Secure Transmission Design for Virtual Antenna Array-Aided Device-to-Device Multicast Communications

Xinyue Hu, Yibo Yi, Student Member, IEEE, Kun Li, Hongwei Zhang, and Caihong Kai, Member, IEEE

Abstract—This paper investigates the physical-layer security in a Virtual Antenna Array (VAA)-aided Device-to-Device Multicast (D2DM) communication system, where the User Equipments (UEs) who cache the common content will form a VAA system and cooperatively multicast the content to UEs who desire it. Specifically, with the target of securing the VAA-aided D2DM communication under the threat of multiple eavesdroppers, we propose a secure beamforming scheme by jointly considering the formed VAA and the Base Station (BS). For obtaining the optimal beamforming vectors, a nonsmooth and nonconvex Weight Sum Rate Maximization Problem (WRMP) is formulated and solved using Successive Convex Approximation (SCA) approach. Furthermore, we consider the worst case that eavesdroppers cooperatively form a eavesdrop VAA to enhance the overhearing capacity. In the capacity analysis, we modify the secure beamforming scheme, formulate the corresponding WRMP and solve it using a two-level optimization. Simulation results validate the improvements of the VAA-aided D2DM scheme in terms of communication security compared with conventional D2DM schemes.

Index Terms—Physical-layer security, virtual antenna array, D2D multicast communication, beamforming.

I. INTRODUCTION

DEVICE-TO-DEVICE Multicast (D2DM) communication which developed from Device-to-Device (D2D) unicast [1] communication has been regarded as one of the key technologies to improve the data rate and alleviate the workload of cellular networks [2], [3]. By allowing one transmitted information bearing signal to be received and decoded by multiple receivers, D2DM could achieve the large-scale parallel implementation of local contents sharing in high-density environments, thus can support massive connectivity and also reduce the redundancy transmission of the Base Station (BS), signaling overhead, and bandwidth waste. Due to the high spectrum utilization and transmission efficiency, D2DM is not only suitable for the data-rate-hungry mobile applications such as online conference, video streaming, mobile computing, and virtual reality, but also considered as a key enabling technique for various future cellular network services such as mobile edge computing (MEC) [4], [5], [6], [7], [8] and fog-radio access network (F-RAN) [9], [10].

Although D2DM has a wide range of applications and there have been many literatures on how to improve its network delivery efficiency [3], [11], [12], [13], [14], [15], on the other hand, communication security is an important indicator to evaluate the performance of a D2DM system. Physical Layer Security (PLS), which is an essential strategy to protect the information by fully utilizing the basic characteristics of the wireless channel and noise, has been regarded as a highly promising security approach for wireless communications. Compared with the cryptography in the higher layer, PLS is independent of the computational complexity and thus more suitable for computation resource limited networks such as D2D communications. Motivated by this, many research efforts have been devoted to secure D2D communication from the physical layer security perspective [16], [17], [18], [19], [20], [21], [22], [23]. Reference [16] attempted to increase the D2D link’s capacity while guaranteeing the security rate by controlling the transmit power of D2D pairs. Reference [17], [18] considered that multiple D2D pairs can access the same resource block and one D2D pair is also permitted to access multiple Resource Blocks (RBs). In [19], aimed to secure CUE’s communication and increase the energy efficiency of D2D communication, the condition of whether D2D link could reuse a CUE’s RB was derived. Ref. [20] investigated both single-channel and multi-channel D2D communications. For providing security to CUEs and improving the spectral efficiency of the D2D links simultaneously, the authors jointly optimized the power allocation and channel assignment of the D2D links and CUEs. In [21], the model selection of a D2D link under the physical-layer security perspective was investigated. The PLS in UAV-enabled D2D communications was investigated in [22] where a UAV plays the role of flying BS. In [23], authors shown that the Non-Orthogonal Multiple Access (NOMA) technique could also be used to secure D2D communications. However, the above literatures are mainly focused on the D2D unicast scenarios. To the best of our knowledge, the PLS schemes in D2DM are rare [24]. The main difference between unicast and multicast [25] is that the data rate in D2DM is limited by the worst Signal to Interference Plus Noise Ratio (SINR) UE and hence leading to a max-

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TWC.2022.3229077.

Digital Object Identifier 10.1109/TWC.2022.3229077

1536-1276 © 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See https://www.ieee.org/publications/rights/index.html for more information.
minimization problem which is hard to deal with. On the other hand, the above secure schemes in D2D communication are mainly based on cooperative jamming, in which the cellular communication signals and other D2D communication signals are utilized to interfere with eavesdroppers for securing intended D2D communications, or vice versa. Constrained by the limited physical size, UEs usually have only one antenna or multiple antennas that are less distant than the coherent distance. Hence, the multiple-antenna based beamforming techniques for providing PLS [26], [27], [28] are not suitable for D2D communications. Thus, how to secure D2D communications is still an open issue and this paper makes attempt to deal with it by introducing the following Virtual Antenna Array (VAA) technique.

Recently, a novel implementation of Multiple-Input-Multiple-Output (MIMO) wireless system called VAA [29], [30], [31] was proposed as a promising approach to further increase the PLS performance and network delivery efficiency of the above D2DM scenario. The VAA system is realized by permitting adjacent single antenna mobile terminals to cooperate among each other and thus form the so called virtual antenna array. In the VAA system, as a virtual transmitter, the elements in VAA could perform cooperative beamforming to transmit information to receivers, while as a virtual receiver, the elements in VAA could exchange the received signals via some short-range communication techniques such as blue tooth and then perform some multiple-antenna receive techniques like maximum ratio combination to increase the SINR. It is important to note that, compared with the Single-Input-Single-Output (SISO) channel, the spatial diversity of VAA together with cooperative beamforming can significantly improve the quality of the transmitted signal and then enhance the PLS performance [32], [33] and channel capacity [31], [34], [35], [36].

In this paper, we propose a VAA-aided D2M (VD2M) scheme for securing D2M communication. In the VD2M, UEs who cache the common contents cooperatively form a VAA system and each UE could be treated as one of the antennas in the VAA. By multiplying the signals each UE sends itself by a beamforming coefficient (i.e., the corresponding element in the beamforming vector), VAA could jointly conduct cooperative beamforming to multicast the common contents to receivers while preventing eavesdroppers from overhearing. Further, unlike the traditional D2D communications which only allow one UE as the transmitter, the VD2M could take full use of the same common contents cached on different UEs. The main contributions of this paper are summarized as follows:

1) We propose a novel secure VD2M transmission scheme, which integrates the VAA into the D2M underlying cellular network. In the proposed scheme, all UEs are equipped with one antenna, and the BS is equipped with multiple antennas. A group of UEs (i.e., D2D receivers) needs a common confidential information data and in the D2D transmitter group, each UE (i.e., D2D transmitters) has cached the common confidential information desired by the D2D receivers. Under the coordination of the BS, D2D transmitters form a VAA, where each UE multiplies the signals by a complex beamforming coefficient to perform cooperative beamforming for multicasting the confidential information to D2D receivers. Meanwhile, a group of baleful UEs (i.e., eavesdroppers) desires to overhear the information delivered by the VAA. Since the VAA transmission reuses the downlink subcarrier resources of a CUE and hence the downlink signal transmitted by the BS could be treated as cooperative jamming to secure VD2M. To further limit the overhearing capacity of eavesdroppers, the BS splits a part of power to transmit an Artificial Noise (AN) to block eavesdroppers.

2) We explore the difference between the VD2M and the traditional D2M unicast, and then formulate the weighted sum rate maximization problem (WRMP) to increase the achievable rate of CUE and the achievable secrecy rate of VD2M simultaneously by jointly optimizing the transmit beamforming of the BS, the cooperative beamforming vector of the VAA and the covariance matrix of AN. The formulated WRMP is non-convex and non-smooth since both max-min and min-max problems are included, i.e., the achievable performance of the multicast group is generally limited by the receiver with the lowest SINR and the secrecy performance is limited by the eavesdropper with the highest SINR. We then introduce a series of auxiliary variables to transfer the non-convex objective function and constraints into a series of convex objective function and constraints. As last, an effective iteration algorithm is designed to solve it.

3) Moving beyond that, we investigate an extreme case (i.e., the worst case) in which the eavesdroppers also form a VAA and gang up together to jointly overhear the communication of VD2M. In our analysis, we treat eavesdroppers as one equivalent multi-antenna eavesdropper called Eve. In this case, with the help of semidefinite relaxation and slack operation, we can decompose the WRMP into a two-level optimization problem, in which the outer level is a single-variable optimization, and the inner level is a non-convex problem which can be recast to a SemiDefinite Problem (SDP) based on Arithmetic Geometry Mean (AGM) inequality.

The remainder of the paper is organized as follows. Section II introduces our considered system model. Section III gives our formulated WRMP problem and the detailed solution to the formulated problem. Section IV extends the considered scenario to the worst case and gives the corresponding solution. Simulation results are shown in Section V and finally Section VI concludes the paper.

