Physical Layer Security in Wireless Sensor Networks Using Distributed Co-Phasing

Ribhu Chopra, Chandra R. Murthy, and Ramesh Annavajjala

***Abstract*—In this paper, we consider physical layer security in wireless sensor networks (WSNs) using distributed co-phasing (DCP) based transmissions. For this protocol, we first analyze the achievable ergodic secrecy rate of a single stream DCP system in the presence of one or more eavesdroppers. We show that the coherent combining gain offered by DCP leads to the signal to interference plus noise ratio (SINR) over the main channel increasing as the square of the number of SNs N, and that over the eavesdropper channel increasing linearly with N. This results in a strictly positive ergodic secrecy rate that increases as $\log N$. We then analyze the performance of multi-stream DCP and show that using K data streams in DCP leads to a K fold increase in the achievable secrecy rate at high SNRs. We also discuss an alternative power allocation scheme for multi-stream DCP, viz. distributed maximal ratio transmission with a per user power constraint, and show that this improves the achievable secrecy rates as compared to standard multi-stream DCP. Finally, we analyze the role of artificial noise in improving the achievable secrecy rates. We validate the accuracy of these derived results and illustrate the efficacy of DCP in ensuring secure data fusion in WSNs using Monte Carlo simulations.**

I. Introduction

There has been a renewed research interest in wireless sensor networks (WSNs) due to the emergence of the internet of things (IoT) [1], [2]. Traditionally, a WSN comprises a set of spatially distributed sensor nodes (SNs) observing a physical phenomenon of interest, and reporting the observed data to a fusion center (FC) [3]. Secure communication of the observed data from the SNs to the FC is a challenging problem mainly due to the constraints on the capabilities of the SNs [4]–[6]. The goal in secure communications is to ensure that the transmissions by the SNs can be decoded only at the FC. Distributed Co-Phasing (DCP) is a form of distributed transmit beamforming (DTB), where the assumption of the SNs sensing a common field is used to achieve reliable data fusion [7]. Due to the common data being transmitted, the multiple SNs in DCP act as a distributed antenna array, resulting in both diversity gain and coherent combining gain at the FC. Also, since DCP signals are precoded to coherently combine at the FC, they naturally combine incoherently at any unintended location, thereby making DCP inherently secure. In this paper, we quantify this inherent security of DCP systems in terms of the achievable ergodic secrecy rates in the presence of eavesdroppers.

During the first stage of the two stage DCP, the FC transmits known pilot symbols to the SNs. The SNs use these pilots to estimate the respective channels to the FC. In the second stage, the SNs synchronously transmit their data symbols to the FC. The data symbols are pre-rotated to compensate for the estimated channel phase, resulting in coherent combining of the signals at the FC. The reverse link training of the SNs by the FC offers several benefits. Firstly, the FC is connected to the mains and can transmit at higher power compared to the power starved SNs, resulting in better channel estimates. Secondly, reverse link training requires a smaller training overhead compared to forward link training, where the training duration is proportional to the number of SNs. Thirdly, and most relevant to this paper, by initiating the training from the FC, the channel states from the SNs remain unknown at the eavesdroppers' locations.

DCP works under the assumption that the channel is quasi static and reciprocal [8], [9]. The feasibility of DCP in practical implementations, as well as its resilience to channel estimation errors has been well established in the literature [8], [10]. However, while DCP ensures that the symbols transmitted by the SNs can be recovered at the FC with high fidelity, their ability to secure the transmission against reception by an eavesdropper is yet to be studied. In a practical setting, an eavesdropper may exist in the network, and may attempt to access sensitive private information intended for the FC. Therefore, it is interesting to investigate the conditions under which secrecy of the transmitted data can be ensured. In this work, our main focus is to analyze the maximum rates at which the SNs can transmit to the FC, while ensuring secrecy in the presence of one or more eavesdroppers within the network.

A. Related Work

The basic model for DCP, i.e., a DTB system involving multiple SNs transmitting coherently to an FC, was first discussed in [4] using a master slave architecture. Following this, the experimental feasibility of achieving

R. Chopra is with the Indian Institute of Technology Guwahati, Assam, India. C. R. Murthy is with the Indian Institute of Science, Bangalore, India. R. Annavajjala is affiliated with the Northeastern University, Boston, MA, USA. Emails: ribhu@outlook.com, cmurthy1@gmail.com, ramesh.annavajjala@gmail.com.

carrier frequency synchronization among multiple distributed SNs was demonstrated in [8] and [11]. Since DTB schemes involve a phase compensation operation at the SNs, accurate channel state information (CSI) is required. The effects of inaccurate CSI on the performance of DTB systems was investigated in [12]. Various CSI acquisition approaches, such as reverse link training [10], and feedback based approaches [9], [13], [14] have also been discussed in the literature. In [15], asymptotic results are used to evaluate the performance of a WSN system with an multi-antenna FC, under both full and phase only CSI at the SNs.

The BER performance of DCP is compared against distributed maximal ratio transmission, censored transmission and truncated channel inversion in [10] for constant modulus constellations under generalized fading channels. The spectral efficiency of non-constant modulus constellations along with an associated blind channel estimation technique was discussed in [16]. The spectral efficiency of DCP systems was further enhanced in [17], wherein it is proposed that the SNs can simultaneously transmit multiple data streams to a multiantenna FC. Further, the channel gain information available at the SNs has been used in [18] to provide unequal error protection to different data bits using autonomous constellation selection at the SNs. However, these works disregard the physical layer security requirements of WSNs. In many applications, it is important to consider the performance of DCP systems in the presence of one or more eavesdroppers in the network. As we will show, DCP natively supports information theoretically secure communications between the SNs and the FC.

Since DCP is essentially a multi-antenna technique, the metrics used for quantifying its security performance need to be similar to those for other multi-antenna systems. The issue of physical layer security for multiantenna systems was first discussed in [19], wherein, the secrecy performance of a 2×2 MIMO channel in the presence of a single antenna eavesdropper was evaluated. A comprehensive survey on multi-antenna techniques for physical layer security can be found in [20]. Similar to the standard wiretap channel model, the security performance of a MIMO wiretap channel is also measured in terms of the secrecy rate [21] when all the channel coefficients are known. However, practical systems need to work with estimated CSI, which makes the assumption of perfect knowledge of CSI at the SNs/FC untenable.

Recently, physical layer security for MISO systems has been studied in terms of the secrecy outage probability [22]–[25], lower bound on the sum secrecy rate [26], ergodic secrecy rate [27], [28], and secrecy energy efficiency [25], [29], [30]. However, all these works focus exclusively on the physical layer security aspects of *centralized* MISO systems. To the best of our knowledge, the secrecy performance of a DTB system has not been analyzed till date. In this work, we use the ergodic secrecy rate [31], [32] as a metric of the secrecy performance of DCP. Further, we account for channel estimation errors in our performance analysis.

B. Contributions

In this paper, we consider distributed transmission from the SNs to an FC using the co-phasing approach, as opposed to centralized beamforming considered in the past literature, for secure communications. Our analysis accounts for channel estimation errors at the SNs and the resulting phase errors. We derive the achievable ergodic secrecy rates of both single and multistream DCP systems in the presence of one or more eavesdroppers. Our contributions are as follows:

1) We derive the ergodic secrecy rates for a single antenna DCP system with N SNs, with a single eavesdropper, and under both ideal and practical DCP. (See Section II)
2) We extend the results derived in Section II to L eavesdropper, and observe that, under conditions stated later, positive secrecy rates can be achieved using single stream DCP, even with multiple colluding eavesdroppers. (See Section III.)
3) We then consider the more general case of multi-stream DCP with K streams, and show that it results in a K-fold increase in the achievable ergodic secrecy rates. (See Section IV.)
4) We consider an MRT-like transmission scheme for multi-stream DCP with a per antenna power constraint. We show that the use of this scheme further increases the achievable rates over the main channel, and, consequently, the secrecy rate of multi-stream DCP, in the presence of multiple eavesdroppers. (See Section V.)
5) We consider the addition of artificial Gaussian noise to the proposed system. We derive an expression for the optimal fraction of power to be transmitted from the SNs as artificial noise for maximizing the secrecy rate. (See Section VI).
6) Via detailed simulations, we validate the derived theory and evaluate the achievable ergodic secrecy rates under finite constellations. (See Section VII.)

