IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 1, 2021, accepted February 15, 2021, date of publication February 22, 2021, date of current version March 4, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3060799

Equalization-Based Beamforming for Secure Multicasting in Multicast Wiretap Channels

DUCKDONG HWANG[1], (Member, IEEE), JANGHOON YANG[2], (Member, IEEE), KUHYUNG KWON[3], JINGON JOUNG[4], (Senior Member, IEEE), AND HYOUNG-KYU SONG[5,6], (Member, IEEE)

[1]Department of Electronics and Communication Engineering, Sejong University, Seoul 05006, South Korea
[2]Seoul Media Institute of Technology, Seoul 03925, South Korea
[3]Samsung Electronics, Suwon 16677, South Korea
[4]School of Electrical and Electronics Engineering, Chung-Ang University, Seoul 06974, South Korea
[5]Department of Information and Communications Engineering, Sejong University, Seoul 05006, South Korea
[6]Department of Convergence Engineering for Intelligent Drone, Sejong University, Seoul 05006, South Korea

Corresponding author: Janghoon Yang (jhyang@smit.ac.kr)

This work was supported in part by the Ministry of Science and Information and Communication Technologies (ICT) (MSIT), Korea, through the Information Technology Research Center (ITRC) support program supervised by the Institute for Information and communications Technology Promotion (IITP) under Grant IITP-2019-2018-0-01423, and in part by the Basic Science Research Program through the National Research Foundation of Korea (NRF) grant by the Ministry of Education under Grant 2020R1A6A1A03038540.

ABSTRACT In this paper, a beamforming scheme is proposed to maximize a secrecy multicast rate (SMR) in the multicast wiretap channel, in which the multiple unauthorized users overhear the multicast messages. The SMR is formulated by the ratio of multicast rate and information leakage in the numerator and denominator, respectively. By exploiting the SMR structure, we propose three doubly equalizing beamforming approaches: i) zero-forcing algorithm, ii) bottom-first algorithm, and iii) top-first algorithm. Depending on the algorithms, either the legitimate user channels or the unauthorized user channels are fully equalized, and the other set of channels are then equalized through a least-squares approach. While the zero-forcing algorithm optimizes the strength of legitimate user channels, the bottom-first and the top-first algorithms find the balance between the strengths of legitimate user channels and unauthorized user channels. The top-first algorithm encompasses the bottom-first algorithm, where the bottom-first algorithm encompasses the zero-forcing algorithm. Consequently, the proposed top-first algorithm outperforms the other two algorithms. The proposed top-first algorithm improves SMR by effectively preventing overhearing while sustaining almost maximum multicast rate and provide comparable SMR to the multicast rate obtained without unauthorized users. These results are verified by simulation.

INDEX TERMS Secrecy rate, multicast channel, beamformer, equalization.

I. INTRODUCTION

Multicast techniques allow the access points (AP) to distribute common messages to groups of users [3]–[5] so that they can supplement the cellular systems based on the delivery of separate messages for individual users. The throughput of the multicast channel is determined by the weakest channel among the user channels served by the same message, where the optimal beamforming at the APs is approached by the semi-definite programming method [3], [4]. The coordinated beamforming in the multi-cell environment also supports multi group multicast [5]. On the other hand, the physical layer security [6]–[9] can protect message delivery from security attacks, independent of high-layer-based security measures, which is typically expensive. Various aspects of physical layer security have drawn much attention from industry and academia [7], [10]–[22].

Multicast transmissions also need confidentiality from unauthorized or malicious users, audio/video streaming only to subscribed users and emergency messaging only to related users are few such examples. The application of physical layer security approaches provides inexpensive alternatives for such requirements [23]. Most studies on the security of multicast channel have been considered in

The associate editor coordinating the review of this manuscript and approving it for publication was Meng-Lin Ku.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

conjunction with radio-frequency energy harvesting at the same time [24]–[28]. In [26], the authors proposed a nested optimization structure, in which the transmit power was minimized for the fixed rate or a secrecy multicast rate (SMR) was maximized for the fixed power when multi-party eavesdroppers collude and legitimate users harvest radio-frequency energy at the same time. In a similar setting, the authors of [27] proposed a semi-definite relaxation (SDR) and Charnes-Cooper transformation-based SMR maximization within energy harvesting constraints. Video multicast with the passive eavesdroppers and energy harvesting constraint was considered in [24] and the beamforming in the relay aided multicast networks was considered in [25]. The resource allocation for the multi-group multicast orthogonal-frequency-division multiplexing systems with simultaneous wireless information and power transfer was considered in [28]. Herein, we consider the SMR maximizing beamforming in multicast networks with multiple malicious users eavesdropping. Since the SMR in the multicast wiretap channel is characterized by a rational function with a minimum operator among the multicast channels in the numerator and a maximum operator among the wiretap channels in the denominator, respectively [23], [26], [27], sub-optimal approaches based on SDR to acquire the SMR have been introduced. Also, a SDR based optimal beamforming is introduced in [1]. However, the computation required to execute the SDR of these approaches asks for excessive resources.

In this paper, we propose three algorithms to design the multicast beamforming vectors based on the least-squares (LS) linear equalization, so that their computational complexity is significantly reduced and practically implementable compared to the SDR-based approaches, while the resulting SMR values attain a comparable portion of those from the optimal scheme and the multicast rate. The proposed three algorithms are composed of two steps of beamforming. In the first step, either the multicast channels or the wiretap channels are fully equalized. In the second step, using the orthogonal complement of the space used for the equalization, the LS estimation is applied to equalize the other unequalized channels from the first step, which results in a limited estimation error. Throughout the two steps, we obtain SMR expressions as rational functions consist of parameters of the two equalized levels. The strength of the fully equalized channels, as a part of an SMR function, can be parameterized and makes the overall SMR function unimodal over this strength parameter, which allows us to obtain the optimal points by using a one-dimensional search such as golden section search (GSS). The first proposed algorithm, i.e., called a *zero-forcing* algorithm, forces the wiretap channels to be equalized to zero (nulled out) and maximizes the multicast rate while the LS estimation error is within a certain bound. The second proposed algorithm, i.e., called a *bottom-first* algorithm, starts to equalize the wiretap channels, applies then the LS estimation to equalize the multicast channel, and finally applies the GSS over the channel strength parameter. The third proposed algorithm, i.e., called a *top-first* algorithm, equalizes the multicast channels first, applies then the LS estimation to equalize the wiretap channel, and finally applies the GSS over the channel strength parameter. To progressively improve SMR, the top-first algorithm includes the bottom-first algorithm, where the bottom-first algorithm includes the zero-forcing algorithm. Thus, the SMR can be progressively improved and the proposed top-first algorithm can provide the largest SMR as verified by numerical results.

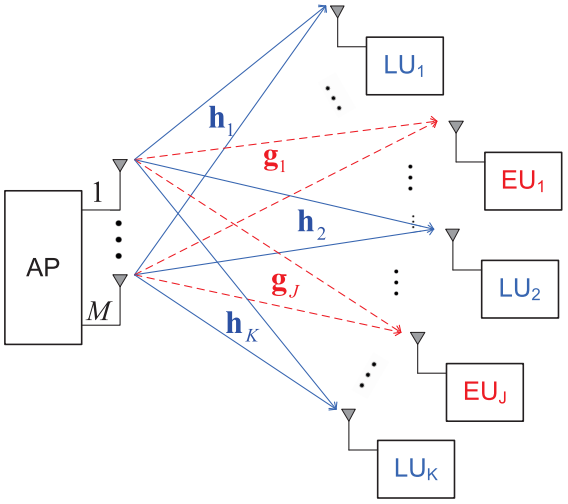

FIGURE 1. Multicast wiretap channel with an AP, K legitimate users (LUs), and J eavesdropping users (EUs).

This paper is organized as follows. In Section II, the system model of the proposed multi-antenna multicast channel with multiple unauthorized eavesdropping users is presented. Three beamforming designs are presented in Section III. After presenting the corroborating numerical results in Section IV, Section V concludes this paper.

Notations: The notations $\mathbf{A}^H$, $\mathbf{A}^T$, and $\mathbf{A}^*$ are the Hermitian transpose, the transpose and conjugate of a matrix $\mathbf{A}$, respectively. $|a|$ and $\|\mathbf{a}\|$ denote the absolute value of a and the norm of $\mathbf{a}$, respectively. The notation $\mathbf{1}_J$ denotes the all one vector with J elements and $\phi(\mathbf{a})$ generates a vector whose nth element is the phase of the nth element of $\mathbf{a}$ with unit magnitude. $\mathbf{A}_{i,j}$ represents the (i,j)th element of $\mathbf{A}$; $\mathbf{a} \sim \mathcal{CN}(\mathbf{0}, \mathbf{C})$ denotes a complex white Gaussian random vector $\mathbf{a}$ with zero mean vector $\mathbf{0}$ and the covariance matrix $\mathbf{C}$. $\mathsf{E}[a]$ takes the expectation of a and $\angle(\mathbf{a})$ returns the phase vector of a complex vector $\mathbf{a}$. The operator $[a,b]^+$ returns the $\max\{a,b\}$.