Notations: $\mathbb{C}$ and $\mathbb{R}$ denote the sets of complex and real numbers, respectively; $\text{Rank}(\cdot)$, $\text{Tr}(\cdot)$, $|\cdot|^{-1}$, $|\cdot|^T$, and $|\cdot|^H$ denote the rank, trace, inverse, transpose, and conjugate-transpose operations, respectively; $|\cdot|_F$ and $[\cdot, \cdot]^+$ denote the Frobenius norm and the maximum value of its argument, respectively. Except for $e$, bold symbols in capital letter and small letter denote matrices and vectors, respectively and $e$ is the natural constant. $A \succeq 0$ means $A$ is positive
transmitters, manner, meanwhile the VD2DM may be under the risk of eavesdrop attack 
could share the internal information via VD2DM in a timely and convenient 
semidefinite matrix. \(a[n]\) and \(A[n]\) are the \(n^{th}\) element of the vector \(a\) and the \(n^{th}\) element of the diagonal entry of the 
Fig. 1. System scenario of the considered VD2DM, in which exists 
D2D receiver \(n\) who pre-cache the identical confidential information will form 
obtain identical confidential information, and a group of UEs 
lays over the downlink spectrum of a cellular communication 
shares its downlink resource (e.g., subcarriers in OFDMA 
matrix.

II. SYSTEM MODEL AND PRELIMINARY

Consider a VD2DM communication scenario which under- 
over the downlink spectrum of a cellular communication 
A. A group of D2D receivers want to 
pre-cache the identical confidential information and, a group of UEs 
for the downlink resource (e.g., subcarriers in OFDMA 
for the D2D link to reuse. Also, in the system, a group of 
_nodes are equipped with one antenna, and the BS has \(K\) 

Let \(M \triangleq \{1, 2, \ldots, M\}\) denote the set of D2D transmitters, \(N \triangleq \{1, 2, \ldots, N\}\) denote the set of D2D receivers and \(L \triangleq \{1, 2, \ldots, L\}\) denote the set of eavesdroppers. Define \(h_{D,n}\) as the channel vector between D2D transmitters and D2D receiver \(n\), \(h_l\) as the channel vector between D2D transmitters and eavesdropper \(l\), \(h_C\) as the channel vector between D2D transmitters and the CUE, \(h_{B,l}\) as the channel vector between BS and D2D receiver \(n\), \(h_{B,l}\) as the channel vector between BS and D2D receiver \(n\), and \(h_{BC}\) as the channel vector between BS and CUE, respectively. The Rayleigh block-fading channel model is assumed in this paper. The cellular network is considered as a kind of centralized network architecture and the eavesdroppers are also be considered as the registered active user in the cellular network,

\[ y_n = h_{D,n}^H w s_D + h_{B,n}^H w_B s_B + h_{B,n}^H n_B + n_n, n \in N, \]
\[ y_l = h_l^H w s_D + h_{B,l}^H w_B s_B + h_{B,l}^H n_B + n_l, l \in L, \]
\[ y_C = h_{BC}^H w_B s_B + h_{C}^H w s_D + h_{BC}^H n_B + n_c, \]

where \(n_i \sim \mathcal{CN}(0,1), i \in \{N, L, C\}\) is the Additive White Gaussian Noise (AWGN).

From (2), (3) and (4), the channel capacities of D2D receiver \(n\), the eavesdropper \(l\) to overhearing \(s_D\), the eavesdropper \(l\) to decoding \(s_B\) and the CUE are

\[ C_n = \log \left( 1 + \frac{|h_{D,n}^H w|^2}{|h_{B,n}^H w_B|^2 + \text{Tr}(H_{B,n}Q) + 1} \right), \]
\[ C_l = \log \left( 1 + \frac{|h_l^H w|^2}{|h_{B,l}^H w_B|^2 + \text{Tr}(H_{B,l}Q) + 1} \right), \]
\[ C_l = \log \left( 1 + \frac{|h_{BC}^H w_B|^2}{|h_{C}^H w|^2 + \text{Tr}(H_{BC}Q) + 1} \right), \]

\[ 3 \text{For example, in the LTE system, the BS and D2D transmitters could perform channel quality indication estimation from the received sounding reference signal transmitted by eavesdroppers and then obtain } h_C \text{ and } h_l, \text{ respectively. Further, D2D transmitters could periodic or aperiodic report } h_l \text{ to the BS through the physical uplink control channel. Interested readers can read [37] for the details.} \]
respectively, in which $H_{B,n} \triangleq h_{B,n}h_{B,n}^H$, $H_{B,l} \triangleq h_{B,l}h_{B,l}^H$ and $H_{BC} \triangleq h_{BC}h_{BC}^H$.

Let $R_S$ be the achievable secrecy rate of the D2D multicast communication and $R_C$ be the achievable rate of the CUE. Then an achievable rate region is given as the set of nonnegative rate pairs $(R_S, R_C)$ satisfying

$$R_S \leq \min_{n \in N} C_n - \max_{i \in \mathcal{L}} C_l,$$

and

$$R_C \leq C_C,$$

in which $\min_{n \in N} C_n$ means the achievable rate of D2D multicast is determined by the receiver who has the minimum channel capacity. Also, $\max_{i \in \mathcal{L}} C_l$ means the eavesdropping rate is determined by the eavesdropper who has the maximum channel capacity since the confidential information cannot be overheard by any eavesdropper. $C_C$ guarantees that the eavesdroppers could not perform non-orthogonal multiple access (NOMA) to decode and eliminate the interfering signals from the D2D transmitters and the BS.

As can be seen in (5), (6), (7) and (8), the beamforming vector $w_B$, cooperative beamforming vector $w$ and the covariance matrix of AN, $Q$ directly determine the achievable data rates, thus our work focuses on the design of $w_B$, $w$ and $Q$, under an achievable rate region maximization (RRM) formulation with power constraint. The formulated RRM is a vector maximization problem, i.e. (12), in which $\chi$ is an arbitrarily number greater than zero that converts “$>$” to “$\geq$”. In (12), $P_{\text{max}}$ and $P_B$ are the total power budgets of the VAA and the BS, respectively, the constraints $C1$ and $C2$ are the maximal power constraint of each D2D transmitter and the BS, $C3, C4$ and $C5$ are corresponding to (9), (10) and (11), respectively. The RRM problem in (12) is a non-convex vector optimization and thus difficult to solve. In the next section, we elaborate our approaches to tackle (12), shown at the bottom of the page.

III. A TRACTABLE APPROACH TO TACKLE THE RRM PROBLEM (WRMP)

A common approach for dealing with the vector optimization problem (12) is referred to as scalarization, whose basic idea is to transform the vector optimization into the weighted sum maximization optimization. In the rest of this section, we transform the RRM into a WRMP and then deal with it.

A. Weighted Rate Maximization Problem

The target of WRMP is to maximize the total rate including the secrecy rate of D2D multicast communication and the rate of CUE under the total power constraints of both the D2D transmitters and the BS.

Form (5), (6), (7) and (8) we can see that, the transmitted signal vector from the D2D transmitter group, i.e., the VAA, $w_{SD}$, not only could be overheard by eavesdroppers, but also interferes the CUE. Thus, the cooperative beamforming vector $w$ should be carefully designed for securing the D2D multicast communication while limiting the interference to the CUE. On the other hand, the transmitted signal vector from the BS, $w_Bs_B$, could be treated as a cooperative jamming signal to interfere eavesdroppers from overhearing the D2D multicast communication. Thus we need to design the beamforming vector $w_B$ to increase the channel capacity of the CUE whereas decrease the channel capacities of eavesdroppers. Moreover the covariance matrix of the AN, $Q$ also should be jointly designed to secure the communication while does not cause too much interference to other nodes.

$$\begin{align*}
(P1) \quad \max_{w_B, w, Q} \quad & \frac{R_S w_B^H w_B + R_C w^H w}{2} \\
\text{s.t.} \quad & C1 : \|w[m]\|_2^2 \leq P_{\text{max}}/M, m \in \mathcal{M} \\
& C2 : \|w_B\|_2^2 \leq P_B \\
& C3 : \min_{n \in N} \log \left( 1 + \frac{|h_{D,n}^H w_B|^2}{|h_{B,n}^H w_B|^2 + \text{Tr}(H_{B,n}Q) + 1} \right) \\
& \quad - \max_{i \in \mathcal{L}} \log \left( 1 + \frac{|h_{B,i}^H w_B|^2}{|h_{B,i}^H w_B|^2 + \text{Tr}(H_{B,i}Q) + 1} \right) \geq R_S \\
& C4 : \log \left( 1 + \frac{|h_{BC}^H w_B|^2}{|h_{BC}^H w_B|^2 + \text{Tr}(H_{BC}Q) + 1} \right) - R_C \geq 0 \\
& C5 : R_C \geq \log \left( 1 + \frac{|h_{B,l}^H w_B|^2}{|h_{B,l}^H w_B|^2 + \text{Tr}(H_{B,l}Q) + 1} \right) + \chi, l \in \mathcal{L}.\end{align*}$$
Since our aim is to maximize the total rate of the system, we then rewrite (12) into the following WRMP:

$$\begin{align*}
\max_{w, w_B} & \alpha R_S + (1 - \alpha) R_C \\
\text{s.t.} & \ C1, C2, C3, C4, C5.
\end{align*}$$

In (13), $\alpha \in [0, 1]$ is the weighted coefficient, i.e., the larger $\alpha$ corresponds to that we tend to maximize the secrecy rate, vice versa.