The take-away from this study is that DCP can be used to provide secure physical layer communication for a wireless sensor network under practical channel estimation at the SNs, and in both single stream and multi-stream setups.

Notation: Boldface lowercase and uppercase letters represent vectors and matrices, respectively. The kth column of the matrix $\mathbf{A}$ is denoted by $\mathbf{a}_k$. $(\cdot)^H$ represents the Hermitian of a vector or a matrix. $\|\cdot\|_2$ and $\|\cdot\|_F$ respectively represent the ℓ_2 norm of a vector and the

Frobenius norm of a matrix. $\Re\{.\}$ and $\Im\{.\}$ represent the real and imaginary parts of a complex number respectively. $[x]^+$ is defined as $\max(x, 0)$. $E[\cdot]$ and $\text{var}(\cdot)$ represent the mean and variance of a random variable.

In the next section, we derive the achievable ergodic secrecy rate of single stream DCP in the presence of a single eavesdropper.

II. Single Stream DCP with a Single Eavesdropper

We consider a WSN consisting of N single-antenna SNs communicating with a single antenna FC, with an eavesdropper (EVE) in the vicinity of this network. In DCP, the SNs first estimate the channels to the FC using training signals broadcast by the latter. Then, the nodes transmit their data symbols simultaneously by pre-rotating them using the estimated channel phase, such that they combine coherently at the receiver. For the data detection at the FC, the FC can perform blind channel estimation using the data symbols transmitted by the SNs [16]. Note that, for constant envelop modulation schemes, data can be detected even without blind channel estimation, albeit with a small loss of performance. Throughout this paper, we assume that the communication takes place over a quasi-static block fading narrowband channel [33]. That is, we assume that the channel coefficients remain constant over a block consisting of M channel uses. The channel coefficients vary in an independent and identically distributed (i.i.d.) fashion across blocks. Out of the M channel uses within a block, the first M_p instants are used for reverse link training The next $M_d = M - M_p$ channel uses are used for data transmission from the SNs to the FC.

The received signal at the ith SN during the downlink training stage ($n \in \{1, 2, \ldots, M_p\}$) is

$$q_i[n] = a_{1,i}\sqrt{\mathcal{E}_p} + w_i[n] = \alpha_{1,i}e^{j\theta_{1,i}}\sqrt{\mathcal{E}_p} + w_i[n] \quad (1)$$

with $a_{1,i}$ being the zero mean circularly symmetric complex Gaussian distributed channel coefficient for the channel between the FC and the ith SN with a mean squared channel power $\Omega_{1,i}$, denoted as $a_{1,i} = \alpha_{1,i}e^{j\theta_{1,i}} \sim \mathcal{CN}(0, \Omega_{1,i})$. Also, $w_i[n] \sim \mathcal{CN}(0, N_0)$ is the additive white Gaussian noise (AWGN) at the SN.

Conditioned on $y_i[n]$, $n = 1, \ldots, M_p$, the MMSE estimate of the channel coefficient $a_{1,i}$ at the ith SN can be shown to be

$$\hat{a}_{1,i} = \frac{\sqrt{M_p\mathcal{E}_p\Omega_{1,i}}}{N_0 + M_p\mathcal{E}_p\Omega_{1,i}} \sum_{n=1}^{M_p} q_i[n], \quad (2)$$

with $\mathcal{E}_p$ denoting the pilot power. Therefore, the channel magnitude and phase estimates can be written respectively as $\hat{\alpha}_{1,i} = |\hat{a}_{1,i}|$ and

$$\widehat{\theta}_{1,i} = \tan^{-1}\left(\frac{\Im\{\hat{a}_{1,i}\}}{\Re\{\hat{a}_{1,i}\}}\right). \quad (3)$$

The modulation symbol common to all the SNs is denoted by $s[n]$. To coherently align $s[n]$ at the FC, the ith SN pre-rotates $s[n]$ to compensate for the estimated phase and transmits the symbol $x_i[n]$ such that

$$x_i[n] = \sqrt{\mathcal{E}_s}e^{-j\widehat{\theta}_{1,i}}s[n] \quad n = M_p + 1, \ldots, M, \quad (4)$$

with $\mathcal{E}_s$ denoting the symbol energy. In the following subsections, we derive expressions for the achievable ergodic secrecy rates with both ideal and practical DCP. For the derivation, we assume that the EVE has perfect knowledge of its channels to the SNs, although no explicit training signals are sent by the SNs. This results in a lower bound on the achievable secrecy rate, and is a commonly used assumption in physical layer security related studies.

A. Achievable Ergodic Secrecy Rate under Ideal DCP

Under ideal DCP, we assume that accurate CSI is available at all the SNs, and therefore, $\hat{\theta}_{1,i} = \theta_{1,i}$. Consequently, the signal received by the FC at the nth instant can be expressed as

$$\begin{aligned} y_1[n] &= \sum_{i=1}^{N} \alpha_{1,i}e^{j\theta_{1,i}}x_i[n] + w_1[n] \\ &= N\sqrt{\mathcal{E}_s}h_1 s[n] + w_1[n] \end{aligned} \quad (5)$$

with $w_1[n] \sim \mathcal{CN}(0, N_0)$, and $h_1 \triangleq \frac{1}{N}\sum_{i=1}^{N}\alpha_{1,i}$.

To obtain the achievable ergodic secrecy rates for this system, we need to separately determine the achievable ergodic secrecy rates for the main channel and the eavesdroppers channel [21]. These rates are given in Lemmas 1 and 2 below.

Lemma 1. *For the single antenna DCP system with non identically distributed channels, the achievable rate over the main channel satisfies*

$$\begin{aligned} R_m \geq \eta_p \Bigg(&\log_2\left(\frac{\pi}{4}\frac{\mathcal{E}_s}{N_0}\sum_{i=1}^{N}\sum_{m=1}^{N}\sqrt{\Omega_{1,i}\Omega_{m,i}}\right) \\ &+ \log_2(e)\left(2E[\psi] - \frac{E[\psi^2]}{2} - \frac{3}{2}\right)\Bigg) \end{aligned} \quad (6)$$

with $E[\psi]$ defined in (8)*, $E[\psi^2]$ defined in* (9)*, and $\eta_p = \left(\frac{M-M_p}{M}\right)$, for non identically distributed channels, and*

$$R_m \geq \eta_p\left(\log_2\left(\frac{\pi N^2\mathcal{E}_s}{4N_0}\Omega\right) - \frac{0.3944}{N} - \frac{4.24}{N^2}.\right) \quad (7)$$

for identically distributed channels, with $\Omega_{1,i} = \Omega$ for $i = 1 \ldots N$.

Proof: See Appendix A. ∎

We now turn our attention to the eavesdropper's channel. Letting $b_{1,i} \sim \mathcal{CN}(0, \Delta_{1,i})$ be the channel coefficients between the ith SN and the EVE, we can write the signal received by the EVE as $z[n] =$

$$E[\psi] = \frac{4N^2}{\pi \sum_{i,m=1}^{N} \sqrt{\Omega_{1,i}\Omega_{m,i}}} E[|h_1|^2] = 1 + \left(\frac{4}{\pi} - 1\right) \left(\frac{\sum_{i=1}^{N} \Omega_{1,i}}{\sum_{i,m=1}^{N} \sqrt{\Omega_{1,i}\Omega_{m,i}}}\right) \tag{8}$$

$$E[\psi^2] = \frac{16N^4 E[|h_1|^4]}{\pi^2 \left(\sum_{i,m=1}^{N} \sqrt{\Omega_{1,i}\Omega_{m,i}}\right)^2} = \frac{16}{\pi^2 \left(\sum_{i,m=1}^{N} \sqrt{\Omega_{1,i}\Omega_{m,i}}\right)^2} \Bigg(2\sum_{i=1}^{N} \Omega_{1,i} + 3\sum_{i=1}^{N} \sum_{\substack{k=1 \\ k\neq i}}^{N} \Omega_{1,i}^{3/2} \Omega_{1,k}^{1/2} + 3\sum_{i=1}^{N} \sum_{\substack{k=1 \\ k\neq i}}^{N} \Omega_{1,i}\Omega_{1,k} + 6\sum_{i=1}^{N} \sum_{\substack{k=1 \\ k\neq i}}^{N} \sum_{\substack{l=1 \\ l\neq i,k}}^{N} \Omega_{1,i}\Omega_{1,k}^{1/2}\Omega_{1,l}^{1/2} + \sum_{i=1}^{N} \sum_{\substack{k=1 \\ k\neq i}}^{N} \sum_{\substack{l=1 \\ l\neq i,k}}^{N} \sum_{\substack{m=1 \\ m\neq i,k,l}}^{N} \Omega_{1,i}^{1/2}\Omega_{1,k}^{1/2}\Omega_{1,l}^{1/2}\Omega_{1,m}^{1/2} \Bigg). \tag{9}$$

$\sqrt{\mathcal{E}_s} s[n] \sum_{i=1}^{N} b_{1,i} e^{-j\theta_{1,i}} + v[n] = N\sqrt{\mathcal{E}_s} g_1 s[n] + v[n]$, where $v[n] \sim \mathcal{CN}(0, N_0)$ is the AWGN at the EVE, and $g_1 = \frac{1}{N} \sum_{i=1}^{N} b_{1,i} e^{-j\theta_{1,i}}$. Since g_1 is the sum of independent zero mean circularly symmetric complex Gaussian (ZMCSCG) r.v.s, it is also ZMCSCG.