II. SYSTEM MODEL

As shown in Fig. 1, the AP tries to send multicast messages to K legitimate users (LUs) while J unauthorized users, i.e., the eavesdropping users (EUs), may attempt to overhear the multicast messages. In such a scenario, the protection of the messages from eavesdropping is necessary in addition to the message delivery toward the legitimate users. We assume that the AP has M antennas whereas each user has a single receive antenna. Since the zero forcing (ZF) suppression of the

unauthorized user channel is a simple and effective approach with a large M, the overloaded condition, $M \geq \max\{K, J\}$ and $M < (K + J)$, is assumed here so that the proposed scheme is expected to make a large improvement over the simple one. The multiple-input single-output (MISO) channel from the AP to the kth LU, i.e., LU_k, is denoted by an $M \times 1$ vector $\mathbf{h}_k$, $k = 1, \ldots, K$ and the MISO channel from the AP to the jth EU, i.e., EU_j is denoted by $M \times 1$ vector $\mathbf{g}_j$, $j = 1, \ldots, J$, whose elements are independent identically distributed as $\mathcal{CN}(0, 1)$.

The received signal of LU_k and EU_j are written as follow[1]

$$y_k = \mathbf{h}_k^T \mathbf{w} x + n_k, \tag{1a}$$
$$r_j = \mathbf{g}_j^T \mathbf{w} x + n_j, \tag{1b}$$

where x is the multicast message signal for K LUs with $\mathsf{E}[|x|^2] = P$ and $\mathbf{w}$ is the $M \times 1$ AP precoder satisfying $\|\mathbf{w}\|^2 = 1$. The rate of x is R bits per second per channel use and n_k and n_j are the additive noise signals at LU_k and EU_j, respectively, with $\mathcal{CN}(\mathbf{0}, \mathbf{1})$ distribution. The signal-to-noise ratio γ at LU_k and EU_j are then given as

$$\gamma_k = |\mathbf{h}_k^T \mathbf{w}|^2 P, \tag{2a}$$
$$\gamma_j = |\mathbf{g}_j^T \mathbf{w}|^2 P. \tag{2b}$$

Defining two sets $\mathcal{K} = \{1, \ldots, K\}$ and $\mathcal{J} = \{1, \ldots, J\}$, we set the SMR as [7], [9]

$$R_{SMR} = \max_{\mathbf{w}} \left[0, \log_2 \left(\frac{1 + \min_{k \in \mathcal{K}} |\mathbf{h}_k^T \mathbf{w}|^2 P}{1 + \max_{j \in J} |\mathbf{g}_j^T \mathbf{w}|^2 P} \right) \right]^+. \tag{3}$$

Here, the optimal AP precoder can be obtained by solving the following problem.

$$\max_{\mathbf{w}} \frac{1 + \min_{k \in \mathcal{K}} |\mathbf{h}_k^T \mathbf{w}|^2 P}{1 + \max_{j \in J} |\mathbf{g}_j^T \mathbf{w}|^2 P}. \tag{4}$$

The denominator of the objective function of (4) makes the problem a non-convex problem. Hence, it is difficult to apply an SDR-based method to directly solve (4). On the other hand, ignoring the denominator of the objective function, the problem (4) becomes a beamformer design problem for the multicast transmission in [3], [4], where the SDR is adopted as a sub-optimal approach. To effectively solve (4) providing near-optimal performance, we propose an efficient design framework in the next section. We assume that the channel status information (CSI) of the legitimate users and the unauthorized users is available through some pilot training procedures.

[1]In this study, it is assumed that the AP knows the EU channels (i.e, $\mathbf{g}_j$). Here, we may assume that EUs operate as the normal users yet do not have permission to access the message x. Thus, the eavesdropping channels can be measured at the AP throughout channel estimation using signals from the EUs. Alternatively, we may assume an EU as Mallory, i.e., an active eavesdropper emitting the jamming signals [29]. Here, the AP also can estimate the eavesdropping channels.

III. BEAMFORMER DESIGN

We define

$$\mathbf{H} \triangleq [\mathbf{h}_1, \ldots, \mathbf{h}_K], \tag{5a}$$
$$\mathbf{G} \triangleq [\mathbf{g}_1, \ldots, \mathbf{g}_J], \tag{5b}$$

with the associated QR decompositions as

$$\mathbf{H} \triangleq \mathbf{Q}_H \mathbf{R}_H, \tag{6a}$$
$$\mathbf{G} \triangleq \mathbf{Q}_G \mathbf{R}_G, \tag{6b}$$

where $\mathbf{Q}_H$ and $\mathbf{Q}_G$ are the $M \times K$ and $M \times J$ basis matrices, respectively, and $\mathbf{R}_H$ and $\mathbf{R}_G$ are the $K \times K$ and $J \times J$ upper triangular matrices, respectively. Here, the QR decomposition is used to identify the basis spaces spanned by the two sets of users. Consider an $M \times M$ unitary matrix

$$\mathbf{Q} = \left[\mathbf{Q}_G^*, \bar{\mathbf{Q}}_G \right], \tag{7}$$

where $\bar{\mathbf{Q}}_G$ is the $M \times (M - J)$ matrix composed of the orthogonal complement basis of $\mathbf{Q}_G$. We can then construct a unit-norm AP precoder as

$$\mathbf{w} = \mathbf{Q}\mathbf{x} = \mathbf{Q}_G^* \mathbf{x}_1 + \bar{\mathbf{Q}}_G \mathbf{x}_2, \tag{8}$$

where $\mathbf{x}_1$ and $\mathbf{x}_2$ are the $J \times 1$ and $(M - J) \times 1$ arbitrary vectors, respectively, with $\|\mathbf{x}_1\|^2 + \|\mathbf{x}_2\|^2 = 1$.

Since the optimization in (4) is hard to handle, we modify the problem. For the denominator of the objective function in (4), we set

$$\mathbf{x}_1 = \sqrt{\frac{\nu}{P}} (\mathbf{R}_G^T)^{-1} \mathbf{1}_J, \tag{9}$$

for a positive ν. We then equalize the eavesdropper channels to the level ν as $\mathbf{G}^T \mathbf{w} = \sqrt{\frac{\nu}{P}} \mathbf{1}_J$. Accordingly, the denominator of (4) becomes $1 + \nu$ by equalizing all the eavesdropper channels. Note that the value of ν should be limited such that

$$\nu \leq \frac{P}{\|(\mathbf{R}_G^T)^{-1} \mathbf{1}_J\|^2} \tag{10}$$

to meet the condition $\|\mathbf{x}_1\| \leq 1$. For the numerator of the objective function in (4), we consider

$$\begin{aligned} \mathbf{H}^T \mathbf{w} &= \mathbf{H}^T \mathbf{Q}_G^* \mathbf{x}_1 + \mathbf{H}^T \bar{\mathbf{Q}}_G \mathbf{x}_2 \\ &= \mathbf{a} + \mathbf{H}^T \bar{\mathbf{Q}}_G \mathbf{x}_2, \end{aligned} \tag{11}$$

where we intend to remove the 'min' operation by setting

$$\mathbf{H}^T \mathbf{w} = \sqrt{\frac{\mu}{P}} \phi(\mathbf{a}) \triangleq \mathbf{z} \tag{12}$$

for a certain equalized legitimate signal level μ (≥ 0) and

$$\mathbf{a} = \mathbf{H}^T \mathbf{Q}_G^* \mathbf{x}_1. \tag{13}$$

Since such an equalization of the legitimate user channels ($\mathbf{z} - \mathbf{a} = \mathbf{H}^T \bar{\mathbf{Q}}_G \mathbf{x}_2$) requires finding $\mathbf{x}_2$ corresponding to μ without the guaranteed solution set, we resort a well-known LS method that minimizes the LS estimation error with the magnitude constraint, i.e., $\|\mathbf{x}_2\|^2 = 1 - \|\mathbf{x}_1\|^2$. For this magnitude constrained LS estimation, the following Lemma 1 is useful.

Lemma 1: Suppose the LS estimation of a vector $\mathbf{b}$ via vector $\mathbf{x}$ is given as $\hat{\mathbf{b}} = \mathbf{B}\mathbf{x}$. The LS estimation of vector $\mathbf{b}$ via vector $\mathbf{x}$ with a magnitude constraint $\|\hat{\mathbf{b}}\| = \xi$ is then given as the re-scaled vector $\xi\mathbf{B}\mathbf{x}/\|\mathbf{B}\mathbf{x}\|$ when $\xi \leq \|\mathbf{B}\mathbf{x}\|$.

