for outstanding self-financed students abroad in 2018.

Hsiao-Hwa Chen (Fellow, IEEE) received the B.Sc. and M.Sc. degrees from Zhejiang University, China, and the Ph.D. degree from the University of Oulu, Finland, in 1982, 1985, and 1991, respectively. He is currently a Distinguished Professor with the Department of Engineering Science, National Cheng Kung University, Taiwan. He has authored or coauthored over 400 technical articles in major international journals and conferences, six books, and more than ten book chapters in the areas of communications. He has served as the General Chair, TPC Chair, and Symposium Chair for major international conferences. He is a Fellow of the IET. He is a recipient of the Best Paper Award at the IEEE WCNC 2008 and a recipient of the IEEE 2016 Jack Neubauer Memorial Award. He has served as the Editor-in-Chief of the IEEE WIRELESS COMMUNICATIONS from 2012 to 2015. He was an elected Member-at-Large of the IEEE ComSoc from 2015 to 2016. He has served or is serving as an Editor or a Guest Editor for numerous technical journals. He is the founding Editor-in-Chief of the *Security and Communication Networks Journal* (Wiley).



Liangmin Wang (Member, IEEE) received the B.S. degree in computational mathematics from Jilin University, Changchun, China, in 1999, and the Ph.D. degree in cryptology from Xidian University, Xi'an, China, in 2007. He is a Full Professor with the School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang, China. He has been honored as a "Wan-Jiang Scholar" of Anhui Province since Nov. 2013. Now his research interests include data security & privacy. He has published more than 60 technical papers at premium international journals and conferences, like the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE GLOBAL COMMUNICATIONS CONFERENCE, IEEE WIRELESS COMMUNICATIONS AND NETWORKING CONFERENCE. He has served as a TPC member of many IEEE conferences, such as IEEE ICC, IEEE HPCC, IEEE TrustCOM. Now he is an Associate Editor of Security and Communication Networks, a member of the IEEE, ACM, and a Senior Member of Chinese Computer Federation.

Nan Cheng (Member, IEEE) received the B.E. and M.S. degrees from Tongji University, Shanghai, China, in 2009 and 2012, respectively, and the Ph.D. degree from University of Waterloo in 2016. He worked as a Postdoctoral Fellow with the Department of Electrical and Computer Engineering, University of Toronto, from 2017 to 2019. He is currently a Professor with the State Key Lab of ISN and with School of Telecommunication Engineering, Xidian University, Shaanxi, China. His current research focuses on B5G/6G, space-air-ground integrated network, big data in vehicular networks, and self-driving system. His research interests also include performance analysis, MAC, opportunistic communication, and application of AI for vehicular networks.

Weixiao Meng (Senior Member, IEEE) received the B.Eng., M.Eng., and Ph.D. degrees from the Harbin Institute of Technology (HIT), Harbin, China, in 1990, 1995, and 2000, respectively. From 1998 to 1999, he worked at NTT DoCoMo on adaptive array antenna and dynamic resource allocation for beyond 3G as a Senior Visiting Researcher. He is now a Full Professor and the Vice Dean of the School of Electronics and Information Engineering of HIT. He has published 4 books and over 300 papers on journals and international conferences. He is the Chair of IEEE Communications Society Harbin Chapter, a Fellow of the China Institute of Electronics, a Senior Member of the IEEE ComSoc and the China Institute of Communication. He served in the editorial board of IEEE Communications Surveys and Tutorials from 2014 to 2017 and IEEE Wireless Communications since 2015. In 2005 he was honored provincial excellent returnee and selected into New Century Excellent Talents (NCET) plan by Ministry of Education, China in 2008. Under his leading, Harbin Chapter won IEEE ComSoc Chapter of the Year Award and Asia Pacific Region Chapter Achievement Award, and he won Member & Global Activities Contribution Award in 2018.

Xuemin (Sherman) Shen (Fellow, IEEE) received the Ph.D. degree in electrical engineering from Rutgers University, New Brunswick, NJ, USA, in 1990. He is currently a University Professor with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. He is a registered Professional Engineer of Ontario, Canada, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, a Royal Society of Canada Fellow, a Chinese Academy of Engineering Foreign Fellow, and a Distinguished Lecturer of the IEEE Vehicular Technology Society and Communications Society. Dr. Shen was the recipient of the R.A. Fessenden Award in 2019 from IEEE, Canada, James Evans Avant Garde Award in 2018 from the IEEE Vehicular Technology Society, Joseph LoCicero Award in 2015 and Education Award in 2017 from the IEEE Communications Society. He was also the recipient of the Excellent Graduate Supervision Award in 2006 and Outstanding Performance Award 5 times from the University of Waterloo and the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada. He was the Technical Program Committee Chair/Co-Chair for the IEEE Globecom16, the IEEE Infocom14, the IEEE VTC10 Fall, the IEEE Globecom07, the Symposia Chair for the IEEE ICC10, the Tutorial Chair for the IEEE VTC11 Spring, and the Chair for the IEEE COMMUNICATIONS SOCIETY TECHNICAL COMMITTEE ON WIRELESS COMMUNICATIONS. He is an Editor-in-Chief for the IEEE INTERNET OF THINGS JOURNAL and the Vice President on Publications of the IEEE Communications Society.