Lemma 2. *The achievable rate over the EVE's channel in case of a block fading channel is upper bounded as*

$$R_e \leq \eta_p \left(\log_2 \left(1 + \frac{N\mathcal{E}_s}{N_0} \Delta \right) \right). \tag{10}$$

with $\Delta = \frac{1}{N} \sum_{i=1}^{N} \Delta_{1,i}$.

Proof: See Appendix B. ∎

Using these results, a lower bound on the achievable ergodic secrecy rate of the DCP system can be obtained using Theorem 1.

Theorem 1. *The achievable ergodic secrecy rate of the DCP system can be lower bounded as*

$$R_s \geq \eta_p \Bigg[\log_2 \left(\frac{\pi}{4} \frac{\mathcal{E}_s}{N_0} \sum_{i,m=1}^{N} \sqrt{\Omega_{1,i}\Omega_{1,m}} \right) + \log_2(e) \times \left(2E[\psi] - \frac{E[\psi^2]}{2} - \frac{3}{2} \right) - \log_2 \left(1 + \frac{N\mathcal{E}_s}{N_0} \Delta \right) \Bigg]^+. \tag{11}$$

for non identically distributed channels, and

$$R_s \geq \eta_p \Bigg[\log_2 \left(\frac{\pi \mathcal{E}_s}{4N_0} N^2 \Omega \right) - \frac{0.3944}{N} - \frac{4.24}{N^2} - \log_2 \left(1 + \frac{N\mathcal{E}_s}{N_0} \Delta \right) \Bigg]^+. \tag{12}$$

for identically distributed channels.

Proof: We know that, for memoryless AWGN channels, the achievable secrecy rate can be expressed in terms of the achievable rates over the main and the wiretap channels as [21]

$$R_s = [R_m - R_e]^+. \tag{13}$$

Therefore, (12) can be obtained by plugging the expressions for R_m and R_e into (13). ∎

Note that the argument inside the logarithm of the first term of (12) scales as N^2, and that of the third term scales linearly with N. Therefore, for large enough N, DCP can ensure secure communication at a nonzero rate between the SNs and the FC even when the channels from the SNs to the FC are weaker than the channels from the SNs to the EVE.Under high SNR, we can approximate the lower bound on the achievable ergodic secrecy rate for identically distributed channels as

$$R_s \approx \eta_p \left[\log_2 \left(N \frac{\pi}{4} \frac{\Omega}{\Delta} \right) - \frac{0.3944}{N} - \frac{4.24}{N^2} \right]^+. \tag{14}$$

In other words, as the SNR increases, the secure communication rate saturates to a value that depends only on the number of SNs participating in the DCP, and is independent of the SNR.

B. Practical DCP

In practice, the SNs need to estimate the CSI using pilot symbols transmitted by the FC. In this section, we analyze the effect of channel estimation errors on the secrecy rates of DCP systems. The actual channel from the ith SN to the FC, $a_{1,i}$, can be expressed in terms of its MMSE estimate at the SN, $\hat{a}_{1,i}$, as

$$a_{1,i} = \sqrt{\frac{\xi\Omega_{1,i}}{1 + \xi\Omega_{1,i}}} \hat{a}_{1,i} + \sqrt{\frac{\Omega_{1,i}}{1 + \xi\Omega_{1,i}}} \tilde{a}_{1,i} \tag{15}$$

where $\xi = \frac{M_p \mathcal{E}_p}{N_0}$ is the pilot SNR, and $\tilde{a}_{1,i} \sim \mathcal{CN}(0,1)$, such that $E[\hat{a}_{1,i}\tilde{a}_{1,i}^*] = 0$ due to the MMSE estimation. Here it is important to note that this decomposition is applicable only for ZMCSCG rvs.

In this case, we present lower bounds on the achievable rate over the main channel, and on the achievable secrecy rate, as Lemma 3 and Theorem 2, respectively.

Lemma 3. *The achievable rate over the main channel*

for practical DCP is bounded as

$$R_m \geq \eta_p \left(\log_2 \left(\frac{\pi \mathcal{E}_s}{4N_0} \sum_{i,k=1}^{N} \sqrt{\frac{\xi \Omega_{1,i}^2}{1+\xi\Omega_{1,i}} \frac{\xi \Omega_{1,k}^2}{1+\xi\Omega_{1,k}}} \right) - \frac{1}{N} \left(2E[\bar{\psi}] - \frac{E[\bar{\psi}^2]}{2} - \frac{3}{2} \right) \right), \quad (16)$$

$$R_m \geq \eta_p \left(\log_2 \left(\frac{N^2 \mathcal{E}_s}{N_0} \frac{\pi}{4} \frac{\xi \Omega^2}{1+\xi\Omega} \right) - \frac{0.3944}{N} - \frac{4.24}{N^2} \right) \quad (17)$$

for independent and non-identically distributed (i.n.d.) and i.i.d. channels, respectively.

Proof: See Appendix C ∎

Since the channels between the EVE and the SNs are independent of the CSI at the SNs, the channel statistics for the the EVE's channel remain unaltered under practical DCP.

Theorem 2. *The ergodic secrecy rates for DCP based on estimated channels can be approximated as*

$$R_s \geq \eta_p \left[\log_2 \left(\frac{\pi \mathcal{E}_s}{4N_0} \sum_{i,k=1}^{N} \sqrt{\frac{\xi \Omega_{1,i}^2}{1+\xi\Omega_{1,i}} \frac{\xi \Omega_{1,k}^2}{1+\xi\Omega_{1,k}}} \right) - \left(2E[\bar{\psi}] + E[\bar{\psi}^2] - \frac{3}{2} \right) - \log_2 \left(1 + \frac{\mathcal{E}_s}{N_0} \sum_{i=1}^{N} \Delta_{1,i} \right) \right]^+, \quad (18)$$

and

$$R_s \geq \eta_p \left[\log_2 \left(\frac{\pi N^2 \mathcal{E}_s}{4N_0} \frac{\xi \Omega^2}{1+\xi\Omega} \right) - \frac{0.3944}{N} - \frac{4.24}{N^2} - \log_2 \left(1 + \frac{N\mathcal{E}_s}{N_0} \Delta \right) \right]^+ \eta_p, \quad (19)$$

for i.n.d. and i.i.d. channels, respectively.

At high SNR, the ergodic secrecy rate for i.i.d. channels can be approximated as

$$R_s \approx \eta_p \left[\log_2 \left(\frac{\pi}{4} \frac{N}{\Delta} \frac{\xi \Omega^2}{1+\xi\Omega} \right) - \frac{0.3944}{N} - \frac{4.24}{N^2} \right]^+. \quad (20)$$

Compared to the ideal DCP case in (14), we see that the effect of imperfect channel estimation at the SNs manifests as the $\xi\Omega/(1+\xi\Omega)$ term inside the logarithm. The loss in rate compared to (14) thus depends on the pilot SNR, ξ.

We next extend the above analysis to derive the achievable ergodic secrecy rates in the presence of L colluding eavesdroppers.

III. Single Stream DCP with L Colluding Eavesdroppers

The system model for the WSN in this case is the same as the one considered in Section II, consisting of N single antenna SNs communicating with a single antenna FC. However, there are now $L \geq 1$ colluding EVEs in proximity of the WSN with accurate information about the channels between themselves and the SNs. We also assume that the EVEs can share their observations over an error free communication channel, such that the EVE network can be viewed as a single EVE with L antennas.