Proof: The use of un-scaled LS estimation, i.e., $\hat{\mathbf{b}} = \mathbf{B}\mathbf{x}$, is the best strategy when the magnitude constraint is excessively large such that $\xi \geq \|\mathbf{B}\mathbf{x}\|$. Otherwise, suppose the LS estimation with the magnitude constraint, i.e., $\|\hat{\mathbf{b}}\| = \xi$, is given as $\tilde{\xi}\mathbf{B}\mathbf{x}/\|\mathbf{B}\mathbf{x}\| + \mathbf{e}$ with $\tilde{\xi} < \xi$, $\mathbf{e}^H\mathbf{B}\mathbf{x} = 0$, and $\|\mathbf{e}\|^2 + \tilde{\xi}^2 = \xi^2$. Applying repeatedly a triangular inequality reveals that the square error fulfills $\|\mathbf{b} - \tilde{\xi}\mathbf{B}\mathbf{x}/\|\mathbf{B}\mathbf{x}\| - \mathbf{e}\| \geq \|\mathbf{b} - \xi\mathbf{B}\mathbf{x}/\|\mathbf{B}\mathbf{x}\|$ with the equality being hold when $\tilde{\xi} = \xi$ and $\mathbf{e}$ is a all zero vector. Therefore, the LS estimation with the magnitude constraint is the re-scaled vector of $\mathbf{B}\mathbf{x}$. ■

Let us define

$$\mathbf{S}_H \triangleq (\bar{\mathbf{Q}}_G^H\mathbf{H}^*\mathbf{H}^T\bar{\mathbf{Q}}_G)^{-1}\bar{\mathbf{Q}}_G^H\mathbf{H}^*, \tag{14}$$

For positive μ, the LS estimate of $\mathbf{z} - \mathbf{a}$ with the magnitude constraint $\|\mathbf{x}_2\|^2 = 1 - \|\mathbf{x}_1\|^2$ is achieved with

$$\mathbf{x}_2 = \begin{cases} \sqrt{1-\|\mathbf{x}_1\|^2}\dfrac{\mathbf{S}_H(\mathbf{z}-\mathbf{a})}{\|\mathbf{S}_H(\mathbf{z}-\mathbf{a})\|}, & \text{if } \dfrac{\|\mathbf{S}_H(\mathbf{z}-\mathbf{a})\|}{\sqrt{1-\|\mathbf{x}_1\|^2}} \geq 1, \\ \mathbf{S}_H(\mathbf{z}-\mathbf{a}), & \text{o.w.} \end{cases} \tag{15}$$

Defining

$$\mathbf{A}(\mu) \triangleq \mathbf{I}_K - \min\left\{1, \frac{\sqrt{1-\|\mathbf{x}_1\|^2}}{\|\mathbf{S}_H(\mathbf{z}-\mathbf{a})\|}\right\}\mathbf{H}^T\bar{\mathbf{Q}}_G\mathbf{S}_H, \tag{16}$$

the square of the estimation error is given as

$$\varepsilon = \|\mathbf{A}(\mu)(\mathbf{z}-\mathbf{a})\|^2. \tag{17}$$

It is noteworthy that $\mathbf{A}(\mu)$ becomes a zero matrix when $\sqrt{1-\|\mathbf{x}_1\|^2} \geq \|\mathbf{S}_H(\mathbf{z}-\mathbf{a})\|$ and $M \geq K + J$, which makes $\varepsilon = 0$. For ν, the LS-based equalization approach allows us to approximate the numerator of the metric in (4) conservatively as $1 + \mu - \varepsilon P$. Consequently, we formulate a sub-optimal optimization problem from (4) as follows:

$$\max_{\nu,\mu} \frac{1+\mu-\varepsilon P}{1+\nu}. \tag{18}$$

A. EAVESDROPPER ZERO-FORCING SCHEME ($\nu = 0$)

We are left with optimizing μ and ν in (18), where setting $\nu = 0$ (zero-forced eavesdropper channels) simplifies the problem and leaves only μ to be decided. Here, no leakage signal reaches the eavesdroppers at all so that complete avoidance of the eavesdropping, i.e., the zero-forced EUs, is possible. Here, $\mathbf{x}_1$ becomes an all-zero vector with

$$\mathbf{x}_2 = \begin{cases} \dfrac{\mathbf{S}_H\mathbf{z}}{\|\mathbf{S}_H\mathbf{z}\|}, & \text{if } \|\mathbf{S}_H\mathbf{z}\| \geq 1, \\ \mathbf{S}_H\mathbf{z}, & \text{o.w.} \end{cases} \tag{19}$$

Note that $\phi(\mathbf{a})$ takes only the phases of $\mathbf{a}$ so that we consider a vector $\mathbf{a}$ with a non zero ν though $\mathbf{a}$ is an all zero vector in this subsection. As μ increases from zero, the magnitude of LS estimator is required to be constrained to one from the point with $\|\mathbf{S}_H\mathbf{z}\| = 1$. Also note that the LS estimator does not need to subtract the term $\mathbf{H}^T\mathbf{Q}_G^*\mathbf{x}_1$ from $\mathbf{z}$ since we set $\nu = 0$ in the denominator of (18). We then have

$$\mathbf{A}_0(\mu) = \mathbf{I}_K - \min\left\{1, \frac{1}{\|\mathbf{S}_H\mathbf{z}\|}\right\}\mathbf{H}^T\bar{\mathbf{Q}}_G\mathbf{S}_H, \tag{20}$$

and the square of the estimation error is given as

$$\varepsilon = \frac{\mu\|\mathbf{A}_0(\mu)\phi(\mathbf{a})\|^2}{P}. \tag{21}$$

With the ν fixed to zero, we need to optimize the channel strength μ such that the resulting SMR expression is maximized. Consider the numerator of (18) given as $1+\mu-\varepsilon P = 1 + \mu(1 - \|\mathbf{A}_0(\mu)\phi(\mathbf{a})\|^2)$, which is an increasing function of μ as long as the condition $\|\mathbf{A}_0(\mu)\phi(\mathbf{a})\|^2 < 1$ is fulfilled and the other way around. However, it is easy to show that $\|\mathbf{A}_0(\mu)\phi(\mathbf{a})\|^2$ takes a fixed value as μ increases up to a point where $\|\mathbf{S}_H\mathbf{z}\| = 1$, and then increases if μ increases further. Finally, $\|\mathbf{A}_0(\mu)\phi(\mathbf{a})\|^2$ approaches $\|\phi(\mathbf{a})\|^2 = K$ as μ closes to the infinity. Moreover, it is easy to show that the derivative of $\|\mathbf{A}_0(\mu)\phi(\mathbf{a})\|^2$ with respect to μ is positive for all positive μ, and thus $\mu - \varepsilon P$ is a concave function of μ. The magnitude constraint of the LS estimator orchestrates the above interesting behavior of ε. Therefore, the maximum of $1+\mu(1-\|\mathbf{A}_0(\mu)\phi(\mathbf{a})\|^2)$ can be obtained at μ^* by conducting the GSS over μ within the feasible range of $0 \leq \mu \leq \bar{\mu} = \min_{k\in\mathcal{K}}\|\mathbf{h}_k\|^2 P$. The zero-forced scheme in this subsection is shown in Algorithm 1. Here, the parameter σ is the constant in the GSS to reduce the search range at each iteration.

Algorithm 1 Zero-Forcing Algorithm

1. Set $\sigma = 0.382$.
2. For a $\nu > 0$, find $\mathbf{x}_1 = \sqrt{\frac{\nu}{P}}(\mathbf{R}_G^T)^{-1}\mathbf{1}_J$ such that $\|\mathbf{x}_1\| \leq 1$ and find $\mathbf{a} = \mathbf{H}^T\mathbf{Q}_G^*\mathbf{x}_1$.
3. Find the orthogonal decomposition $\phi(\mathbf{a}) = \mathbf{a}_0 + \mathbf{e}_1$.
4. Set $\nu = 0$ and find $\mathbf{x}_2 = \mathbf{S}_H\mathbf{z}/\|\mathbf{S}_H\mathbf{z}\|$.
5. Conduct the GSS over μ to find μ^* where $\mu - \varepsilon P$ peaks.
6. Find the SMR: $R_{ZF} = \log_2(1 + \mu^* - \varepsilon P)$.