**B. Solving (13)**

In the formulated WRMP, (13), although the constraints C1, C2 and the objective function are convex, the constraint C3 includes max-min and min-max structure simultaneously, which is non-convex and non-smoothness. To solve it, we next introduce a series of slack variables to transform it into convex expressions.

First, we introduce two auxiliary variables $\varphi$ and $\beta$ to transform the originally constraint C3 into a smooth form. Specifically, let $R_S = [\varphi - \beta, 0]^T$, (13) can be equivalently recast as (14), shown at the bottom of the page.

In (14), the original non-smooth constraint C3 is decomposed into groups of smooth constraints C6 and C7. However, constraints C6, C7, C4 and C5 are still non-convex and hard to deal with. Next, we respectively process C6, C7, C4 and C5 to transform them into convex constraints.

1) Convex Approximation of C6: Let us introduce a group of auxiliary variables $\{a, b, c, d\}$, then the constraint C6 can be further decomposed into the following constraints:

- C8 : $\log (1 + a) \geq \varphi \Rightarrow 1 + a \geq e^\varphi$
- C9 : $b^2 \geq a$
- C10 : $d \geq b^2$
- C11 : $\|h_{B,n}^H w\|^2 \geq d, \forall n \in \mathcal{N}$
- C12 : $c \geq \|h_{B,n}^H w_B\|^2 + \text{Tr} (H_{B,n} Q) + 1, \forall n \in \mathcal{N}$. (15)

Now, C6 has been decomposed into a series of constraints. However, although C8, C10 and C12 are convex, they are not in the simplest form. Also, C9 and C11 are still non-convex.

Let us first check C8, it is an exponential cone constraint and can be solved by existing nonlinear solvers (e.g., SDPT3 in CVX). To further reduce the computational complexity, C8 can be approximated in terms of a series of second order conic (SOC) constraints. Let $q \triangleq [q_1, q_2, \ldots, q_{U+4}]^T$ be the introduced slack variables, C8 can be approximatively rewritten as

$$C8' : \begin{cases}
1 + a \geq q_{n,U+4} \\
1 + q_{U+4} \geq \|1 - q_{U+4}, 2q_{U+3}\|_2 \\
1 + q_i \geq \|1 - q_i, 2q_{i-1}\|_2, i = 5, \ldots, U + 3 \\
q_i \geq 19/72 + q_2 + q_3/24 \\
1 + q_5 \geq \|1 - q_3, 2q_{12}\|_2 \\
1 + q_2 \geq \|1 - q_5, 3 + \varphi/2U\|_2 \\
1 + q_1 \geq \|1 - q_1, 2 + \varphi/2U^2\|_2 \\
\end{cases}$$

in which $U + 4$ is the number of a series auxiliary variable $q$, and the approximate accuracy increases as $U + 4$ increases.

It is easy to see that constraints C10 and C12 can be directly transformed to SOC forms as

$$C10' : \frac{d + 1}{2} \geq \|b, d - 1\|_2, \forall n \in \mathcal{N}, \tag{17}$$

and

$$C12' : \frac{1}{\varphi} e^{-\text{Tr}(H_{B,n} Q)} \geq \|\left[h_{B,n}^H w_B, \frac{1}{\varphi} e^{-\text{Tr}(H_{B,n} Q)}\right]_2, \forall n \in \mathcal{N}, \tag{18}$$

respectively. We next deal with C9. Based on the fact that the first-order Taylor expansion of a convex function is its lower bound, we employ the first-order Taylor series expansion of the left hand side of C9 around $b^0$ and $c^0$, i.e.,

$$\frac{b^2}{c} \geq 2 \left(\frac{b^0}{c^0}\right) b - \left(\frac{b^0}{c^0}\right)^2 c. \tag{19}$$

Then, C9 can be recast to

$$C9' : 2 \left(\frac{b^0}{c^0}\right) b - \left(\frac{b^0}{c^0}\right)^2 c \geq a. \tag{20}$$

---

$^{(1)}$The $[\bullet, \bullet]^+$ operator ensures that $R_S$ is not less than zero, however for guaranteeing that the objective function of (14) is linear, the $[\bullet, \bullet]^+$ operator is omitted and when $\varphi - \beta < 0$, $R_S$ is set to zero.

---

(P2) $\begin{align*}
\max_{w, w_B, Q \succeq 0, \varphi, \beta, R_C} & \alpha (\varphi - \beta) + (1 - \alpha) R_C \\
\text{s.t.} & \ C1, C2, C4, C5 \\
C6 : & \log \left(1 + \frac{\|h_{B,n}^H w\|^2}{\|h_{B,n}^H w_B\|^2 + \text{Tr} (H_{B,n} Q) + 1}\right) - \varphi \geq 0, \forall n \in \mathcal{N} \\
C7 : & \beta - \log \left(1 + \frac{\|h_{B,n}^H w\|^2}{\|h_{B,l}^H w_B\|^2 + \text{Tr} (H_{B,l} Q) + 1}\right) \geq 0, \forall l \in \mathcal{L}. \tag{14}
\end{align*}$
Note that, in C9, we use the lower bound of the left hand side of C8 to instead itself, thus the feasible region of C9 must be the subset of C9.

Let $H_{D,n} \triangleq h_{D,n} h_{D,n}^H$, the left hand side of C11 can be written to $w^H H_{D,n} w$, which is a semipositive definite quadratic form in complex domain. Following [38], we define $g(w,w^H) = w^H H_{D,n} w$, according to eq.(15) in [38], giving a differential of $w$, $\delta w$, we have

$$
\delta g = (\nabla_w g)^T \delta w + (\nabla_{w^H} g)^T \delta w^* = 2 \text{Re} \left( (\nabla_w g)^H \delta w \right),
$$

(21)
in which $\nabla_w g$ and $\nabla_{w^H} g$ are the generalized complex gradient and the conjugate complex gradient of $g(w,w^H)$ defined in [38], respectively.

With the help of two types of gradients, it is easy to calculate that

$$
\nabla_{w^H} g = H_{D,n} w.
$$

(22)

Hence the first-order Taylor series expansion of the left hand side of C11 around $w^0$ is

$$
w^0 H_{D,n} w^0 + 2 \text{Re} \left( w^0 H_{D,n} (w-w^0) \right)
= 2 \text{Re} \left( w^0 H_{D,n} w \right) - w^0 H_{D,n} w^0,
$$

(23)

and then C11 can be approximated as

$$
\text{C11}' : 2 \text{Re} \left( w^0 H_{D,n} w \right) - w^0 H_{D,n} w^0 \geq d, \forall n \in N.
$$

(24)

Thus far, the non-convex constraint C6 has been decomposed to a series of convex constraints.

2) Convex Approximation of C7: By introducing another group of auxiliary variable $\{e,f\}$, C7 can be decomposed into the following constraints:

$$
\text{C13} : \beta - \log(1+e) \geq 0
$$

$$
\text{C14} : e \geq \frac{|h^H_l w|^2}{f}, \forall l \in L
$$

$$
\text{C15} : |h^H_l w|^2 + \text{Tr} (H_{B,l} Q) + 1 \geq f, \forall l \in L.
$$

(25)

In (25), C13 and C15 are still non-convex and C14 can be rewritten to SOC form directly:

$$
\text{C14}' : \frac{e+f}{2} \geq \left\| \left[ e - \frac{f}{2}, |h^H_l w| \right]^T \right\|_2, \forall l \in L.
$$

(26)

By preforming the first-order Taylor series expansion, C13 and C15 can be approximated as

$$
\text{C13}' : \beta - \log(1+e^0) - \frac{1}{1+e^0} (e-e^0) \geq 0,
$$

(27)

and

$$
\text{C15}' : 2 \text{Re} \left( w^0 B_{B,l} H_{B,l} w_B \right)
- w^0 B_{B,l} H_{B,l} w_B^0 + \text{Tr} (H_{B,l} Q) + 1 \geq f, \forall l \in L.
$$

(28)

respectively. With the series of constraints C13', C14' and C15', C7 has been approximated to a convex constraint.