Letting $b_{l,i} \sim \mathcal{CN}(0, \Delta_{l,i})$ be the channel between the lth EVE and the ith SN, the signal received at the lth EVE can be expressed as

$$z_l[n] = N\sqrt{\mathcal{E}_s} g_l s[n] + v_l[n] \quad (21)$$

with $v_l[n] \sim \mathcal{CN}(0, N_0)$ and $g_l \triangleq \frac{1}{N} \sum_{i=1}^{N} b_{l,i} e^{-j\hat{\theta}_{1,i}} \sim \mathcal{CN}\left(0, \frac{1}{N^2} \sum_{i=1}^{N} \Delta_{l,i}\right)$, as shown in Section II.

The achievable ergodic secrecy rate in this case can be lower bounded according to Theorem 3.

Theorem 3. *With L colluding eavesdroppers, the achievable ergodic secrecy rate under i.n.d. and i.i.d. channels can be lower bounded as*

$$R_s \geq \eta_p \left[\log_2 \left(\frac{\pi \mathcal{E}_s}{4N_0} \sum_{i,k=1}^{N} \sqrt{\frac{\xi \Omega_{1,i}^2}{1+\xi\Omega_{1,i}} \frac{\xi \Omega_{1,k}^2}{1+\xi\Omega_{1,k}}} \right) - \log_2 \left(1 + \frac{N\mathcal{E}_s}{N_0} L\Delta \right) - \left(2E[\bar{\psi}] + E[\bar{\psi}^2] - \frac{3}{2} \right) \right]^+ \quad (22)$$

and

$$R_s \geq \left[\log_2 \left(\frac{N^2 \mathcal{E}_s}{N_0} \frac{\pi}{4} \frac{\xi \Omega^2}{1+\xi\Omega} \right) - \frac{0.3944}{N} - \frac{4.24}{N^2} - \log_2 \left(1 + \frac{N\mathcal{E}_s}{N_0} L\Delta \right) \right]^+ \eta_p, \quad (23)$$

respectively.

Proof: The vector signal received by the EVEs is

$$\mathbf{z}[n] = N\sqrt{\mathcal{E}_s} \mathbf{g} s[n] + \mathbf{v}[n], \quad (24)$$

with $\mathbf{g} = [g_1, \ldots, g_L]^T$. The achievable ergodic rate of the wiretap channel can therefore be given as

$$\begin{aligned} R_e &= \eta_p E \left[\log_2 \left(1 + \frac{N^2 \mathcal{E}_s}{N_0} \|\mathbf{g}\|_2^2 \right) \right] \\ &\leq \eta_p \log_2 \left(1 + \frac{N^2 \mathcal{E}_s}{N_0} \sum_{l=1}^{L} E\left[|g_{l,i}|^2 \right] \right) \\ &= \eta_p \log_2 \left(1 + \frac{\mathcal{E}_s}{N_0} \sum_{i=1}^{N} \sum_{l=1}^{L} \Delta_{l,i} \right) \end{aligned} \quad (25)$$

Letting $\Delta = \frac{1}{NL}\sum_{i=1}^{N}\sum_{l=1}^{L}\Delta_{l,i}$, be the average eavesdropper channel power, we can write

$$R_e \leq \eta_p \log_2\left(1 + NL\Delta\frac{\mathcal{E}_s}{N_0}\right). \tag{26}$$

Substituting this in (11) and (12) completes the proof. ∎

Under high data SNRs, this can be approximated as

$$R_s \approx \eta_p\left[\log_2\left(\frac{N}{L}\frac{\Omega}{\Delta}\frac{\pi}{4}\frac{\xi\Omega}{1+\xi\Omega}\right) - \frac{0.3944}{N} - \frac{4.24}{N^2}\right]^+. \tag{27}$$

Thus, L colluding eavesdroppers can reduce the achievable secrecy rate of a DCP system. We next analyze the performance of *multi-stream* DCP in the presence of L colluding eavesdroppers. Multi-stream DCP is possible when the FC is equipped with $K > 1$ antennas.

IV. Secrecy rate of Conventional Multi-stream DCP

A. System Model

We consider N single antenna SNs reporting to an FC equipped with K receive antennas. Each SN simultaneously transmits data over K streams with equal power. It is assumed that there are L colluding EVEs, having accurate CSI for all the channels from the SNs. We also assume that all the channels remain static over one DCP frame duration comprising M channel uses. During the first KM_p channel uses, the FC transmits M_p pilot symbols from each of its K antennas. These pilots are used by the SNs to estimate the channels to the respective FC antennas. Following this, the SNs simultaneously transmit K streams of data to each of the FC antennas during the next $M_d = M - KM_p$ channel uses.

Letting $a_{k,i} = \alpha_{k,i}e^{j\theta_{k,i}} \sim \mathcal{CN}(0, \Omega_{ki})$ denote the channel between the kth FC antenna and the ith SN, the signal received at the ith SN during the nth training instant ($n \in \{(k-1)M_p + 1, \ldots, kM_p\}$) is

$$q_i[n] = a_{k,i}\sqrt{\mathcal{E}_p} + w_i[n] = \alpha_{k,i}e^{j\theta_{k,i}}\sqrt{\mathcal{E}_p} + w_i[n] \tag{28}$$

with $w_i[n] \sim \mathcal{CN}(0,1)$ being the ZMCSCG AWGN at the ith SN. The MMSE estimate of the channel coefficient between the ith SN and the kth FC antenna is computed at the ith SN as

$$\hat{a}_{k,i} = \frac{\sqrt{M_p\mathcal{E}_p\Omega_{ki}}}{N_0 + M_p\mathcal{E}_p\Omega_{ki}}\sum_{n=(k-1)M_p+1}^{kM_p} q_i[n]. \tag{29}$$

This is used to obtain the gain and phase estimates for the corresponding channel as $\hat{\alpha}_{k,i} = |\hat{a}_{k,i}|$ and

$$\hat{\theta}_{k,i} = \tan^{-1}\left(\frac{\Im\{\hat{a}_{k,i}\}}{\Re\{\hat{a}_{k,i}\}}\right), \tag{30}$$

respectively. Compensating for the estimated phase to each of the FC antennas, the ith SN then transmits the symbol $x_i[n]$ given as

$$x_i[n] = \sqrt{\frac{\mathcal{E}_s}{K}}\sum_{k=1}^{K} s_k[n]e^{-j\hat{\theta}_{k,i}},\ n = KM_p + 1, \ldots, M, \tag{31}$$

Note that the transmit energy is normalized w.r.t. the number of streams being used. In the following subsections, we discuss the received signal model and the achievable ergodic secrecy rates for the ideal and practical DCP cases.

B. Ergodic Secrecy Rate with Ideal DCP

We first calculate the ergodic secrecy achievable rate over the main channel, for which the signal received by the kth FC antenna is

$$\begin{aligned} y_k[n] &= \sum_{i=1}^{N} a_{k,i}x_i[n] + w_k[n] \\ &= \sqrt{\frac{\mathcal{E}_s}{K}}\sum_{m=1}^{K} s_m[n]\sum_{i=1}^{N}\alpha_{k,i}e^{j(\theta_{k,i}-\theta_{m,i})} + w_k[n]. \end{aligned} \tag{32}$$

Letting $h_{km} = \frac{1}{N}\sum_{i=1}^{N}\alpha_{k,i}e^{j(\theta_{k,i}-\theta_{m,i})}$ denote the effective channel coefficient between the kth FC antenna and the mth stream of data, we can write (32) as

$$\begin{aligned} y_k[n] &= N\sqrt{\frac{\mathcal{E}_s}{K}}h_{kk}s_k[n] \\ &\quad + N\sqrt{\frac{\mathcal{E}_s}{K}}\sum_{m=1;m\neq k}^{K} h_{km}s_m[n] + w_k[n]. \end{aligned} \tag{33}$$

Equivalently, the vector signal received at the FC, $\mathbf{y}[n] \triangleq [y_1[n], y_2[n], \ldots, y_K[n]]^T$, can be written as

$$\mathbf{y}[n] = N\mathbf{H}\mathbf{s}[n] + \mathbf{w}[n], \tag{34}$$

where $\mathbf{H}$ is the effective channel matrix with its (k,m)th entry equal to h_{km}, and $\mathbf{s}[n] \triangleq [s_1[n], s_2[n], \ldots, s_K[n]]^T$ is the data vector. Assuming the data across different streams to be independent, i.e., $E[\mathbf{s}[n]\mathbf{s}^H[n]] = \mathbf{I}_K$, the ergodic achievable rate over the main channel is given by [33]

$$R_m = \eta_{p,K}E_{\mathbf{H}}\left[\log_2\left(\det\left(\mathbf{I}_K + \frac{N^2\mathcal{E}_s}{KN_0}\mathbf{H}^H\mathbf{H}\right)\right)\right], \tag{35}$$

with $\eta_{p,K} = \left(\frac{M-KM_p}{M}\right)$. A lower bound on (35) can be obtained using Lemma 4.