B. BOTTOM-FIRST SCHEME ($\nu > 0$)

The doubly equalizing approach of this paper simplifies the SMR as a function of ν, μ and ϵ as in (18). In this subsection, the unimodal property of the SMR on these parameters is presented and a GSS based algorithm is suggested when we start from equalizing the unauthorized user channels to a certain level ν. When $\nu > 0$, we estimate $\mathbf{z} - \mathbf{a}$ and begin with inspecting its effect on ϵ. From the definition of the matrix $\mathbf{A}(\mu)$ and the associated ε expression, it is readily shown that ε depends on $\|\mathbf{S}_H(\mathbf{z}-\mathbf{a})\|$ and $\|\mathbf{z}-\mathbf{a}\|$. Lemma 2 shows how ε depends on these values: ε is minimized at the point $\sqrt{\frac{\mu}{P}}\mathbf{a}_0 = \mathbf{a}$ if $\|\mathbf{a}_0\| > \|\mathbf{e}_1\|$, and at the point $\mu = 0$ otherwise. The following decomposition of vector $\phi(\mathbf{a})$ is useful in this work. For an arbitrary $\mathbf{a}$, we can decompose $\angle(\mathbf{a})$ as $\phi(\mathbf{a}) = \mathbf{a}_0 + \mathbf{e}_1$ as in Fig. 2, where the vector $\mathbf{e}_1$ satisfies

the orthogonal condition as $\mathbf{a}_0^H\mathbf{e}_1 = 0$ so that the vector $\mathbf{a}_0$ is the orthogonal projection of $\phi(\mathbf{a})$ onto the direction of $\mathbf{a}$ with the error vector $\mathbf{e}_1$. Lemma 2 reveals us the convex shape of epsilon over μ, which helps us to devise the following μ deciding algorithm for a ν.

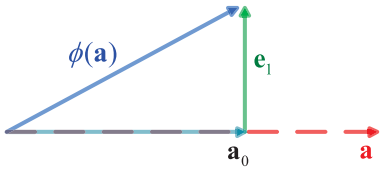

FIGURE 2. The orthogonal decomposition of $\phi(\mathbf{a})$.

Lemma 2: For a fixed ν, the square of the estimation error, i.e., ε, is a strict convex function of μ with the minimum which is achieved at $\sqrt{\frac{\mu}{P}}\mathbf{a}_0 = \mathbf{a}$ if $\|\mathbf{a}_0\| > \|\mathbf{e}_1\|$. If $\|\mathbf{a}_0\| \le \|\mathbf{e}_1\|$, ε is a monotonically increasing function of μ.

Proof: For a fixed ν, the vector to be LS estimated is $\mathbf{z}-\mathbf{a} = \sqrt{\frac{\mu}{P}}\mathbf{a}_0 - \mathbf{a} + \sqrt{\frac{\mu}{P}}\mathbf{e}_1$ so that the magnitude of the first vector $\sqrt{\frac{\mu}{P}}\mathbf{a}_0 - \mathbf{a}$ (on the direction of $\mathbf{a}$) is convex on μ in contrast to that of the second vector $\sqrt{\frac{\mu}{P}}\mathbf{e}_1$. Therefore, $\|\mathbf{z}-\mathbf{a}\|$ is strictly convex on μ if $\|\mathbf{a}_0\| > \|\mathbf{e}_1\|$ and is an increasing function of μ otherwise. Similar property holds for $\|\mathbf{S}_H(\mathbf{z}-\mathbf{a})\|$ depending on the condition $\|\mathbf{S}_H\mathbf{a}_0\| \ge \|\mathbf{S}_H\mathbf{e}_1\|$. The LS estimate of $\mathbf{z}-\mathbf{a}$ becomes $\min\{1, \frac{\sqrt{1-\|\mathbf{x}_1\|^2}}{\|\mathbf{S}_H(\mathbf{z}-\mathbf{a})\|}\}\mathbf{H}^T\bar{\mathbf{Q}}_G\mathbf{S}_H(\mathbf{z}-\mathbf{a})$. Now, the expression for ε can be concisely expressed as $\frac{xb(x)-\tilde{b}(x)}{b(x)}$, where $x = \|\mathbf{z}-\mathbf{a}\|^2$, $b(x) = \|\mathbf{S}_H(\mathbf{z}-\mathbf{a})\|^2$ and $\tilde{b}(x) = \min\{(1-\|\mathbf{x}_1\|^2), \|\mathbf{S}_H(\mathbf{z}-\mathbf{a})\|^2\}\|\mathbf{H}^T\bar{\mathbf{Q}}_G\mathbf{S}_H(\mathbf{z}-\mathbf{a})\|^2$, which confirms, together with the above observations, that the statements of the Lemma 2 are true. This completes the proof. ∎

Note that the magnitude constraint of LS estimator is still in effect so that the dependence of ε on μ is sustained even for a large μ as in the case when $\nu = 0$. Our discussion above focuses on characterizing how ε is related with μ when ν is fixed. However, both μ and ν highly affect the behavior of the objective function $\frac{1+\mu-\varepsilon P}{1+\nu}$ in (18) and they should be carefully designed for the overall beamformer. Hence, μ should be decided as a function of ν such that the objective function in (18) is maximized. Above observation including Lemma 2 leads us to consider the following μ deciding scheme according to a fixed ν, which utilizes the relation

$$\sqrt{\frac{\mu^*}{P}}\mathbf{a}_0 = \mathbf{a} = \sqrt{\frac{\nu}{P}}\mathbf{H}^T\mathbf{Q}_G^*(\mathbf{R}_G^T)^{-1}\mathbf{1}_J \tag{22}$$

regardless of the sign of $\|\mathbf{a}_0\| - \|\mathbf{e}_1\|$. From the found μ^*, we further increase μ as $\mu = \mu^* + \triangle\mu$ until the function $\mu - \varepsilon P$ does not increase.[2] The LS estimated vector then becomes

$$\left(\sqrt{\frac{\mu^*+\triangle\mu}{P}} - \sqrt{\frac{\mu^*}{P}}\right)\mathbf{a}_0 + \sqrt{\frac{\mu^*+\triangle\mu}{P}}\mathbf{e}_1 \tag{23}$$

[2]Note that $\mu = \mu^*$ does not maximize $\mu - \varepsilon P$ though it achieves the minimum of error square. Though both increasing and decreasing μ from μ^* maximize $\mu - \varepsilon P$, we choose increasing because μ appears on the numerator of (18).

with the estimation error

$$\begin{aligned}\varepsilon = &\left(\sqrt{\frac{\mu^*+\triangle\mu}{P}} - \sqrt{\frac{\mu^*}{P}}\right)^2\|\mathbf{A}(\mu)\mathbf{a}_0\|^2 \\ &+2\left(\sqrt{\frac{\mu^*+\triangle\mu}{P}} - \sqrt{\frac{\mu^*}{P}}\right)\left(\frac{\mu^*+\triangle\mu}{P}\right) \\ &\times|\mathbf{a}_0^H\mathbf{A}(\mu)^H\mathbf{A}(\mu)\mathbf{e}_1| \\ &+\left(\frac{\mu^*+\triangle\mu}{P}\right)\|\mathbf{A}(\mu)\mathbf{e}_1\|^2.\end{aligned} \tag{24}$$

Considering the fractional function $\frac{1+ax}{1+x}$, $x \ge 0$, it is easy to show that the function is a monotonically increasing function of x if $a > 1$, whereas it is a monotonically decreasing function of x if $a < 1$. Therefore, the objective function, $\frac{1+\mu-\varepsilon P}{1+\nu}$, increases for the interval with the derivative satisfying $\frac{\partial(\mu-\varepsilon P)}{\partial\nu} > 1$, whereas it decreases for the interval with $\frac{\partial(\mu-\varepsilon P)}{\partial\nu} < 1$. Lemma 3 utilizes this fact to identify the condition, where the above μ deciding method makes the objective function $\frac{1+\mu-\varepsilon P}{1+\nu}$ in (18) is unimodal over ν.

Lemma 3: The above mechanism to decide μ stops at the peak point of unimodal function $\mu - \varepsilon P$ for a fixed ν. Also, it results in a unimodal objective function $\frac{1+\mu-\varepsilon P}{1+\nu}$ of ν if the condition $\|\mathbf{H}^T\mathbf{Q}_G^*(\mathbf{R}_G^T)^{-1}\mathbf{1}_J\| > \|\mathbf{a}_0\|$ holds.