3) Convex Approximation of C4 and C5: Note that C4 and C6 have the similar formation, thus with the same approach of C6 above, C4 could be approximated to the following constraints C16, C17, C18, C19 and C20 corresponding to C8', C9', C10', C11' and C13', respectively.

Similarly, C5 could be approximated to C21, C22 and C23 with the same approach of C7 above. For briefly, we have omitted the details of constraints C16–C23.

Now, all non-convex constraints have been approximated to convex constraints, the approximated version of WRMP is given by

$$
\begin{align*}
\max_{c, d, e, f, \alpha} & \alpha (\varphi - \beta) + (1 - \alpha) R_C \\
\text{s.t.} & \text{C1}, \text{C2}, \text{C8}', \text{C9}', \text{C10}', \text{C11}', \text{C12}' , \\
& \text{C13}', \text{C14}', \text{C15}', \text{C16}, \text{C17}, \text{C18}, \text{C19}, \\
& \text{C20}, \text{C21}, \text{C22}, \text{C23}.
\end{align*}
$$

(29)

Note that, for briefly, the auxiliary variables for approximating C4 and C5 are omitted in P3. It easy to see that P3 is a convex problem, which can be efficiently solved by using interior point methods, or standard convex optimization tool, e.g., CVX. The detailed procedure is summarized in Algorithm 1.

Algorithm 1 Solving the WRMP in (13)

1. Initialization:
   • Setting the initial values $b^0, c^0, e^0, w^0$ and $w_B^0$,
   • Setting maximum number of iterations $J_{\text{max}}$ iteration counter $j = 1$ and iteration termination accuracy $\psi > 0$.
2. Repeat:
   3. Solving the WRMP with current $b^0, c^0, e^0, w^0, w_B^0$ and obtaining the optimal $b^*, c^*, e^*, w^*, w_B^*$.
   4. if $\|w^*-w^0\|_2 + \|w_B-w_B^0\|_2 \leq \psi$ then
      5. The optimal solutions of WRMP are $w^*$ and $w_B^*$.
   6. Break
   7. else
      8. Setting $b^0 = b^*, c^0 = c^*, e^0 = e^*, w^0 = w^*$ and $w_B^0 = w_B^*$.
   9. end if
10. $j = j + 1$
11. Until $j > J_{\text{max}}$

**Complexity and convergence:** The complexity of interior point method for solving a convex optimization problem (i.e., line 3 in Algorithm 1) is $O \left( \sigma^{0.5}(\sigma + \varsigma)^2 \right)$ [39], in which $\sigma = 2U + N + 4L + 19$ is the number of inequality constraints and $\varsigma = 2K + 4M + 2U + 24$ is the number of optimization variables. Combining with the fact that the iterative number of Algorithm 1 is bounded by $J_{\text{max}}$, we have the total computational complexity of Algorithm 1 is $O \left( J_{\text{max}}^{0.5}(\sigma + \varsigma)^2 \right)$.

The convergence of Algorithm 1 could refer to Proposition 2 in [1].

**Remark 1:** Our formulated WRMP in both the normal case and the worst case does not include the quality of service (QoS) ensuring constraints that limit the achievable rate of CUE and the achievable secrecy rate of D2DM at least to a certain value, that is because the QoS constraints may lead to the WRMP being unsolvable. In practice, if the achievable secrecy rate of the solution, $R_S$ is too small, we could increase $\alpha$ appropriately, vice versa.
IV. EXTENSION TO THE WORST CASE

In Section III above, we only considered the scenario in which multiple eavesdroppers overhear the confidential information independently. However, in the worst case that the eavesdroppers may collude and form another VAA to jointly process the eavesdropped information (such as maximum ratio combination and MMSE receiver) to increase the overhearing capacity. We next make efforts to investigate the PLS scheme in such a scenario.

Since the eavesdroppers are ganged up together and form an eavesdropping VAA, the group of eavesdroppers i.e., the eavesdropping VAA could be treated as a virtual multi-antenna eavesdropper which is equipped with L antennas. In the rest of this paper, unless particularly stated, we use Eve to represent the so-called eavesdropping VAA, i.e., the equivalent L-antenna eavesdropper.

Since the eavesdroppers form the eavesdropping VAA, the channel vector from the D2D transmitter group to the $l^{th}$ eavesdropper, $h_l$ could be treated as the channel vector from the D2D transmitter group to the $l^{th}$ antenna of Eve. We use $G_E = [h_1, h_2, \ldots, h_L]$ represent the channel matrix between D2D transmitter group and Eve. Similarly, we use $G_B = [h_B, h_{B,2}, \ldots, h_{B,L}]$ represent the channel matrix between BS and Eve. Then the received signals of D2D receiver $n$, Eve and CUE can be expressed as

$$y_n = h_{D,n}^H w s_D + h_{B,n}^H w_B s_B + n_B + n_n, n \in \mathcal{N},$$

$$y_E = G_E^H w s_D + G_B^H w_B s_B + G_B^H n_B + n_E,$$

and

$$y_C = h_{BC}^H w_B s_B + h_{BC}^H n_B + h_{BC}^H w s_D + n_C,$$

respectively, where $n_E \sim CN(0, I_L)$ is the AWGN vector at Eve. Similar with the normal case, from (30), (31) and (32), we can write the eavesdropped channel has transformed from MISO to MIMO, and the corresponding channel capacity becomes (34) and (35).

The achievable rate region is then defined as the set of nonnegative rate pairs $(R_S^{worst}, R_C^{worst})$ satisfying

$$R_S^{worst} \leq \min_{n \in \mathcal{N}} C_n^{worst} - C_E^{worst},$$

and

$$C_E^{worst} < R_C^{worst}.$$  

In the worst case, to reduce computational complexity, we discuss the WRMP in two subcases and formulate corresponding optimization problems. Note that, different from the WRMP in the normal case which includes constraints C5 to guarantee that the eavesdroppers could not perform NOMA to decode and eliminate the $s_B$ first. In both subcases, we do not consider (39) into the optimization problems, the detailed reasons please see Remark 3 at last of this section.

In subcase 1, we consider that Eve could not decode and eliminate the $s_B$ first and formulate the corresponding sub-WRMP, P4_1. On the contrary, in subcase 2, we consider that Eve could decode and eliminate the $s_B$ first and formulate the corresponding sub-WRMP, P4_2.

We first consider subcase 1 and formulate the following P4_1 to maximize the weighted sum of $R_S^{worst}$ and $R_C^{worst}$ (40), shown at the bottom of the next page, where $R_S^{worst} = \varphi^{worst} - \beta^{worst}$ and $\alpha$ is the weighted coefficient. $C'_4, C'_6$ and $C'_7$ are evolved from $C_4, C_6$ and $C_7$ in (14) respectively, because of the different expressions of the channel capacity of CUE, D2D receivers and Eve.

Note that, P4_2 is basically the same as P4_1, by replacing $C'_7$ with

$$C'_7 = \varphi^{worst} - \log \left( \det \left( I_L + G_E^H w_B w_B H_E G_E \right) \right) \geq 0.$$  

P4_2 can be obtained. In $C'_7$, only the AN could interfere with Eve since Eve could decode and eliminate $s_B$ first.

We first make effort to solve P4_1, it is easy to see that $C'_4$ and $C'_6$ have the same structure as $C_4$ and $C_6$, respectively, and the technique used to transform $C_4$ and $C_6$ to series of convex constraints in Section III.B could still be used to deal with $C'_4$ and $C'_6$. However, due to the determinant operation, $C'_7$ in (40) is a non-convex constraint and non-trivial to deal with.

A. A Semidefinite Relaxation Based Approach for Handling $C'_7$

Observing that, $x^H R x = \text{Tr} \left( R xx^H \right)$, when $x$ is a complex vector and $R$ is Hermitian, to handle problem (40),
we define $W_B \triangleq w_B h_B^H$, $W \triangleq w w^H$ and ignore the non-convex constraints $\text{Rank}(W) \leq 1$, $\text{Rank}(W_B) \leq 1$ to obtain a relaxed problem version of (40) as follow (42), shown at the bottom of the page.

In (42), $C_7''$ is still hard to handle. Before we deal with it, we first introduce the following lemma whose proof can be found in [40]:

**Lemma 1:**

$$C_7'' \Rightarrow C_{24} : \left(e^{\beta_{\text{worse}} - 1}\right) \left(G_B^H W_B G_B + G_B^H Q G_B + I_L\right) - G_E^H W G_E \geq 0.$$  \hfill (43)

For any $G_E \in M \times L$, $G_B \in K \times L$, $W_B \geq 0$, $W \geq 0$ and $Q \succeq 0$. Furthermore, the equivalence in (43) holds if $\text{Rank}(W) \leq 1$.