Lemma 4. *The achievable rate over the main channel can be lower bounded as*

$$R_m \geq \eta_{p,K}\left(\sum_{k=1}^{K}\log_2\left(\frac{\pi\mathcal{E}_s}{4KN_0}\sum_{i,m=1}^{N}\sqrt{\Omega_{ki}\Omega_{km}}\right) + E\left[\log_2\left(\det\left(\boldsymbol{\Psi}\right)\right)\right]\right). \quad (36)$$

where

$$\boldsymbol{\Psi} \triangleq \mathbf{D}^{-1}\mathbf{H}^H\mathbf{H}. \quad (37)$$

and

$$\mathbf{D} = \frac{\pi}{4N^2}diag\left(\left[\sum_{i,m=1}^{N}\sqrt{\Omega_{ki}\Omega_{km}}\right]_{k=1}^{K}\right), \quad (38)$$

Proof: See Appendix D ∎

Now, the diagonal entries of $\mathbf{H}$ correspond to weighted sums of Rayleigh random variables, and the off-diagonal entries correspond to ZMCSCG random variables. Therefore, it is not possible to determine the distribution of $\log_2\left(\det(\boldsymbol{\Psi})\right)$ in closed form. Hence, this term is evaluated for i.i.d. channels using Monte Carlo simulations as

$$E\left[\log_2\left(\det\left(\boldsymbol{\Psi}\right)\right)\right] \approx -\frac{1}{N}\left(2.2K^2 - 1.8K\right) \quad (39)$$

It is observed that the variances of both the diagonal and off-diagonal entries of $\mathbf{H}$ decay as $\frac{1}{N}$, and therefore the entries of $\mathbf{H}$ concentrate around their expected values as N increases, resulting in the functions of $\mathbf{H}$, $\boldsymbol{\Psi}$ and $\log_2\left(\det\left(\boldsymbol{\Psi}\right)\right)$ concentrating around their means. This is evident in the behavior of the simulated lower bound on $\log_2\left(\det\left(\boldsymbol{\Psi}\right)\right)$. Therefore, the achievable rate over the main channel, for i.i.d. channels can be evaluated as

$$R_m \geq K\eta_{p,K}\left(\log_2\left(\frac{N^2\mathcal{E}_s}{KN_0}\frac{\pi}{4}\Omega\right) - \frac{1}{N}\left(2.2K - 1.8\right)\right). \quad (40)$$

A comparison of the behavior of the achievable rates over the main channel with the derived bound for different values of K and N for $\frac{\mathcal{E}_s}{N_0} = 1$ is plotted in Fig. 1. The plot illustrates that the achievable rate increases linearly in K and logarithmically in N, as expected from (40). It is also interesting that for $K = 1$ and moderately large values of N, this bound closely approximates the bound derived for the single stream case.

Considering the EVE's channel, we can write the received signal at the lth EVE antenna as

$$z_l[n] = N\sqrt{\frac{\mathcal{E}_s}{K}}\sum_{k=1}^{K}g_{lk}s_k[n] + v_l[n] \quad (41)$$

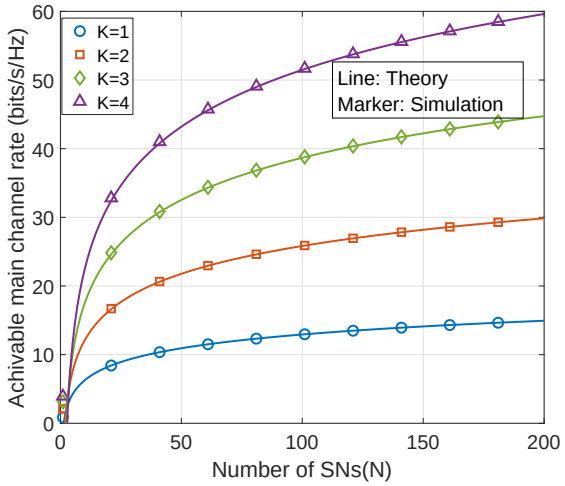

Fig. 1. The Achievable data rates for the main multi-stream DCP channel for different numbers of SNs and FC antennas

where $g_{lk} \triangleq \frac{1}{N}\sum_{i=1}^{N}b_{l,i}e^{-j\theta_{k,i}}$ is ZMCSCG with $E[|g_{lk}|^2] = \frac{1}{N^2}\sum_{i=1}^{N}\Delta_{li}$.

The signal received at the EVE's channel can be written as

$$\mathbf{z}[n] = N\sqrt{\frac{\mathcal{E}_s}{K}}\mathbf{G}\mathbf{s}[n] + \mathbf{v}[n], \quad (42)$$

where $\mathbf{G}$ denotes the effective channel with (l,k)th entry g_{lk}. Lemma 5 presents an upper bound on the achievable rate over the channel described in (42).

Lemma 5. *The achievable rate over the EVE's channel can be upper bounded as*

$$R_e \leq K\log_2\left(1 + \frac{NL\mathcal{E}_s\Delta}{KN_0}\right), \quad (43)$$

where $\Delta \triangleq \frac{1}{NL}\sum_{l=1}^{L}\sum_{i=1}^{N}\Delta_{li}$.

Proof: See Appendix E ∎

Theorem 4. *The achievable ergodic secrecy rate for multi-stream DCP with perfect CSI at the SNs, and a K antenna FC is given by*

$$R_s \geq \eta_{p,K}\left[K\left(\log_2\left(\frac{N^2\mathcal{E}_s}{KN_0}\frac{\pi}{4}\Omega\right) - \log_2\left(1 + \frac{N\mathcal{E}_s}{KN_0}L\Delta\right) - \frac{1}{N}\left(2.2K - 1.8\right)\right)\right]^+. \quad (44)$$

Under high SNRs, this can be approximated as

$$R_s \approx \eta_{p,K}\left[K\left(\log_2\left(\frac{\Omega}{\Delta}\frac{N}{L}\frac{\pi}{4}\right) - \frac{1}{N}\left(2.2K - 1.8\right)\right)\right]^+. \quad (45)$$

Therefore, multi-stream DCP with K FC antennas can achieve is approximately K times the ergodic secrecy achievable rate by single stream DCP in the presence of the same number of eavesdroppers.

C. Ergodic Secrecy Rate with Estimated Channels

The channel coefficient between the kth antenna at the FC and the ith SN is given as

$$a_{k,i} = \sqrt{\frac{\xi\Omega_{ki}}{1+\xi\Omega_{ki}}}\hat{\alpha}_{ki}e^{j(\hat{\theta}_{ki})} + \sqrt{\frac{\Omega_{ki}}{1+\xi\Omega_{ki}}}\tilde{a}_{ki} \quad (46)$$

with $\tilde{a}_{ki} \sim \mathcal{CN}(0,1)$. The signal received at the kth FC antenna is therefore given as

$$y_k[n] = N\sqrt{\frac{\mathcal{E}_s}{K}}\bar{h}_{kk}s_k[n] + N\sqrt{\frac{\mathcal{E}_s}{K}}\sum_{\substack{m=1\\m\neq k}}^{K}\bar{h}_{km}s_m[n] + w_k[n], \quad (47)$$

where $\hat{h}_{kk} = \frac{1}{N}\sum_{i=1}^{N}\sqrt{\frac{\xi\Omega_{ki}}{1+\xi\Omega_{ki}}}\hat{\alpha}_{ki}$, $\tilde{h}_{kk} = \frac{1}{N}\sum_{i=1}^{N}\sqrt{\frac{\Omega_{ki}}{1+\xi\Omega_{ki}}}\tilde{a}_{ki}e^{-j\hat{\theta}_{ki}}$, $\bar{h}_{kk} = \hat{h}_{kk} + \tilde{h}_{kk}$ and $\bar{h}_{km} = \frac{1}{N}\sum_{i=1}^{N}a_{ki}e^{-j\hat{\theta}_{mi}}$, and equivalently, the received signal vector can be written as,

$$\mathbf{y}[n] = \sqrt{\frac{\mathcal{E}_s}{K}}\bar{\mathbf{H}}\mathbf{s}[n] + \mathbf{w}[n]. \quad (48)$$

The rate achievable over the channel described by (48) can be lower bounded using Lemma 6.