Proof: Similarly as in subsection III-A, ε above is a linearly increasing function of μ before the magnitude of LS estimator is constrained, and then it approaches $\mu K/P$ afterward. Therefore, the function $\mu - \varepsilon P$ for a fixed ν is concave and the above mechanism to decide μ stops at the peak point of the function. When $\|\mathbf{H}^T\mathbf{Q}_G^*(\mathbf{R}_G^T)^{-1}\mathbf{1}_J\| > \|\mathbf{a}_0\|$, the above mechanism produces $\mu^* > \nu$, and thus we have $\frac{\partial\mu^*}{\partial\nu} > 1$. Since μ varies as $\mu = \mu^* + \triangle\mu$, the derivative $\frac{\partial(\mu-\varepsilon P)}{\partial\nu}$ becomes less than one at a point after ε starts to approach $\mu K/P$. Therefore, the objective function $\frac{1+\mu-\varepsilon P}{1+\nu}$ is a unimodal function of ν. This completes the proof. ∎

In summary, the SMR is a unimodal function of ν when $\|\mathbf{a}_0\| < \|\mathbf{H}^T\mathbf{Q}_G^*(\mathbf{R}_G^T)^{-1}\mathbf{1}_J\|$, and we cannot do better than taking $\nu = 0$ as the case in subsection III-A otherwise. From the observations of Lemma 3, the proposed algorithm summarized in Algorithm 2 searches ν that maximizes the objective function with μ maximizing $\mu - \varepsilon P$ in the inner loop. The approaches in subsection III-A and subsection III-B are applied sequentially to produce two SMRs, namely R_{ZF} from a zero-forcing algorithm and R_3 from a bottom-first algorithm, respectively, and the best one between two SMRs is selected finally, i.e., R_{BF}. When the condition in Lemma 3 is fulfilled, the algorithm operates the GSS to locate the peak SMR $R_{s,1}$. Recall that ν should be limited as $\nu \le \frac{P}{\|(\mathbf{R}_G^T)^{-1}\mathbf{1}_J\|^2}$.

C. TOP-FIRST SCHEME

The bottom-first scheme in the previous subsection starts from equalizing the eavesdropper channels. We can develop an alternative algorithm by equalizing the multicast channels first which is called a top-first scheme. We first present the

Algorithm 2 Bottom-First Algorithms

1. Perform Algorithm 1 and obtain R_{ZF}.
2. Set $\sigma = 0.382$.
3. **if** $\|\mathbf{H}^T\mathbf{Q}_G^*(\mathbf{R}_G^T)^{-1}\mathbf{1}_J\| \le \|\mathbf{a}_0\|$ **then**
4. Set $y_{min} = 0$ and $y_{max} = \frac{P}{\|(\mathbf{R}_G^T)^{-1}\mathbf{1}_J\|^2}$.
5. Set $\Delta = y_{max} - y_{min}$.
6. **while** $(\Delta \ge \epsilon)$ (ϵ: sufficiently small value) **do**
7. Set $y_1 = y_{min} + \sigma\Delta$ and $y_2 = y_{max} - \sigma\Delta$.
8. **for** $i = 1, 2$, set $\nu = y_i$. **do**
9. For the ν, find $\mathbf{a} = \sqrt{\frac{\nu}{P}}\mathbf{H}^T\mathbf{Q}_G^*(\mathbf{R}_G^T)^{-1}\mathbf{1}_J$.
10. From $\sqrt{\frac{\mu^*}{P}}\mathbf{a}_0 = \mathbf{a}$, increase $\triangle\mu$ until
11. $\mu - \varepsilon P/K$ stops increasing and $\mu \in [0, \bar{\mu}]$ with $\varepsilon = \left(\sqrt{\frac{\mu^*+\triangle\mu}{P}} - \sqrt{\frac{\mu^*}{P}}\right)^2\|\mathbf{A}(\mu)\mathbf{a}_0\|^2 + 2\left(\sqrt{\frac{\mu^*+\triangle\mu}{P}} - \sqrt{\frac{\mu^*}{P}}\right)\left(\frac{\mu^*+\triangle\mu}{P}\right)|\mathbf{a}_0^H\mathbf{A}(\mu)^H\mathbf{A}(\mu)\mathbf{e}_1| + \left(\frac{\mu^*+\triangle\mu}{P}\right)\|\mathbf{A}(\mu)\mathbf{e}_1\|^2$.
12. Calculate $R_i = \max\left[0, \log_2\left(\frac{1+\mu-\varepsilon P}{1+\nu}\right)\right]$.
13. **end for**
14. **if** $R_1 \le R_2$ **then**
15. $y_{mim} = y_1$.
16. **else**
17. $y_{max} = y_2$.
18. **end if**
19. Set $\Delta = y_{max} - y_{min}$.
20. **end while**
21. Set $\nu = y = \frac{y_{min}+y_{max}}{2}$, calculate $\mathbf{x}_1, \mathbf{x}_2, \mu$, and $R_3 = \max\left[0, \log_2\left(\frac{1+\mu-\varepsilon P}{1+\nu}\right)\right]$.
22. **end if**
23. Find the SMR: $R_{BF} = \max[R_{ZF}, R_3]$.

beam design in this case and follow a similar approach as in subsection III-B to find the unimodal property of the SMR on the equalized level parameters and to suggest another GSS based algorithm for the beamfomer optimization. Suppose that we construct the $M \times M$ unitary matrix

$$\mathbf{Q} = \left[\mathbf{Q}_H^*, \bar{\mathbf{Q}}_H\right], \tag{25}$$

where $\bar{\mathbf{Q}}_H$ is an $M \times (M-K)$ matrix composed of the orthogonal complement basis of $\mathbf{Q}_H$. The unit-norm AP precoder can be put as

$$\mathbf{w} = \mathbf{Q}\mathbf{x} = \mathbf{Q}_H^*\mathbf{x}_1 + \bar{\mathbf{Q}}_H\mathbf{x}_2, \tag{26}$$

where $\mathbf{x}_1$ and $\mathbf{x}_2$ are arbitrary $K \times 1$ and $(M-K) \times 1$ vectors, respectively, with $\|\mathbf{x}_1\| + \|\mathbf{x}_2\| = 1$. Similarly, we set

$$\mathbf{x}_1 = \sqrt{\frac{\mu}{P}}\left(\mathbf{R}_H^T\right)^{-1}\mathbf{1}_K \tag{27}$$

for a positive μ. Accordingly, $\mathbf{H}\mathbf{w} = \sqrt{\frac{\mu}{P}}\mathbf{1}_K$, and then the numerator of (4) becomes $1 + \mu$. Note that the value of μ should be limited such that

$$\mu \le \frac{P}{\|(\mathbf{R}_H^T)^{-1}\mathbf{1}_K\|^2} \tag{28}$$

to meet the condition $\|\mathbf{x}_1\| \le 1$. For the denominator of the objective function in (4), we consider

$$\mathbf{G}^T\mathbf{w} = \mathbf{G}^T\mathbf{Q}_H^*\mathbf{x}_1 + \mathbf{G}^T\bar{\mathbf{Q}}_H\mathbf{x}_2 \tag{29}$$

so that, for a certain ν, the eavesdropper channels are equalized by the LS estimation of $\mathbf{v} - \mathbf{b}$, where

$$\mathbf{v} = \sqrt{\frac{\nu}{P}}\phi(\mathbf{b}), \tag{30}$$

$$\mathbf{b} = \mathbf{G}^T\mathbf{Q}_H^*\mathbf{x}_1. \tag{31}$$

Let us define

$$\mathbf{S}_G = \left(\bar{\mathbf{Q}}_H^H\mathbf{G}^*\mathbf{G}^T\bar{\mathbf{Q}}_H\right)^{-1}\bar{\mathbf{Q}}_H^H\mathbf{G}^*. \tag{32}$$

For a positive μ, the LS estimate of $\mathbf{v}-\mathbf{b}$ with the magnitude constraint $\|\mathbf{x}_2\|^2 = 1 - \|\mathbf{x}_1\|^2$ is achieved with

$$\mathbf{x}_2 = \begin{cases} \sqrt{1-\|\mathbf{x}_1\|^2}\frac{\mathbf{S}_G(\mathbf{v}-\mathbf{b})}{\|\mathbf{S}_G(\mathbf{v}-\mathbf{b})\|}, & \text{if } \frac{\|\mathbf{S}_G(\mathbf{v}-\mathbf{b})\|}{\sqrt{1-\|\mathbf{x}_1\|^2}} \ge 1 \\ \mathbf{S}_G(\mathbf{v}-\mathbf{b}), & \text{o.w.,} \end{cases} \tag{33}$$

which satisfies $\|\mathbf{x}_2\|^2 \le 1 - \|\mathbf{x}_1\|^2$. Defining

$$\mathbf{C}(\nu) \triangleq \mathbf{I}_J - \min\left\{1, \frac{\sqrt{1-\|\mathbf{x}_1\|^2}}{\|\mathbf{S}_G(\mathbf{v}-\mathbf{b})\|}\right\}\mathbf{G}^T\bar{\mathbf{Q}}_H\mathbf{S}_G, \tag{34}$$

the square of estimation error is derived as

$$\varepsilon = \|\mathbf{C}(\nu)(\mathbf{v}-\mathbf{b})\|^2. \tag{35}$$

For a fixed μ, the LS-based equalization approach allows us to approximate the denominator of the objective function in (4) as $1 + \nu + \varepsilon P$ so that we can formulate a conservative and sub-optimal optimization problem as follows.

$$\max_{\nu,\mu} \frac{1+\mu}{1+\nu+\varepsilon P}. \tag{36}$$

Obviously, $\nu + \varepsilon P$ in the denominator of the objective function should be minimized for a fixed μ, which will be carried out by the ν deciding method appears below. Again, we can decompose $\phi(\mathbf{b})$ as $\phi(\mathbf{b}) = \mathbf{b}_0 + \mathbf{e}_2$ with a vector $\mathbf{e}_2$ satisfying the orthogonal condition as $\mathbf{b}_0^H\mathbf{e}_2 = 0$ and the vector $\mathbf{b}_0$ being the orthogonal projection of $\phi(\mathbf{b})$ onto the direction of $\mathbf{b}$.