Replacing $C_7''$ with $C_{24}$, (42) becomes:

$$(P6) \max_{\beta_{\text{worse}}, R_C^{\text{worse}}, \alpha, \mathbf{w}, \mathbf{Q}, \mathbf{g}, \mathbf{r}} \alpha \left(\varphi_{\text{worse}} - \beta_{\text{worse}}\right) + (1 - \alpha) R_C^{\text{worse}} \quad \text{s.t.} \quad C1', C2', C4', C6', C24.$$  \hfill (44)

$^6$When the optimal solution $\{\mathbf{W}^*, \mathbf{W}_B^*\}$ to (45) satisfies $\text{Rank}(\mathbf{W}) \leq 1$, $\text{Rank}(\mathbf{W}_B) \leq 1$, the corresponding maximum weight sum rate could be obtained via single-stream transmit beamforming, which facilitates the implementation of physically realizable transceiver with low complexity. However the Rank constrains is non-convex and hard to deal with, here we omit them and will discuss it in Section IV-D.

It is obvious that when $\beta_{\text{worse}}$ is fixed, $C_{24}$ becomes a linear matrix inequality which is a convex constraint. Hence (44) could be deposed into a two-level optimization: the inner-level optimization is convex with a fixed $\beta_{\text{worse}}$, and the outer-level is a single-variable optimization with respect to $\beta_{\text{worse}}$.

**B. The Inner-Level Optimization**

With a fixed $\beta_{\text{worse}}$, the inner-level optimization can be written as

$$(P7) \max_{\beta_{\text{worse}}, R_C^{\text{worse}}, \alpha, \mathbf{w}, \mathbf{Q}, \mathbf{g}, \mathbf{r}} \alpha \left(\varphi_{\text{worse}} - \beta_{\text{worse}}\right) + (1 - \alpha) R_C^{\text{worse}} \quad \text{s.t.} \quad C1', C2', C4', C6', C24.$$  \hfill (45)

In (45), although $C1'$, $C2'$ and $C24$ are convex constraints, we still need to deal with the non-convex constraints $C4'$ and $C6'$. Note that, the convex approximation approach in Section III.B could be used to transfer $C4'$ and $C6'$ into convex form. However, observing that the expressions inside the logarithm of $C4'$ and $C6'$ are in the form of linear function, hence, in the following, we give an easier approach that does not need complex domain Taylor expansion.

**1) Convex Approximation of $C4'$:** By introducing auxiliary variable $r_{\text{worse}}$, $C4'$ can be decomposed into

$$C_{25} : \log (1 + r_{\text{worse}}) \geq R_C^{\text{worse}} \Leftrightarrow 1 + r_{\text{worse}} \geq e^{R_C^{\text{worse}}},$$  \hfill (46)

**2) Convex Approximation of $C6'$:**

$$\text{max}_{\mathbf{g}, \mathbf{r}} \alpha \left(\varphi_{\text{worse}} - \beta_{\text{worse}}\right) + (1 - \alpha) R_C^{\text{worse}} \quad \text{s.t.} \quad C1', C2', C4', C6', C24.$$  \hfill (47)

In (47), although $C1'$, $C2'$ and $C24$ are convex constraints, we still need to deal with the non-convex constraints $C4'$ and $C6'$. Note that, the convex approximation approach in Section III.B could be used to transfer $C4'$ and $C6'$ into convex form. However, observing that the expressions inside the logarithm of $C4'$ and $C6'$ are in the form of linear function, hence, in the following, we give an easier approach that does not need complex domain Taylor expansion.
and
\[
C26 : \frac{\text{Tr} (H_{BC} W_B)}{\text{Tr} (QH_{BC}) + \text{Tr} (H_C W) + 1} \geq r_{\text{w}}
\]
\[
\Leftrightarrow \text{Tr} (H_{BC} W_B) \geq r_{\text{w}} (\text{Tr} (QH_{BC}) + \text{Tr} (H_C W) + 1).
\]
\[(47)\]

Like C8 in (15), C25 is an exponential cone constraint and can be approximated in terms of a series of SOC constraints with the same formation of C8. For brevity, we denote the series of SOC constraints derived from C25 by C25′ and omitting its detailed expression.

Then, arithmetic geometry mean (AGM) inequality is applied to get an approximation of the non-convex constraint, i.e., C26. We first introduce the AGM inequality. The AGM applied to get an approximation of the non-convex constraint, expression of it. With the help of AGM inequality, C28 can be recast into solving a sequence of convex optimization subproblem

\[
\text{max} \ (1 + a_{\text{w}}) \geq \varphi_{\text{w}} \Leftrightarrow 1 + a_{\text{w}} \geq e^{r_{\text{w}}},
\]
\[(49)\]

and
\[
C28 : \frac{\text{Tr} (H_{D,n} W)}{\text{Tr} (H_{B,n} W_B) + \text{Tr} (QH_{B,n}) + 1} \geq a_{\text{w}} \Leftrightarrow \text{Tr} (H_{D,n} W) \geq a_{\text{w}} (\text{Tr} (H_{B,n} W_B) + \text{Tr} (QH_{B,n}) + 1), \forall n \in N.
\]
\[(50)\]

Similar with how we process C25, C27 is replaced by a series of SOC constraints, i.e., C27′ and we omit the detailed expression of it. With the help of AGM inequality, C28 can also be approximated to a convex constraint:
\[
\text{C28} : \text{Tr} (H_{D,n} W) \geq \frac{1}{2} \left( \frac{\eta_n a_{\text{w}}}{\eta_n} \right)^2 + \frac{1}{2} \left( \frac{\text{Tr} (H_{B,n} W_B) + \text{Tr} (QH_{B,n}) + 1}{\eta_n} \right)^2, \forall n \in N.
\]
\[(51)\]

Now, with the help of C25′, C26′, C27′ and C28′, (45) can be recast into solving a sequence of convex optimization subproblem:
\[
\text{max} \ W \geq 0, W_B \geq 0, Q \geq 0, a \geq 0, r_{\text{w}} \geq 0,
\]
\[
al (\varphi_{\text{w}} - \beta_{\text{w}}) + (1 - a) R_{C_{\text{w}}}
\]
\[
s.t. C1', C2', C4, C25', C26', C27', C28'.
\]
\[(52)\]

Now, (52) is a semidefinite program (SDP) which is convex and can be solved by using interior point methods, or standard convex optimization tool, e.g., CVX. The detailed procedure is summarized in Algorithm 2.

**Algorithm 2 Solving (40)**

1. **Initialization:**
   - Setting the initial values $W^0$, $W_B^0$, $Q^0$, $\eta_0$ and $\eta_n$, $n \in N$.
   - Setting maximum number of iterations $j_{\text{max}}$, iteration counter $j = 1$ and iteration termination accuracy $\psi > 0$.
2. **Repeat**
3. **Solving (52) with current $\eta_0$, $\eta_n$, $n \in N$ and obtaining the optimal $W^*$, $W_B^*$ and $Q^*$.
4. If $\|W^* - W^0\|_2 + \|W_B^* - W_B^0\|_2 + \|Q^* - Q^0\|_2 \leq \psi$, then
5. The optimal solutions of (56) are $W^*$, $W_B^*$ and $Q^*$.
6. **Break**
7. **else**
8. Setting $\eta_0 = \sqrt{\text{Tr} (QH_{BC}) + \text{Tr} (H_C W) + 1}$, $\eta_n = \sqrt{\text{Tr} (H_{B,n} W_B) + \text{Tr} (QH_{B,n}) + 1}$, $\forall n \in N$, $W^0 = W^*$, $W_B^0 = W_B^*$ and $Q^0 = Q^*$.
9. **end if**
10. $j = j + 1$
11. **Until** $j > j_{\text{max}}$

**C. The Outer-Level Optimization**

The outer-level is a single-variable optimization with respect to $\beta_{\text{w}}$. Let $Y (\beta_{\text{w}})$ be the optimized value of (52) with a given $\beta_{\text{w}}$, then the outer-level optimization is $\max Y (\beta_{\text{w}})$. Note that

\[
0 \leq \beta_{\text{w}} \leq \min_{n \in N} \log \left( \frac{1 + \text{Tr} (H_{D,n} W)}{\text{Tr} (H_{B,n} W_B) + \text{Tr} (QH_{B,n}) + 1} \right) \leq \min_{n \in N} \log \left( 1 + \text{Tr} (H_{D,n} W) \right) \leq \min_{n \in N} \left( 1 + M P_{\text{max}} \right) \left( h_{D,n} \right)_{\text{L}}^2.
\]
\[(53)\]

where the first inequality is due to the non-negative property of rate, the second inequality is because the secrecy rate is non-negative, and the last inequality comes from the fact that $\text{Tr} (H_{D,n} W) \leq \text{Tr} (W) \left( h_{D,n} \right)_{\text{L}}^2$ for any $W \geq 0$ and $W[m] \leq P_{\text{max}}$. From (53), we can see that the optimization variable of the outer-level optimization has a bounded interval, and then we use one-dimensional search technology to solve the outer-level optimization.