Lemma 6. *The achievable rate on the main channel is*

$$R_m \geq \eta_{p,K}\Bigg(E\left[\log_2\left(\det\left(\boldsymbol{\Psi}\right)\right)\right] + \sum_{k=1}^{K}\log_2\left(\frac{\pi\mathcal{E}_s}{4KN_0}\sum_{i,m=1}^{N}\sqrt{\frac{\Omega_{ki}^2}{1+\xi\Omega_{ki}}\frac{\Omega_{km}^2}{1+\xi\Omega_{km}}}\right)\Bigg) \quad (49)$$

for i.n.d. channels, and

$$R_m \geq K\eta_{p,K}\times \left(\log_2\left(\frac{N^2\mathcal{E}_s}{KN_0}\frac{\pi}{4}\frac{\Omega^2}{1+\xi\Omega}\right) - \frac{1}{N}\left(2.2K-1.8\right)\right). \quad (50)$$

for i.i.d. channels, with

$$\mathbf{D} = \frac{\pi}{4N^2}diag\left(\left[\sum_{i,m=1}^{N}\sqrt{\frac{\Omega_{ki}^2}{1+\xi\Omega_{ki}}\frac{\Omega_{km}^2}{1+\xi\Omega_{km}}}\right]_{k=1}^{K}\right) \quad (51)$$

and

$$\boldsymbol{\Psi} \triangleq \mathbf{D}^{-1}\bar{\mathbf{H}}^H\bar{\mathbf{H}} \quad (52)$$

Proof: See Appendix F ∎

Therefore, the achievable secrecy rate of multistream DCP under estimated channels can be lower bounded using Theorem 5.

Theorem 5. *The achievable ergodic secrecy rates for i.n.d and i.i.d. channels with practical multi-stream DCP are given by*

$$R_s \geq \eta_{p,K}\times \Bigg[\sum_{k=1}^{K}\log_2\left(\frac{\pi\mathcal{E}_s}{4KN_0}\sum_{i,m=1}^{N}\sqrt{\frac{\Omega_{ki}^2}{1+\xi\Omega_{ki}}\frac{\Omega_{km}^2}{1+\xi\Omega_{km}}}\right) + E\left[\log_2\left(\det\left(\boldsymbol{\Psi}\right)\right)\right] - K\log_2\left(1+\frac{N\mathcal{E}_s}{KN_0}L\Delta\right)\Bigg]^+ \quad (53)$$

and

$$R_s \geq K\eta_{p,K}\Bigg[\log_2\left(\frac{N^2\mathcal{E}_s}{KN_0}\frac{\pi}{4}\frac{\Omega^2}{1+\xi\Omega}\right) - \frac{1}{N}\left(2.2K-1.8\right) - \log_2\left(1+\frac{N\mathcal{E}_s}{KN_0}L\Delta\right)\Bigg]^+, \quad (54)$$

respectively.

Therefore, by using K antennas at the FC and transmitting K data streams, the achievable secrecy rate over a DCP channel can be scaled up approximately K times.

V. Multi-stream DCP with Constrained Maximal Ratio Transmission

In the previous section, we considered the case where each SN allocates equal power, $\mathcal{E}_s/K$, to each of the transmitted streams. However, from the initial training phase, the nodes have an estimate of the magnitude of the channel to each of the FC antennas. They can potentially use this knowledge to allot power across the K data streams, while meeting an overall transmit per-node power constraint, and thereby improve their data rates. In this section, we evaluate the achievable ergodic secrecy rates with maximal ratio transmission based power allocation across the streams.

We again consider N single antenna SNs reporting to a K antenna FC. If the average energy expended per symbol per node is $\mathcal{E}_s$, and the estimated channel gains at the ith SN are represented using the vector $\hat{\boldsymbol{\alpha}}_i = [\hat{\alpha}_{1i}, \ldots, \hat{\alpha}_{Ki}]^T$, then the energy allocated by the ith node for the kth stream is $\mathcal{E}_s\frac{\hat{\alpha}_{ki}^2}{\|\hat{\boldsymbol{\alpha}}_i\|_2^2}$. Therefore, the symbol transmitted by the ith node can be expressed as

$$x_i[n] = \sqrt{\mathcal{E}_s}\sum_{k=1}^{K}\frac{\hat{\alpha}_{ki}}{\|\hat{\boldsymbol{\alpha}}_i\|_2}s_k[n]e^{-j\hat{\theta}_{ki}}. \quad (55)$$

Note that, as in the previous sections, each SN still transmits its data with a total power $\mathcal{E}_s$ across the K streams. Here, we limit the discussion to the case of i.i.d. channels. The case of i.n.d. channels is analytically

intractable due to the form of the random variables involved, and is beyond the scope of this paper.

With ideal DCP, the signal received at the kth FC antenna is given by

$$y_k[n] = N\sqrt{\mathcal{E}_s}h_{kk}s_k[n]+N\sqrt{\mathcal{E}_s}\sum_{\substack{m=1\\m\neq k}}^{K} h_{km}s_m[n]+w_k[n] \tag{56}$$

where $h_{kk} = \frac{1}{N}\sum_{i=1}^{N}\frac{\alpha_{ki}^2}{\|\boldsymbol{\alpha}_i\|_2}$, $h_{km} = \frac{1}{N}\sum_{i=1}^{N}\frac{\alpha_{ki}\alpha_{mi}}{\|\boldsymbol{\alpha}_i\|_2}e^{j(\theta_{ki}-\theta_{mi})}$.

We can use Lemma 7 to lower bound the achievable rate over the main channel.

Lemma 7. *The achievable rate over the main channel can be lower bounded as*

$$R_m \geq \left(K\log_2\left(\frac{N^2\Omega\mathcal{E}_s}{N_0}\left(\frac{\Gamma(K+\frac{1}{2})}{\Gamma(K+1)}\right)^2\right) + \log_2(\det(\boldsymbol{\Psi}))\right)\eta_{p,K}, \tag{57}$$

where $\boldsymbol{\Psi} = \frac{1}{\Omega}\left(\frac{\Gamma(K+1)}{\Gamma(K+\frac{1}{2})}\right)^2\mathbf{H}^H\mathbf{H}$*, and* $\mathbf{H}$ *is the effective channel matrix with* (k,m)*th entry* h_{km}*.*

Proof: See Appendix G ∎

It is not possible to determine the distribution or the moments of $\log_2(\det(\boldsymbol{\Psi}))$ in closed form. Using Monte Carlo simulations similar to the previous section, we evaluate this term as

$$\log_2(\det(\boldsymbol{\Psi})) \geq -\frac{K-2}{2} - \frac{K}{N}(1.11K-1.28). \tag{58}$$

Therefore, the achievable rate over the main channel can be lower bounded as,

$$R_m \geq \eta_{p,K}\left(K\log_2\left(\frac{N^2\Omega\mathcal{E}_s}{N_0}\left(\frac{\Gamma(K+\frac{1}{2})}{\Gamma(K+1)}\right)^2\right) - \frac{K-2}{2} - \frac{K}{N}(1.11K-1.28)\right). \tag{59}$$

For the wiretap channel, the signal received by the lth EVE can be written as

$$z_l[n] = N\sqrt{\mathcal{E}_s}\sum_{m=1}^{K} g_{lm}s_m[n] + w_k[n] \tag{60}$$

with $g_{lm} = \frac{1}{N}\sum_{i=1}^{N}\frac{b_{li}\alpha_{mi}}{\|\boldsymbol{\alpha}_i\|_2}e^{j(-\theta_{mi})}$.