From the definition of $\mathbf{C}(\nu)$, we can show that the associated ε depends on $\|\mathbf{S}_G(\mathbf{v}-\mathbf{b})\|$ and $\|\mathbf{v}-\mathbf{b}\|$. Here, Similar steps as in Lemma 2 lead us to Corollary 1.

Corollary 1: For a fixed μ, the square of estimation error, ε, is a strict convex function of ν with the minimum achieved at $\sqrt{\frac{\nu}{P}}\mathbf{b}_0 = \mathbf{b}$ when $\|\mathbf{b}_0\| \ge \|\mathbf{e}_2\|$. Otherwise, ε is a monotonically increasing function of ν.

The dependence of ε on ν according to the magnitude constraint of LS estimation is sustained as stated in the previous subsection. Again, we consider a mechanism to determine ν, for a fixed μ, from $\sqrt{\frac{\nu^*}{P}}\mathbf{b}_0 = \mathbf{b} = \sqrt{\frac{\mu}{P}}\mathbf{G}^T\mathbf{Q}_H^*(\mathbf{R}_H^T)^{-1}\mathbf{1}_K$.

From the found ν^*, suppose decreasing ν as $\nu = \nu^* - \min[\triangle\nu, \nu^*]$ until the function $\nu + \varepsilon P$ stops decreasing with $\nu \geq 0$. The LS estimated vector then becomes

$$\left(\sqrt{\frac{\nu^*}{P}} - \sqrt{\frac{\nu^* - \min[\triangle\nu, \nu^*]}{P}}\right)\mathbf{b}_0 + \sqrt{\frac{\nu^* - \min[\triangle\nu, \nu^*]}{P}}\mathbf{e}_2 \quad (37)$$

with the estimation error

$$\begin{aligned}\varepsilon = &\left(\sqrt{\frac{\nu^*}{P}} - \sqrt{\frac{\nu^* - \min[\triangle\nu, \nu^*]}{P}}\right)^2 \|\mathbf{C}(\nu)\mathbf{b}_0\|^2 \\ &+2\left(\sqrt{\frac{\nu^*}{P}} - \sqrt{\frac{\nu^* - \min[\triangle\nu, \nu^*]}{P}}\right) \\ &\times\sqrt{\frac{\nu^* - \min[\triangle\nu, \nu^*]}{P}}\left|\mathbf{e}_2^H\mathbf{C}(\nu)^H\mathbf{C}(\nu)\mathbf{b}_0\right| \\ &+\left(\frac{\nu^* - \min[\triangle\nu, \nu^*]}{P}\right)\|\mathbf{C}(\nu)\mathbf{e}_2\|^2. \end{aligned} \quad (38)$$

The above steps of decreasing ν is in stark contrast to adding $\triangle\mu$ to μ^* in the case of subsection III-B.[3] This difference can be understood if we compare two optimization metric models of (18) and (36), where the above ν deciding method with a fixed μ minimizes the denominator of (36) contrary to maximizing the numerator of (18) in the μ deciding method of subsection III-B.

For a fixed μ, we are interested in the variation of $\nu + \varepsilon P$ resulting from the above method to decide ν as summarized in Lemma 4.

Lemma 4: $\nu = \nu^* - \min[\triangle\nu, \nu^*]$ decreases and stops either at $\nu = 0$ ($\triangle\nu = \nu^*$) or at $\nu = \nu^*$ ($\triangle\nu = 0$).

Proof: According to Corollary 1, it can be readily shown that $\nu + \varepsilon P$ in the denominator of the objective function in (36) is a decreasing function of $\triangle\nu$ for a fixed μ when $\|\mathbf{b}_0\| < \|\mathbf{e}_2\|$. Otherwise, ε increases as ν decreases and then $\nu + \varepsilon P$ becomes a decreasing or increasing function of $\triangle\nu$ depending on the increase rate of ε compared to the decreasing rate of ν. If ε increases faster than the decrease of ν, then $\nu + \varepsilon P$ increases as $\triangle\nu$ increases, and vice versa. Therefore, the statement of the Lemma holds. ■

When the above ν-deciding mechanism stops at $\nu = 0$, which makes the error variance zero, such as $\varepsilon = 0$, and thus the objective function in (36) becomes $1 + \mu$. We then can take the maximum of μ as $\mu_{MAX} = \frac{P}{\|(\mathbf{R}_H^T)^{-1}\mathbf{1}_K\|^2}$. On the other hand, if the mechanism stops at $\nu = \nu^*$, the objective function in (36) becomes $\frac{1+\mu}{1+\nu^*+\varepsilon P}$, which is a concave function of μ if $\max[\|\mathbf{e}_2\|, \|\mathbf{G}^T\mathbf{Q}_H^*(\mathbf{R}_H^T)^{-1}\mathbf{1}_K\|] < \|\mathbf{b}_0\|$, which can be readily shown from Lemma 3. From these observations, the proposed top-first algorithm summarized in Algorithm 3 searches μ that maximizes the SMR for the two cases discussed above and results in two SMR values with ν minimizing $\nu + \varepsilon P$ in the inner loop.

[3]Note that one-dimensional $\mathbf{b}$ case (when $J = 1$) does not require the equalization among the eavesdropper channels, and thus we can choose ν by setting $\mathbf{v} = \mathbf{b}$, which makes $\varepsilon = 0$ with zero error vector ($\mathbf{e}_2$). Such ν corresponds to the ν^* so that we can back off from the ν^* as described above.

Algorithm 3 Top-First Algorithm

1. Perform Algorithms 1 and 2 and obtain R_{ZF} and R_{BF}.
2. Set $\sigma = 0.382$ $R_1 = 0$ and $R_2 = 0$.
3. For a $\mu > 0$, find $\mathbf{x}_1 = \sqrt{\frac{\mu}{P}}(\mathbf{R}_H^T)^{-1}\mathbf{1}_K$ such that $\|\mathbf{x}_1\| \leq 1$ and find $\mathbf{b} = \mathbf{G}^T\mathbf{Q}_H^*\mathbf{x}_1$.
4. Find the orthogonal decomposition $\phi(\mathbf{b}) = \mathbf{b}_0 + \mathbf{e}_2$.
5. **if** $\|\mathbf{b}_0\| < \|\mathbf{e}_2\|$ **then**
6. With $\mu_{MAX} = \frac{P}{\|(\mathbf{R}_H^T)^{-1}\mathbf{1}_K\|^2}$, set the SMR as $R_1 = \max\left[0, \log_2(1 + \mu_{MAX})\right]$.
7. **else if** $\max[\|\mathbf{e}_2\|, \|\mathbf{G}^T\mathbf{Q}_H^*(\mathbf{R}_H^T)^{-1}\mathbf{1}_K\|] < \|\mathbf{b}_0\|$ **then**
8. Set $y_{min} = 0$ and $y_{max} = \mu_{MAX}$.
9. Set $\Delta = y_{max} - y_{min}$.
10. **while** ($\Delta \geq \epsilon$) (ϵ: sufficiently small value) **do**
11. Set $y_1 = y_{min} + \sigma\Delta$ and $y_2 = y_{max} - \sigma\Delta$.
12. **for** $i = 1, 2$, set $\mu = y_i$ **do**
13. For the μ, find $\mathbf{b} = \sqrt{\frac{\mu}{P}}\mathbf{G}^T\mathbf{Q}_H^*(\mathbf{R}_H^T)^{-1}\mathbf{1}_K$.
14. From $\sqrt{\frac{\nu^*}{P}}\mathbf{b}_0 = \mathbf{b}$, find ν^* within $\nu \in [0, \bar{\nu}]$ and calculate $\varepsilon = \frac{\nu^*}{P}[\|\mathbf{C}(\nu^*)\mathbf{b}_0\|^2 + 2|\mathbf{b}_0^H\mathbf{C}(\nu^*)^H\mathbf{C}(\nu^*)\mathbf{e}_2| + \|\mathbf{C}(\nu^*)\mathbf{e}_2\|^2]$.
15. Calculate $R_{s,i} = \max\left[0, \log_2\left(\frac{1+\mu}{1+\nu^*+\varepsilon P}\right)\right]$.
16. **end for**
17. **if** $R_1 \leq R_2$ **then**
18. $y_{mim} = y_1$.
19. **else**
20. $y_{max} = y_2$.
21. **end if**
22. Set $\Delta = y_{max} - y_{min}$.
23. **end while**
24. Set $\mu = y = \frac{y_{min}+y_{max}}{2}$, calculate ν and $R_3 = \max\left[0, \log_2\left(\frac{1+\mu}{1+\nu^*+\varepsilon P}\right)\right]$.
25. **end if**
26. Find the SMR: $R_{TF} = \max[R_{ZF}, R_{BF}, R_3]$.