So far, we have solved P4.1, the approach to overcome P4.2 is similar to that of P4.1, except for replacing $C7'$ with $C7''$ and we omit the details here.

The whole process of solving the WRMP in the worst case is that, we first solve the P4.1 and test whether (39) is satisfied. If (39) is satisfied, the solution of P4.1 is the solution of the WRMP in the worst case, otherwise, we solve P4.2 and set the solution of it as the solution of the WRMP in the worst case.
Remark 2: In our thousands of simulations results, the solution of (13) makes constraints C5 equal and the solution of $P_{4_1}$ does not satisfy (39) never happen, which means eavesdroppers can not decode $s_B$ with large probability, even if we do not deliberately set constraints to ensure this. In other words, the constraint C5 in (13) and $P_{4_2}$ are redundant in most cases.

Remark 3: The reason why we do not consider (39) into the WRMP in the worst case is because (39) and $C_7'$ have the same structure, for overcoming $C_7'$, we deploy one-dimensional search technology, which means for jointly solving (39) and $C_7'$ a time-consuming two-dimensional search technology should be used. Also, as stated in remark 2, even if we omit (39), the solution of $P_{4_1}$ still satisfies (39) with a large probability.

D. Rank-Profile Analysis

Note that, when the optimal solution $\left(W^*, W_{B}^*\right)$ of (44) satisfies $\text{Rank}(W^*) \leq 1$ and $\text{Rank}(W_{B}^*) \leq 1$ the corresponding weighted maximum rate, i.e., $\alpha \beta \log^2(\text{Tr}(H_{B,n}^*) + (1 - \alpha) R_{\text{worst}}^C)$ could be attained via single-stream transmit beamforming, which facilitates the implementation of physically realizable transceiver with low complexity. Also the beamforming, which facilitates the implementation of physically realizable transceiver with low complexity. Also the beamforming, which facilitates the implementation of physically realizable transceiver with low complexity.

Condition $\text{Rank}(W^*) \leq 1$ guarantees the relaxation from $C_7''$ to C24 is tight, i.e., C24 equivalent to $C_7''$ and (44) equivalent to (40). However, the rank constraint is non-convex does not always lead to the optimal solution of the original problem (40). Apparently, if $W^* (W_{B}^*)$ is of rank one, then via eigenvalue decomposition, the optimal $w^* (w_{B}^*)$ of (40) can be easily obtained. Otherwise, some rank-one approximation procedures for $W^* (W_{B}^*)$ such as Gaussian randomization [41] are applied to obtain a suboptimal solution of (40).

The investigation on rank properties of $W^*, W_{B}^*$ and $Q^*$ is still an open issue. However, thanksfully, we can prove that the rank one property holds for $W^*$ in a special case.

**Proposition 1:** If there exist only one $\forall n \in \mathcal{N}$ satisfies

$$
\log \left(1 + \frac{\text{Tr}(H_{B,n}^*W^*)}{\text{Tr}(H_{B,n}^*W_{B}^*) + \text{Tr}(QH_{B,n}^*) + 1}\right) - \phi \text{worst} = 0, \text{then } W^* \text{ must be of rank one.}
$$

**Proof:** Please see Appendix A.

It is worth noting that, for D2D receivers it is almost impossible that, $C_n = C_m, n, m \in \mathcal{N}, n \neq m$ with similar $(W^*, W_{B}^*, Q^*)$, since the channel conditions of each receiver are independent with each other, which implies that $\text{Rank}(W^*) = 1$ holds with large probability. In fact, in our thousands of simulations results, $\text{Rank}(W^*) > 1$ never happens.

V. SIMULATION RESULTS

This section presents simulation results to validate the performance of our proposed algorithms. The transmit powers are normalized with AWGN power $N_0 = 1$. That is, the transmit power $P$ dB means the transmit power is $10^{P/10}$ times higher than the AWGN power. All channels are considered to be independent quasi-static block Rayleigh fading with

\[CN(0,1).\]

The simulation results are collected from Monte Carlo simulations with 100 independent channel realizations. The suboptimal solutions are based on zero forcing and generalized singular value decomposition, the details please refer to [42].

We first present the impact of the number of the D2D transmitter on the achievable rate. In Fig. 2, the number of eavesdroppers, $L$ is set to zero which corresponds to the normal D2DM communication scenario without the threat of eavesdroppers. Fig. 2 shows that, when $M = 1$, D2DM can achieve only a certain rate through the power control of the transmitter and the BS. While when $M > 1$, the rate of VD2DM increases dramatically, that is because multiple D2D transmitters can form a VAA and play cooperative beamforming to focus the signal on the D2D receiver who has the worst channel conditions. We note that the number of D2D transmitter $M = 1$ represents the traditional D2DM without the assistance of VAA, hence the results demonstrate that the VAA-aided communication can significantly improve the efficiency of D2D multicast communication compare to the traditional D2DM.

We then show the secrecy rate obtained via the aid of VAA under the threat of multiple eavesdroppers. In Fig. 3, when $M = 1$, D2DM can achieve a tiny secrecy rate by relying on the cooperative interference of the BS. However, when $M > 1$, the secrecy rate of VD2DM increases dramatically, because the multiple D2D transmitters form a VAA and play cooperative beamforming to focus the signal on the D2D receivers while preventing the eavesdroppers to overhear. Similar to Fig. 2, the number of D2D transmitter $M = 1$ represents the traditional secrecy D2DM communication without the help of VAA, hence the results in Fig. 3 validate the secrecy improvement brought by VAA.

We next present the achievable secrecy rate of VD2DM with respect to different maximum transmit power of D2D transmitter group. As can be seen in Fig. 4, the achievable secrecy rate of VD2DM monotonously increases with the increase of the maximum transmit power of D2D transmitter group. Also, a larger $\alpha$ will lead to a larger achievable secrecy rate.

\[7\text{We do not consider the specific distribution of each node, and set all channels are rayleigh distribution to reflect the randomness distribution of each node in this paper.}\]
Fig. 3. The achievable secrecy rate of D2DM versus $P_{\text{max}}$ with respect to different number of D2D transmitters, in which $K = 15$, $N = 5$, $L = 5$ and $P_B = 40$ dB.

Fig. 4. The achievable secrecy rate of D2DM versus $P_{\text{max}}$, in which $K = 15$, $M = 5$, $N = 5$, $L = 5$ and $P_B = 40$ dB.

Fig. 5. The achievable rate of CUE with respect to $P_{\text{max}}$, where $K = 15$, $M = 5$, $N = 5$, $L = 5$ and $P_B = 40$ dB.

Fig. 6. Achievable rates with respect to different number of eavesdropper $L$, where $K = 15$, $M = 5$, $N = 5$, $\alpha = 0.5$, $P_{\text{max}} = 20$ dB and $P_B = 40$ dB.

rate. Further more, in the worst case, due to the strong overhearing capability provided by the eavesdropping VAA, the achievable secrecy rate is lower than that of the normal case. However, with the help of AN, the gap between the achievable secrecy rate of the worst case and that of the normal case is small, indicating that the proposed scheme can effectively secure the communication of VD2DM under the worst case. It is also shown in Fig. 4 that the suboptimal secure solution proposed in Section V of [42] can provide a significant achievable secrecy rate, although it is not as good as the optimal solution.

In Fig. 5, we show the achievable rate of CUE as a function of the maximum transmit power of the D2D transmitter group with different $\alpha$. It is easy to see the maximum transmit power of the D2D transmitter group has little effect on CUE’s achievable rate. That is because the proposed algorithms in the normal case and the worst case are to jointly maximize the achievable secrecy rate of VD2DM and achievable rate of CUE, hence the interference at CUE caused by VD2DM keeps limited to a small level. Also, in the suboptimal algorithm, the null-space beamforming ensures that VD2DM does not interfere with CUE. On the other hand, the reason why the achievable rate of the worst case is lower than that of the normal case is that in the worst case, BS needs to split some energy to transmit AN, which decreases the energy to transmit the signal CUE desired. Another interesting observation shown in Fig. 5 is that, when $\alpha = 0.9$, the achievable rate of the suboptimal solution is higher than that of both algorithm 1 and 2. That is because when $\alpha = 0.9$, both algorithm 1 and 2 tend to achieve a higher secrecy rate of D2DM rather than a higher data rate of CUE, which yields more interference at CUE caused by D2D transmitters. By contrast, in the suboptimal scheme, the CUE is always under the null space of D2D transmitters, which means D2D transmitters never interfere with CUE and hence the rate of CUE of the suboptimal algorithm is higher than that of algorithm 1 and 2, note that, the weight sum rates of optimal algorithms are always higher than that of the suboptimal algorithm, whatever the value of $\alpha$ is.