Lemma 8. *The achievable rate over the eavesdroppers channel with maximal ratio beam-forming is given as*

$$R_e \leq \eta_{p,K}K\log_2\left(1+\frac{NL}{K}\frac{\mathcal{E}_s}{N_0}\Delta\right). \tag{61}$$

Proof: $E[g_{lm}] = 0$, and $E[|g_{lm}|^2] = \frac{1}{N^2}\sum_{i=1}^{N}E[|b_{li}|^2]E\left[\frac{\alpha_{mi}^2}{\|\boldsymbol{\alpha}_i\|_2^2}\right]$. Since $\frac{\alpha_{mi}^2}{\|\boldsymbol{\alpha}_i\|_2^2}$ is a beta distributed random variable, $E\left[\frac{\alpha_{mi}^2}{\|\boldsymbol{\alpha}_i\|_2^2}\right] = \frac{1}{K}$, hence, $E[|g_{lm}|^2] = \frac{\Delta}{KN}$, where Δ is as defined earlier. ∎

Theorems 6 and 7 can be used to obtain bounds on the achievable secrecy rates with and without CSI estimation errors in this case.

Theorem 6. *The achievable secrecy rate for ideal DCP with maximal ratio transmission is*

$$R_s \geq \left[K\left(\log_2\left(\frac{N^2\Omega\mathcal{E}_s}{N_0}\left(\frac{\Gamma(K+\frac{1}{2})}{\Gamma(K+1)}\right)^2\right) - \frac{1}{N}(1.11K-1.28) - \log_2\left(1+\frac{NL}{K}\frac{\mathcal{E}_s}{N_0}\Delta\right)\right) - \frac{K-2}{2}\right]^+\eta_{p,K}. \tag{62}$$

Theorem 7. *The achievable secrecy rate for practical DCP with maximal ratio transmission is*

$$R_s \geq \left[K\left(\log_2\left(\frac{N^2\mathcal{E}_s}{N_0}\frac{\xi\Omega^2}{1+\xi\Omega}\left(\frac{\Gamma(K+\frac{1}{2})}{\Gamma(K+1)}\right)^2\right) - \frac{1}{N}(1.11K-1.28) - \log_2\left(1+\frac{NL}{K}\frac{\mathcal{E}_s}{N_0}\Delta\right)\right) - \frac{K-2}{2}\right]^+\eta_{p,K}. \tag{63}$$

VI. Securing Multi-Stream DCP using Added Artificial Noise

In the previous sections, we have considered the achievable secrecy rates of a DCP system that is unaware of the existence of eavesdroppers in the network. However, in case the presence of an eavesdropper is known, then the SNs can use additional physical layer security techniques with the transmitted data to further improve the achievable secrecy rates for the DCP channel. One such technique is the addition of artificial noise to the transmitted signal [34]–[36]. Here, the nodes transmit artificial noise using a fraction of the transmitted power, to reduce the achievable rate at the eavesdropper. It is conventional to assume that the artificial noise is transmitted in the null space of the effective channel matrix. This beam alignment is not possible for DCP due to the unavailability of receive degrees of freedom.

However, if the SNs generate and add independent noise samples to their transmitted signals using a fraction of the transmitted power, then the artificial noise does not have the same array gain as the intended signal, limiting its detrimental effects at the FC. Also, since the eavesdroppers do not achieve the DCP array gain, as discussed in the preceding sections, the use of artificial noise affects the eavesdroppers more than the FC. In this case, determining the fraction of power to be transmitted

as artificial noise becomes important. In this section, we determine the optimal fraction of power to be used for transmitting artificial noise for an i.i.d. channel. We omit the similar case of i.n.d. channels for brevity.

Now, in general, the achievable secrecy rate of a K stream MS-DCP system with L colluding eavesdroppers, without any artificial noise being added, can be expressed as

$$R_s \geq \eta_{p,K}\Bigg[K\left(\log_2\left(\lambda_m\frac{N^2\mathcal{E}_s}{KN_0}\Omega\right) - \log_2\left(1+\frac{NL}{K}\frac{\mathcal{E}_s}{N_0}\Delta\right)\right) - f_c(K)\Bigg]^+, \quad (64)$$

where λ_m is a scale factor depending on the scheme and channel conditions, and $f_c(K)$ is a function of the number of streams. Letting a fraction $1-\mu$ of the total power be allotted to artificial Gaussian noise, the signal transmitted by the ith SN at the nth instant can be written as

$$x_i[n] = \sqrt{\frac{\mu\mathcal{E}_s}{K}}\sum_{k=1}^{K} s_k[n]e^{-j\hat{\theta}_{k,i}} + \sqrt{(1-\mu)\mathcal{E}_s}\nu_i[n]. \quad (65)$$

where $\nu_i[n]$ is the artificial noise generated by the ith SN. It can be shown that achievable secrecy rate over the channel is given as,

$$R_s \geq \eta_{p,K}\Bigg[K\left(\log_2\left(\lambda_m\frac{N^2}{K}\frac{\mu\Omega\mathcal{E}_s}{(1-\mu)\Omega+N_0}\right) - f_c(K) - \log_2\left(1+\frac{NL}{K}\frac{\mu\Delta\mathcal{E}_s}{(1-\mu)\Delta\mathcal{E}_s+N_0}\right)\right)\Bigg]^+. \quad (66)$$

Since λ_m and $f_c(K)$ are independent of μ, the achievable secrecy rate can be maximized by maximizing the fraction

$$T(\mu) = \frac{\frac{\mu\Omega\mathcal{E}_s}{(1-\mu)\Omega\mathcal{E}_s+N_0}}{1+\frac{NL}{K}\frac{\mu\Delta\mathcal{E}_s}{(1-\mu)\Delta\mathcal{E}_s+N_0}}. \quad (67)$$

in terms of μ. It can be observed that for $N > L > K$ and $\Omega > \Delta$, this is a monotonically increasing function of μ, and is therefore maximized for $\mu = 1$. On the other hand, for $\Delta > \Omega$, it can be shown that the optimal μ can be obtained by solving the quadratic equation

$$p\mu^2 + q\mu + r = 0, \quad (68)$$

with $p = (\Omega\Delta\mathcal{E}_s^2 + \Omega\mathcal{E}_sN_0)\left(\left(\frac{NL}{K}-1\right)\Omega\Delta\mathcal{E}_s^2\right) - \Omega\Delta\mathcal{E}_s^2\left(\left(\frac{NL}{K}-2\right)\Omega\Delta\mathcal{E}_s^2 - \Omega\mathcal{E}_sN_0 + \left(\frac{NL}{K}-1\right)\Delta\mathcal{E}_sN_0\right)$, $q = 2\Omega\Delta\mathcal{E}_s^2(\Omega\Delta\mathcal{E}_s^2 + \Omega\mathcal{E}_sN_0 + \Delta\mathcal{E}_sN_0 + N_0^2)$, $r = (\Omega\Delta\mathcal{E}_s^2\Omega\mathcal{E}_sN_0)(\Omega\Delta\mathcal{E}_s^2 + \Omega\mathcal{E}_sN_0 + \Delta\mathcal{E}_sN_0 + N_0^2)$. Out of the two solutions of (68), the one satisfying $0 \leq \mu \leq 1$, optimizes the achievable secrecy rate of the DCP system in the presence of eavesdroppers.

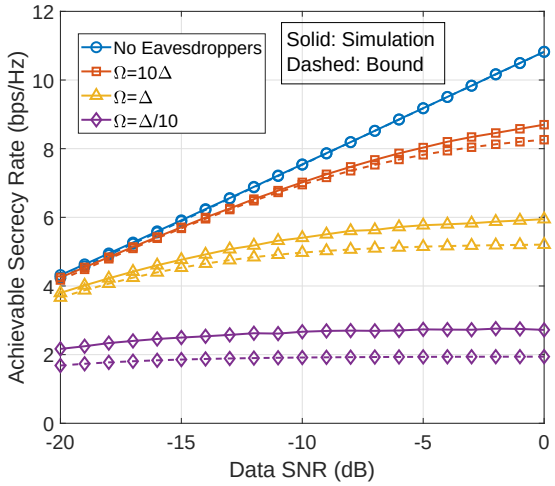

Fig. 2. Achievable secrecy rates for a single antenna, single eavesdropper system, with $N = 50$ SNs.

VII. Simulation Results

In this section, we substantiate the results derived in the previous sections using Monte Carlo simulation experiments. We also use these results to compare the secrecy rate performance of the different multi-stream DCP techniques discussed in the paper.

We assume that the FC transmits training symbols at an SNR of 10 dB, followed by data transmission from the SNs to the FC using DCP. We assume a frame length(M) of 100 channel uses and $M_p = 1$ pilot per stream. Simulations are then carried out for different values of data SNRs, number of eavesdroppers, etc. The achievable rate performances are obtained by averaging over $10,000$ independent channel realizations.