If $\max[\|\mathbf{e}_2\|, \|\mathbf{G}^T\mathbf{Q}_H^*(\mathbf{R}_H^T)^{-1}\mathbf{1}_K\|] < \|\mathbf{b}_0\|$, the algorithm operates the GSS to locate the peak SMR R_3. The top-first algorithm selects the maximum SMR value among R_{ZF}, R_{BF}, and R_3. Note that ν should be bounded within the range of $0 \leq \nu \leq \bar{\nu} = \min_{k\in\mathcal{J}}\|\mathbf{g}_k\|^2 P$.

The three proposed algorithms all rely on the GSS with the computational complexity of $O(\log(\frac{1}{\epsilon}))$, which is much smaller than that of the most popular search for the SDP, interior point method, given as $O(n\log(\frac{n}{\epsilon}))$. Note that the proposed schemes divide the spatial dimension into two orthogonal parts and each part is used to equalize either the eavesdropper channels or the multicast channels. Therefore, each proposed algorithm is restricted in the usage of the spatial dimension when either K or J approaches M. The impact of such limited spatial dimension will appear in a numerical result in the next section.

IV. NUMERICAL RESULTS

In this section, we present numerical results. An AP equipped with M antennas serves K legitimate users while

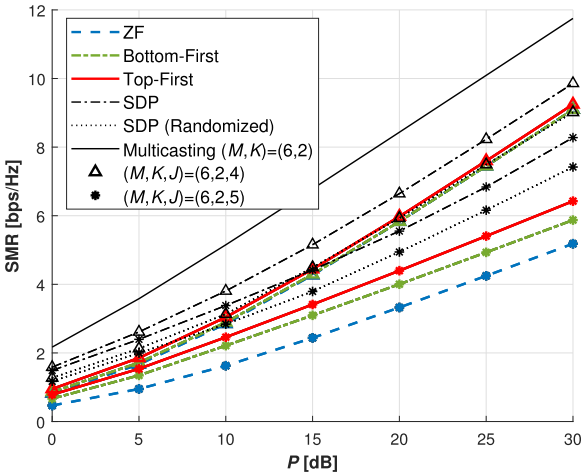

FIGURE 3. Comparison of the multicast rate, SDR based rates and the SMR of proposed schemes as functions of AP power (P). Here, $M = 6$, and K and J vary.

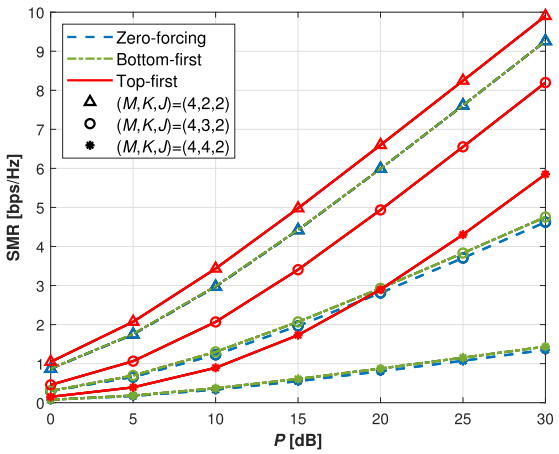

FIGURE 4. SMR comparison of the proposed schemes as functions of AP power (P). Here, $M = 4$, $J = 2$ and K varies. The curves of zero-forcing and the bottom-first algorithms almost coincide for the $K = 2$ case.

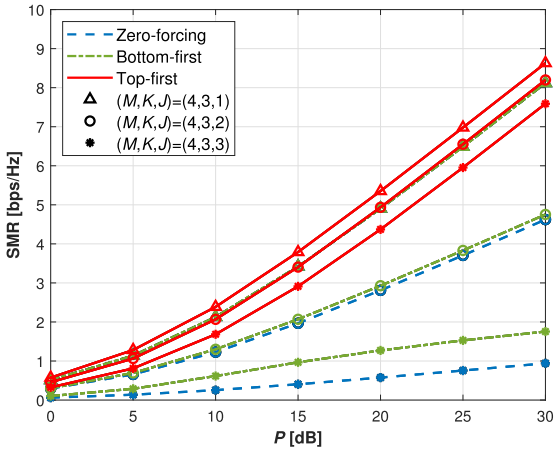

FIGURE 5. SMR comparison of the proposed schemes as functions of AP power (P). Here, $M = 4$, $K = 3$ and J varies. The curves of zero-forcing and the bottom-first algorithms almost coincide for the $J = 1$ case.

J unauthorized users try to overhear the multicast messages. Three proposed beamforming schemes are denoted as follows:

- Zero-forcing: SMR R_{ZF} obtained from Algorithm 1
- Bottom-first: SMR R_{BF} obtained from Algorithm 2
- Top-first: SMR R_{TF} obtained from Algorithm 3

In Fig. 3, the SMRs of proposed schemes are compared to the multicast rate when $M = 6$. Also, plotted are the curves of SDR based scheme of [1], where both the randomized case and the unrandomized case are included. From the comparison, we see how much of the SDR based rates and the multicast rate can be attainable through the proposed schemes. The limitation in the usage of spatial dimension as discussed in the last part of subsection III-C is reflected in the performance of the proposed schemes in comparison with the SDR based rates as follows. When both K and J have enough gaps from M like (M, K, J) of $(6, 2, 4)$, the SMRs of proposed scheme and the randomized SDR scheme are hard to differentiate. If we further reduce the gap between J and M as the case of (M, K, J) of $(6, 2, 5)$, the gap between the SMR R_{TF} and that of the randomized SDR scheme widens. The multicast rate with $J = 0$ also is found from the semi-definite programming-based approaches in [3], [4]. As expected, the top-first algorithm achieves the largest SMR which is closest to the compared rates. As the number of EUs increases, the SMR decreases. Note that the decrease of SMR of the top-first algorithm is relatively smaller than the zero-forcing and bottom-first algorithms.

In Fig. 4, we set $M = 4$ and $J = 2$. By varying K, we observe how the number of LUs, i.e., K, affects the SMR. As K increases with a fixed J, the multicast burden becomes critical to obtain high SMR rather than the security overhead. Hence, the SMRs of the three proposed algorithms decrease as K increases. The zero-forcing and the bottom-first schemes utilize the spatial dimensions for fully equalizing the wiretap channels and only the remaining spatial dimensions are available for equalizing the multicast channels through the LS estimation. On the other hand, the top-first algorithm operates in the other way around. Therefore, the SMR gap between the zero-forcing and bottom-first algorithms is marginal, and the top-first algorithm achieves the largest SMR. This fact makes each scheme perform differently in dealing with the multicast load (i.e., the increase of K) and the wiretapping load (i.e., the increasing J). This is further clarified in Fig. 5.

In Fig. 5 the SMR results are compared by varying the number of EUs, i.e., J, when $M = 4$ and $K = 3$. As J increases and puts more security burden on the multicast channel, the bottom-first algorithm produces more performance improvement compared to the case when K increases, which can be noticed from the comparable gain for the $J = 3$ case. In general, the top-first algorithm makes a large improvement on the SMR. The proposed top-first algorithm can secure the multicast transmission from the increasing security attack.

V. CONCLUSION

We propose beamforming schemes for the multicast wiretap channel, where multiple unauthorized users overhear the

legitimate multicast message transmission. Either the legitimate user channels or the unauthorized user channels are fully equalized and the other set of channels are equalized in the least squares (LS) sense to maximize the secrecy multicast rate (SMR) to protect the multicast transmission from the security attack. Depending on which channel set is fully equalized first and whether the eavesdropper channels are nulled out or not, three algorithms are proposed. They help out each other to produce the best result by progressively including the SMR of each algorithm. Simulations show that the proposed schemes attain quite an amount of rates compared to the multicast rate while protecting the messages being wiretapped by the unauthorized users. Note that the CSI of the multicast users and the eavesdropping users assumed in this paper is not likely to be always sufficient in practical environments. The channel estimator designs under pilot spoofing attack discussed in [2] can be useful measures in such cases. Our approaches need modification to handle the challenge from the limited CSI in near future.