In Fig. 6, we present the impacts of the number of eavesdroppers, $L$, on the achievable secrecy rate. As the number of eavesdroppers increases, the achievable secrecy rate decreases. However, the decreasing trends of achievable secrecy rate are not obvious in both the normal case and the worst case. This is because the proposed algorithms can effectively limit the overhearing capacity of eavesdroppers by jointly optimizing the beamforming vector of the D2D transmitter group and BS. Another point of concern is that, for the suboptimal solution, when $L$ increases from 1 to 3, the decreasing trend of achievable secrecy rate is obvious, but when $L$ increases from 4 to 9, the decreasing trend is not obvious. At last, in the normal case and the worst case, the achievable data rates of CUE are almost unaffected by the number of eavesdroppers, since eavesdroppers only overhear VD2DM and the BS has enough power budget to transmit AN without affecting the transmission of $s_B$. 

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
The relationship between achievable rates and the number of D2D receivers is illustrated in Fig. 7. We can see that as the number of D2D receivers increases, the achievable secrecy rate decreases slowly. The reason why more D2D receivers result in lower achievable secrecy rate is that the larger the number of D2D receivers, the higher the probability of a poor channel condition of the worst channel receiver. However, the proposed algorithms in both the normal case and the worst case are max-min based algorithms that take care of the worst channel receivers. Hence, the trend of decrease is slow.

As above mentioned, as the number of receivers increases, it becomes more difficult to ensure communication security. Thus, the proposed algorithms tend to use the BS’s signals (such as signals desired by CUE and AN) to interfere with eavesdroppers for increasing the achievable secrecy rate, which makes the achievable rate of CUE decrease slowly.

At last, the overall convergence process of the proposed algorithms is shown in Fig. 8. It can be seen that, setting the maximum iteration number of Algorithm 1 and 2 as five is enough to achieve the near optimal solution, which means the proposed algorithms can converge quickly.

VI. CONCLUSION

This paper has studied the secure transmission design for a VAA-aided D2D multicast communication system under the threat of multiple eavesdroppers. By treating eavesdroppers as either independent overhearing or joint overhearing, respectively, two different non-convex optimization problems have been proposed and solved to achieve the sum data rate of both the cellular user equipment and the achievable secrecy rate of the D2D multicast communication. Also a time-saving suboptimal beamforming scheme has been proposed to adapt to the high dynamic network. Simulation results have validated the advantages of the VAA-aided D2D multicast scheme from the perspective of wireless communication security.

APPENDIX A

PROOF OF PROPOSITION 1

Let \( \beta_{\text{worst}}^* \) be the optimal solution of the outer-level optimization problem, \( \mathbf{W}^*, \mathbf{W}_B^*, \mathbf{Q}^* \) and \( \varphi_{\text{worst}}^* \) be the optimal solution of the inner-level problem (45) with fixed \( \beta_{\text{worst}}^* \) (in this case, \( \mathbf{W}^*, \mathbf{W}_B^*, \mathbf{Q}^* \) and \( \varphi_{\text{worst}}^* \) are also the optimal solution of (44)). Then, we formulate the following power minimization problem (54), shown at the top of the next page. Let \( \mathbf{W}, \mathbf{W}_B \) and \( \mathbf{Q} \) be the optimal solutions of (54), following Appendix B in [40], we have \( \mathbf{W}, \mathbf{W}_B \) and \( \mathbf{Q} \) are also the optimal solution of (45) with fixed \( \beta_{\text{worst}}^* \).

Then, we write the Lagrangian associated with (54) as (55), shown at the top of the next page, in which \( \mathbf{A} \succeq 0, \mathbf{B} \succeq 0, \mathbf{C} \succeq 0, \mathbf{D} \succeq 0, \varepsilon_n \geq 0, \lambda \geq 0, \mu \geq 0 \) and \( \nu_n \geq 0, \forall n \in N \) are the dual variables corresponding to primal constraints in (54). Let \( \mathbf{I}_e = \text{diag}(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_M) \), the KKT conditions that are relevant to \( \mathbf{W} \) are given by

\[
\mathbf{I} + \mathbf{I}_e + \mu (\mathbf{R}_C^{\text{worst}}^* - 1) \mathbf{H}_C - \sum_{n=1}^{N} \nu_n \mathbf{H}_{D,n} + \mathbf{G}_E \mathbf{A} \mathbf{G}_E^H - \mathbf{B} = 0
\]

\[
\nu_n (e^{\varphi_{\text{worst}}^*} \text{Tr} (\mathbf{H}_{B,n} \mathbf{W}_B) + e^{\varphi_{\text{worst}}^*} \text{Tr} (\mathbf{QH}_{B,n}) + e^{\varphi_{\text{worst}}^*} - \text{Tr} (\mathbf{H}_{B,n} \mathbf{W}_B) - \text{Tr} (\mathbf{QH}_{B,n}) - \text{Tr} (\mathbf{H}_{D,n} \mathbf{W}) - 1) = 0
\]

\[
\mathbf{W} \succeq 0
\]

\[
\mathbf{B} \mathbf{W} = 0.
\]

Postmultiplying (56) by \( \mathbf{W} \) and making use of (59) yield

\[
\left( \mathbf{I} + \mathbf{I}_e + \mu (\mathbf{R}_C^{\text{worst}}^* - 1) \mathbf{H}_C + \mathbf{G}_E \mathbf{A} \mathbf{G}_E^H \right) \mathbf{W} = \left( \sum_{n=1}^{N} \nu_n \mathbf{H}_{D,n} \right) \mathbf{W}
\]

\[
\text{Rank} (\mathbf{W}) = \text{Rank} \left( \sum_{n=1}^{N} \nu_n \mathbf{H}_{D,n} \right), \text{Rank} (\mathbf{W}) \leq \min \left( \text{Rank} \left( \sum_{n=1}^{N} \nu_n \mathbf{H}_{D,n} \right), \text{Rank} (\mathbf{W}) \right)
\]

From (61) we still can hardly calculate the rank of \( \mathbf{W} \), since the rank of \( \sum_{n=1}^{N} \nu_n \mathbf{H}_{D,n} \) is hardly to be known. However, combining complementary relaxation condition (57)
\[
\min_{\bar{W} \geq 0, \bar{w} \geq 0, \bar{q} \geq 0} \text{Tr} (\bar{W}) + \text{Tr} (\bar{W} B) + \text{Tr} (\bar{Q}) \\
\text{s.t. } C1', C2' \]
\[
C4'': \log \left( 1 + \frac{\text{Tr} (H_{BC} W_B)}{\text{Tr} (Q H_{BC}) + \text{Tr} (H_C W) + 1} \right) \geq R^{w_{\text{worse}}} \\
\iff e^{w_{\text{worse}}} (\text{Tr} (Q H_{BC}) + \text{Tr} (H_C W) + 1) - \text{Tr} (H_{BC} W_B + Q H_{BC} + H_C W) - 1 \leq 0 \\
C6'': \log \left( 1 + \frac{\text{Tr} (H_{D,n} W)}{\text{Tr} (H_{B,n} W_B) + \text{Tr} (Q H_{B,n}) + 1} \right) - \varphi_{w_{\text{worse}}} \geq 0 \\
\iff e^{w_{\text{worse}}} (\text{Tr} (H_{B,n} W_B) + \text{Tr} (Q H_{B,n} + 1)) - \text{Tr} (H_{B,n} W_B + Q H_{B,n} + H_{D,n} W) - 1 \leq 0, \forall n \in N \\
C24': (e^{w_{\text{worse}}} - 1) (G_B^H W_B G_B + G_B^H Q G_B + I_L) - G_B^H W G_E \geq 0. \tag{54}
\]

\[
L (\bar{W}, \bar{B}, Q, \varepsilon, \lambda, \mu, \nu, A, B, C, D) \\
= \text{Tr} (\bar{W}) + \text{Tr} (\bar{W} B) + \text{Tr} (\bar{Q}) + \sum_{m=1}^{M} \varepsilon_m (\bar{w} [m] - P_{\text{max}}/M) + \lambda (\text{Tr} (\bar{W} B) + \text{Tr} (\bar{Q} - P_B) \\
+ \mu (e^{w_{\text{worse}}} (\text{Tr} (Q H_{BC}) + \text{Tr} (H_C W) + 1) - \text{Tr} (H_{BC} W_B + Q H_{BC} + H_C W) - 1) \\
+ \sum_{n=1}^{N} \nu_n (e^{w_{\text{worse}}} (\text{Tr} (H_{B,n} W_B) + \text{Tr} (Q H_{B,n}) + 1)) - \text{Tr} (H_{B,n} W_B + Q H_{B,n} + H_{D,n} W) - 1 \\
+ \text{Tr} (A (1 - e^{w_{\text{worse}}}) (G_B^H W_B G_B + G_B^H Q G_B + I_L) + A G_E^H W G_E) - \text{Tr} (B W) - \text{Tr} (C W B) - \text{Tr} (D Q). \tag{55}
\]

and C6'' in (54), we can conclude that for any \( \forall n \in N \)
\[
\begin{cases}
\nu_n \geq 0, \text{if} \log \left( 1 + \frac{\text{Tr} (H_{D,n} W)}{\text{Tr} (H_{B,n} W_B) + \text{Tr} (Q H_{B,n}) + 1} \right) - \varphi_{w_{\text{worse}}} \leq 0 \\
\nu_n = 0, \text{if} \log \left( 1 + \frac{\text{Tr} (H_{D,n} W)}{\text{Tr} (H_{B,n} W_B) + \text{Tr} (Q H_{B,n}) + 1} \right) - \varphi_{w_{\text{worse}}} > 0.
\end{cases}
\]