REFERENCES

[1] Q. Li and W.-K. Ma, "Multicast secrecy rate maximization for MISO channels with multiple multi-antenna eavesdroppers," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kyoto, Japan, Jun. 2011, pp. 1–5.
[2] D. Darsena, G. Gelli, I. Iudice, and F. Verde, "Design and performance analysis of channel estimators under pilot spoofing attacks in multiple-antenna systems," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 3255–3269, 2020.
[3] N. D. Sidiropoulos, T. N. Davidson, and Z.-Q. Luo, "Transmit beamforming for physical-layer multicasting," *IEEE Trans. Signal Process.*, vol. 54, no. 6, pp. 2239–2251, Jun. 2006.
[4] T.-H. Chang, Z.-Q. Luo, and C.-Y. Chi, "Approximation bounds for semidefinite relaxation of max-min-fair multicast transmit beamforming problem," *IEEE Trans. Signal Process.*, vol. 56, no. 8, pp. 3932–3943, Aug. 2008.
[5] Z. Xiang, M. Tao, and X. Wang, "Coordinated multicast beamforming in multicell networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 12–21, Jan. 2013.
[6] H. V. Poor, "Information and inference in the wireless physical layer," *IEEE Wireless Commun.*, vol. 19, no. 1, pp. 40–47, Feb. 2012.
[7] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.
[8] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
[9] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, Sep. 2013.
[10] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532–3545, Jul. 2012.
[11] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.
[12] M. Lin, J. Ge, and Y. Yang, "An effective secure transmission scheme for AF relay networks with two-hop information leakage," *IEEE Commun. Lett.*, vol. 17, no. 8, pp. 1676–1679, Aug. 2013.
[13] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and P. C. Ching, "Cooperative secure beamforming for AF relay networks with multiple eavesdroppers," *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 35–38, Jan. 2013.
[14] H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.
[15] Y. Zhou, Z. Z. Xiang, Y. Zhu, and Z. Xue, "Application of full-duplex wireless technique into secure MIMO communication: Achievable secrecy rate based optimization," *IEEE Signal Process. Lett.*, vol. 21, no. 7, pp. 804–808, Jul. 2014.
[16] C. Zhang, H. Gao, T. Lv, Y. Lu, and X. Su, "Beamforming for secure two-way relay networks with physical layer network coding," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Austin, TX, USA, Dec. 2014, pp. 1734–1739.
[17] J. H. Lee, "Full-duplex relay for enhancing physical layer security in multi-hop relaying systems," *IEEE Commun. Lett.*, vol. 19, no. 4, pp. 1180–1183, Apr. 2015.
[18] X. Chen, L. Lei, H. Zhang, and C. Yuen, "Large-scale MIMO relaying techniques for physical layer security: AF or DF?" *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 5135–5146, Sep. 2015.
[19] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 574–583, Mar. 2015.
[20] Y. Gao, Y. Cai, Q. Shi, B. Champagne, and M. Zhao, "Joint transceiver designs for secure communications over MIMO relay," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Shanghai, China, Mar. 2016, pp. 3851–3855.
[21] Z. Chu, H. Xing, M. Johnston, and S. L. Goff, "Secrecy rate optimizations for a MISO secrecy channel with multiple multiantenna eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 283–297, Jan. 2016.
[22] D. Hwang, J. Yang, E. Yoon, H.-K. Song, and S. S. Nam, "Secrecy rate maximizing beamforming schemes for the DF relay wiretap channels," *IEEE Access*, vol. 6, pp. 77841–77848, 2018.
[23] K. Cumanan, Z. Ding, M. Xu, and H. V. Poor, "Secrecy rate optimization for secure multicast communications," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1417–1432, Dec. 2016.
[24] D. W. K. Ng, R. Schober, and H. Alnuweiri, "Secure layered transmission in multicast systems with wireless information and power transfer," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Sydney, NSW, Australia, Jun. 2014, pp. 5389–5395.
[25] H. Gao, T. Lv, W. Wang, and N. C. Beaulieu, "Energy-efficient and secure beamforming for self-sustainable relay-aided multicast networks," *IEEE Signal Process. Lett.*, vol. 23, no. 11, pp. 1509–1513, Nov. 2016.
[26] W. Xu, S. Li, C.-H. Lee, Z. Feng, and J. Lin, "Optimal secure multicast with simultaneous wireless information and power transfer in presence of multiparty eavesdropper collusion," *IEEE Trans. Veh. Technol.*, vol. 65, no. 11, pp. 9123–9137, Nov. 2016.
[27] M. Zhang, K. Cumanan, and A. Burr, "Secrecy rate maximization for MISO multicasting SWIPT system with power splitting scheme," in *Proc. IEEE 17th Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Edinburgh, U.K., Jul. 2016, pp. 1–5.
[28] O. T. Demir and T. E. Tuncer, "Max–min fair resource allocation for SWIPT in multi-group multicast OFDM systems," *IEEE Commun. Lett.*, vol. 21, no. 11, pp. 2508–2511, Nov. 2017.
[29] X. Jiang, X. Liu, R. Chen, Y. Wang, F. Shu, and J. Wang, "Efficient receive beamformers for secure spatial modulation against a malicious full-duplex attacker with eavesdropping ability," 2020, *arXiv:2006.01479*. [Online]. Available: http://arxiv.org/abs/2006.01479

DUCKDONG HWANG (Member, IEEE) received the B.S. and M.S. degrees in electronics engineering from Yonsei University, South Korea, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, CA, USA, in May 2005. From 1993 to 1998, he worked as a Research Engineer with Daewoo Electronics, South Korea. In 2005, he joined the Digital Research Center, Samsung Advanced Institute of Technology, as a Research Staff Member. Since 2012, he has been a Research Associate Professor with the School of Information and Communication Engineering, Sungkyunkwan University, the Department of Electrical Engineering, Konkuk University, and the Department of Electronics, Information and Communication Engineering, Sejong University, South Korea. He is interested in the physical layer aspect of the next generation wireless communication systems, including multiple antenna techniques, interference alignment and management, and cooperative relays and their applications in the heterogeneous small cell networks and wireless security issues.

JANGHOON YANG (Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, USA, in 2001. From 2001 to 2006, he was with the Communication Research and Development Center, Samsung Electronics. From 2006 to 2010, he was a Research Assistant Professor with the Department of Electrical and Electronic Engineering, Yonsei University. Since 2010, he has been with the Seoul Media Institute of Technology, Seoul, South Korea, where he is currently an Associate Professor with the Department of New Media. He has published numerous articles in the area of multi-antenna transmission, signal processing, and control. His research interests include wireless system and networks, artificial intelligence, control theory, neuroscience, affective computing, and intervention for special education.

KUHYUNG KWON received the B.S. and Ph.D. degrees in electrical and electronic engineering from Yonsei University, Seoul, South Korea, in 2013 and 2020, respectively. In 2020, he joined Samsung Electronics Company, Ltd., Suwon, South Korea, as a Staff Engineer. His research interests include full-duplex communication systems and beamforming techniques for wireless power transfer and energy harvesting.

JINGON JOUNG (Senior Member, IEEE) received the B.S. degree in radio communication engineering from Yonsei University, Seoul, South Korea, in 2001, and the M.S. and Ph.D. degrees in electrical engineering and computer science from the Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea, in 2003 and 2007, respectively.

He was a Postdoctoral Fellow with KAIST, in 2007, and the University of California (UCLA), CA, USA, in 2008. From 2009 to 2015, he was a Scientist with the Institute for Infocomm Research (I^2R), Agency for Science, Technology and Research (A*STAR), Singapore. In 2016, he joined Chung-Ang University (CAU), Seoul, as a Faculty Member. He is currently an Associate Professor with the School of Electrical and Electronics Engineering, CAU, where he is also the Principal Investigator with the Intelligent Wireless Systems Laboratory. His research interests include wireless communication signal processing, numerical analysis, algorithms, and machine learning.

Dr. Joung was a recipient of the First Prize from the Intel-ITRC Student Paper Contest, in 2006. He was recognized as an Exemplary Reviewer of the IEEE COMMUNICATIONS LETTERS, in 2012 and the IEEE WIRELESS COMMUNICATIONS LETTERS, in 2012, 2013, 2014, and 2019. He served as a Guest Editor for IEEE ACCESS, in 2016. From 2014 to 2019, he served as an Editorial Board member for the *APSIPA Transactions on Signal and Information Processing* and a Guest Editor for the *Electronics* (MDPI), in 2019. He is currently serving as an Associate Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and *Sensors* (MDPI).

HYOUNG-KYU SONG (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electronic engineering from Yonsei University, Seoul, South Korea, in 1990, 1992, and 1996, respectively. From 1996 to 2000, he was a Managerial Engineer with the Korea Electronics Technology Institute, South Korea. Since 2000, he has been a Professor with the Department of Information and Communication Engineering and the Department of Convergence Engineering for Intelligent Drone, Sejong University. His research interests include digital and data communications, information theory, and their applications with an emphasis on mobile communications.