Hence, if there has only one \( \hat{n} \) that makes
\[
\log \left( 1 + \frac{\text{Tr} (H_{D,n} W)}{\text{Tr} (H_{B,n} W_B) + \text{Tr} (Q H_{B,n}) + 1} \right) - \varphi_{w_{\text{worse}}} = 0,
\]
we have
\[
\sum_{n=1}^{N} \nu_n H_{D,n} \rightarrow \nu_{\hat{n}} H_{D,\hat{n}} \text{ or } 0 \text{ which is of rank one and then} \\
\text{we can drive the following inequation (63) from (61), which} \\
\text{implies Rank} (\bar{W}) = 1 \text{ or } 0. \text{ Because Rank} (\bar{W}) = 0 \text{ means} \\
\text{all zero matrix which is meaningless, we have Rank} (\bar{W}) = 1.
\]
\[
\text{Rank} (\bar{W}) \leq \min (\text{Rank} (\nu_{\hat{n}} H_{D,\hat{n}}) \text{ or } 0, \text{Rank} (\bar{W})) \\
= \min (1 \text{ or } 0, \text{Rank} (\bar{W})) \tag{63}
\]

REFERENCES

[1] C. Kai, H. Li, L. Xu, Y. Li, and T. Jiang, “Energy-efficient device-to-device communications for green smart cities,” IEEE Trans. Ind. Informat., vol. 14, no. 4, pp. 1542–1551, Apr. 2018.

[2] M. Peer, V. A. Bohara, and A. Srivastava, “Cache selection in dynamic D2D multicast networks using inhomogeneous Markov model,” IEEE Trans. Netw. Sci. Eng., vol. 7, no. 4, pp. 3235–3245, Oct. 2020.

[3] M. Elnouari, S. Deshmukh, and B. Beferull-Lozano, “Distributed resource allocation in underlay multicast D2D communications,” IEEE Trans. Commun., vol. 69, no. 5, pp. 3409–3422, May 2021.

[4] J. Peng, H. Qiu, J. Cai, W. Xu, and J. Wang, “D2D-assisted multi-user cooperative partial offloading, transmission scheduling and computation allocating for MEC,” IEEE Trans. Wireless Commun., vol. 20, no. 8, pp. 4858–4873, Aug. 2021.

[5] T. Fang, F. Yuan, L. Ao, and J. Chen, “Joint task offloading, D2D pairing, and resource allocation in device-enhanced MEC: A potential game approach,” IEEE Internet Things J., vol. 9, no. 5, pp. 3226–3237, Mar. 2022.

[6] M. Mehrabi, D. You, V. Latzko, H. Salah, M. Reisslein, and F. H. P. Fitzek, “Device-enhanced MEC: Multi-access edge computing (MEC) aided by end device computation and caching: A survey,” IEEE Access, vol. 7, pp. 166079–166108, 2019.

[7] S. Yu, B. Dab, Z. Movahedi, R. Langar, and L. Wang, “A socially-aware hybrid computation offloading framework for multi-access edge computing,” IEEE Trans. Mobile Comput., vol. 19, no. 6, pp. 1247–1259, Jun. 2020.

[8] D. Wang, Y. Lan, T. Zhao, Z. Yin, and X. Wang, “On the design of computation offloading in cache-aided D2D multicast networks,” IEEE Access, vol. 6, pp. 63426–63448, 2018.

[9] R. Karasik, O. Simeone, and S. Shamai (Shitz), “How much can D2D communication reduce content delivery latency in fog networks with edge caching,” IEEE Trans. Commun., vol. 68, no. 4, pp. 2308–2323, Apr. 2020.

[10] M. S. Al-Abiad and M. J. Hossain, “A low-complexity multicast scheduling for D2D-aided F-RANs using network coding,” IEEE Wireless Commun. Lett., vol. 10, no. 11, pp. 2484–2488, Nov. 2021.

[11] F. Jiang, L. Zhang, C. Sun, and Z. Yuan, “Clustering and resource allocation strategy for D2D multicast networks with machine learning approaches,” China Commun., vol. 18, no. 1, pp. 196–211, Jan. 2021.

[12] L. Yang, D. Wu, S. Xu, G. Zhang, and Y. Cai, “Social-energy-aware user clustering for content sharing based on D2D multicast communications,” IEEE Access, vol. 6, pp. 36092–36104, 2018.

[13] L. Yang, D. Wu, Y. Cai, X. Shi, and Y. Wu, “Learning-based user clustering and link allocation for content recommendation based on D2D multicast communications,” IEEE Trans. Multimedia, vol. 22, no. 8, pp. 2111–2125, Aug. 2020.

[14] B. Bhargwaj and S. Agnihotri, “Energy- and spectral-efficiency trade-off for D2D-multicasts in underlay cellular networks,” IEEE Wireless Commun. Lett., vol. 7, no. 4, pp. 546–549, Aug. 2014.

[15] H. Meshgi, D. Zhao, and R. Zheng, “Optimal resource allocation in multicast device-to-device communications underlaying LTE networks,” IEEE Trans. Veh. Technol., vol. 66, no. 9, pp. 8357–8371, Sep. 2017.

[16] J. Yue, C. Ma, H. Yu, and W. Zhou, “Secrecy-based access control for device-to-device communication underlaying cellular networks,” IEEE Commun. Lett., vol. 17, no. 11, pp. 2006–2010, Nov. 2013.
D. H. Brandwood, “A complex gradient operator and its application in L. Lei, Z. Zhong, C. Lin, and X. Shen, “Operator controlled device-
S.-C. Wang and W. Liao, “Cooperative multicasting for wireless
H. Jung, S.-W. Ko, and I.-H. Lee, “Secure transmission using linearly
C. Kai, H. Li, L. Xu, Y. Li, and T. Jiang, “Joint subcarrier assignment with power allocation for sum rate maximization of D2D
Q. Li and W.-K. Ma, “Spatially selective artificial-noise aided transmit
Z.-Q. Luo, W.-K. Ma, A. M.-C. So, Y. Ye, and S. Zhang, “Semidefinite relaxation of quadratic optimization problems,” IEEE Signal Process.
X. Hu, Y. Yi, K. Li, H. Zhang, and C. Kai, “Secure transmission design for virtual antenna array-aided device-to-device multicast communications.” 2022, arXiv:2208.06977.

Xinyue Hu received the B.Eng. and Ph.D. degrees from the Hefei University of Technology, Hefei, China, in 2013 and 2020, respectively. He is currently a Lecturer with the School of Electronic and Information Engineering, Anhui University. His research interests include MIMO, signal processing, cooperative communications, and wireless security communications.

Yibo Yi (Student Member, IEEE) received the B.S. degree in communication engineering and the M.S. degree in electronic and communication engineering from the Hefei University of Technology, Hefei, China, in 2018 and 2021, respectively, where he is currently pursuing the Ph.D. degree in information and communication engineering. His research interests include convex optimization, stochastic geometry, intelligent reflecting surface technology, and resource allocation in wireless communications.

Kun Li received the M.S. degree in communication and information systems and the Ph.D. degree in photogrammetry and remote sensing from Wuhan University, Wuhan, China, in 2006 and 2013, respectively. He has been working as a Senior Engineer in signal processing since 2016. He is currently an Associate Professor with Anhui University. His main research interests include wireless communications, software-defined radio, and radar technology.

Hongwei Zhang received the M.Sc. degree from Anhui University in 2002 and the Ph.D. degree from Shanghai Jiaotong University in 2006. He is currently an Associate Professor and a Master’s Supervisor with Anhui University. His main research interests include wireless communications, the Internet of Things, and big data analysis.

Caihong Kai (Member, IEEE) received the B.S. degree from the Hefei University of Technology, Hefei, China, in 2003, the M.S. degree in electronic engineering and computer science from the University of Science and Technology of China, Hefei, in 2006, and the Ph.D. degree in information engineering from The Chinese University of Hong Kong, Hong Kong, in 2010. She is currently a Professor with the School of Computer Science and Information Engineering, Hefei University of Technology. Her research interests include wireless networking, network protocols, and performance evaluation.