In Fig. 2, we plot the achievable secrecy rates for a single stream DCP system with $N = 50$ SNs in the presence of a single eavesdropper, against the per node SNR, for different ratios of Ω and Δ. It is observed that a DCP system is able to deliver nonnegative rates, even when the EVEs channel is 10 dB stronger than the main users' channel, and the simulated results closely follow the derived bounds.

In Fig. 3, we plot the achievable secrecy rates for a three stream ($K = 3$) DCP system with $N = 20$ against the number of eavesdroppers in the system, for different SNRs, such that $\Omega = 10\Delta$. The system performance is observed to decay with an increase in the number of eavesdroppers, under all cases, which is in accordance with the derived results. Again, the simulated results are observed to follow the derived bounds.

In Fig. 4, we plot the achievable secrecy rates for a multi-stream DCP system with different numbers of streams, in the presence of 10 eavesdroppers against the number of SNs for $\Omega = 10\Delta$ and a data SNR of 0 dB.

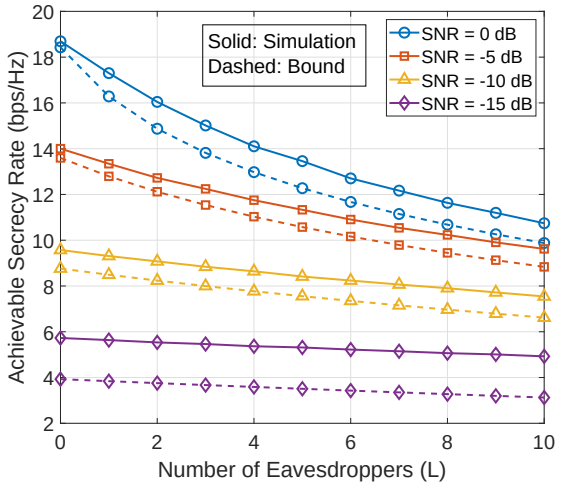

Fig. 3. Achievable secrecy rates for three stream DCP system for different numbers of eavesdroppers, with $N = 20$ SNs.

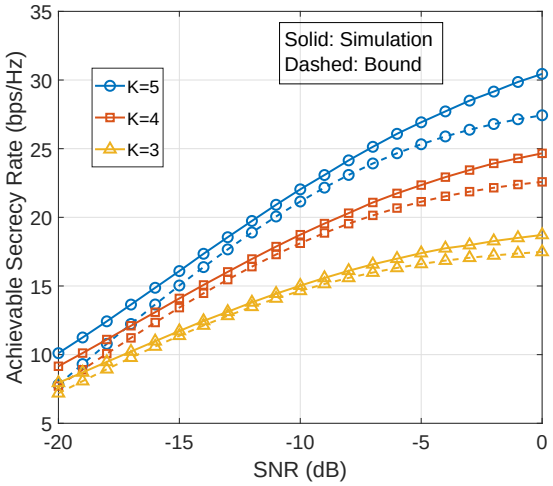

Fig. 5. Achievable secrecy rates for an MRT multi-stream DCP system for $N = 50$ and 5 eavesdroppers at different SNRs.

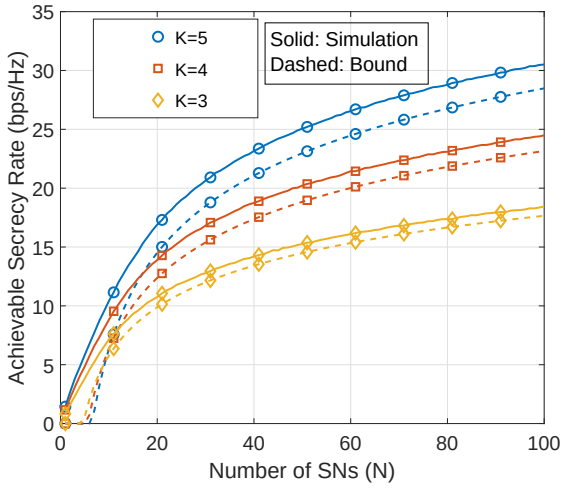

Fig. 4. Achievable secrecy rates for a multi-stream DCP system for different numbers of SNs at a data SNR of 0 dB, with 10 eavesdroppers and $\Omega = 10\Delta$.

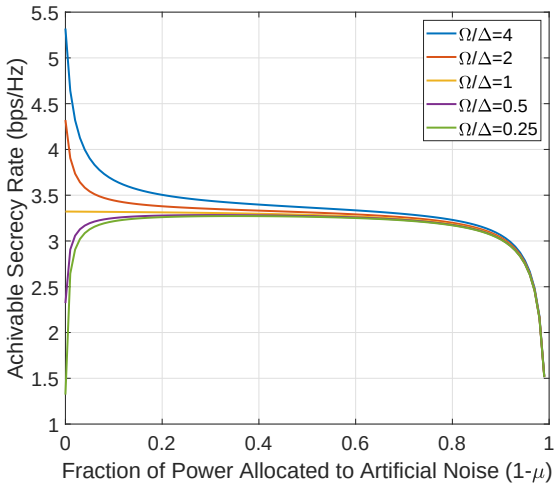

Fig. 6. Achievable secrecy rates for a single user two eavesdropper system for different amounts of added artificial noise.

The achievable secrecy rate is observed to increase with both the number of SNs, and the number of streams, which is as expected.

In Fig. 5, we plot the achievable secrecy rates for an MRT multi-stream DCP system with $N = 20$ SNs against the data SNR, for different number of streams in the presence of $L = 5$ eavesdroppers. The achievable secrecy rates grows almost linearly with the number of streams, as predicted by the derived bounds.

In Fig. 6, we illustrate the effect of adding artificial noise to a DCP system for enhancing physical layer security. We consider a single stream DCP system with $N = 20$ SNs, and $L = 2$ eavesdroppers. When the main channel is stronger than the eavesdroppers channel, the achievable secrecy rate shows a steep increase near $\mu = 1$, indicating that no artificial noise should be added to the system, which is as per the discussion in Section VI. It is also shown in the figure that the use of artificial noise is necessitated when the eavesdropper's channel is stronger than the main channel.

Thus, the simulation results illustrate that the use of DCP provides secure communication between a set of SNs and an FC, without the requirement of any additional signal processing at the SNs, when the main channel is stronger than the eavesdropper channel. It is also shown that the user of DCP enables a nonnegative secrecy rate between the SNs and the FC even when the eavesdropper channel is weaker than the main channel,

and in this case the achievable secrecy rate can be further improved by adding artificial noise to the signals transmitted by the SNs.

VIII. Conclusions

In this work, we showed that the DCP is inherently secure in the presence of eavesdroppers. Specifically, the SINR over the main channel increases as the square of the number of SNs N, while that for the eavesdropper channel increases linearly with N, leading to an achievable rate that grows as $\log N$. We extended the analysis to multi-stream DCP, and showed that the secrecy rates increases roughly linearly with the number of streams. We then considered the secrecy performance of multi-stream DCP with constrained maximal ratio transmission, and showed that this can further improve the secrecy rates achievable by mutlistream DCP. We also studied the effect of adding artificial noise. We found that artificial noise can improve the secrecy rates of a DCP system if the eavesdroppers' channel is stronger than the main channel. Finally, via simulation experiments, we illustrated that the simulated achievable rates closely follow the derived bounds.

Appendix A
Proof of Lemma 1

From (5) we note that,

$$E[h_1] = \frac{1}{N}\sum_{i=1}^{N}\sqrt{\frac{\pi}{4}\Omega_{1,i}}, \tag{69}$$

$$\text{var}(h_1) = \frac{1}{N^2}\left(1-\frac{\pi}{4}\right)\sum_{i=1}^{N}\Omega_{1,i}, \tag{70}$$

when the channels are non identically distributed and $E[h_1] = \sqrt{\frac{\pi}{4}\bar{\Omega}}$; $\text{var}(h_1) = \left(1-\frac{\pi}{4}\right)\frac{\bar{\Omega}}{N}$, when the channels are identically distributed.

The ergodic achievable rate over the main channel under the assumptions of the channel being memoryless, and the additive noise being Gaussian, can be calculated as [33], [37]

$$\begin{aligned} R_m &= \left(\frac{M-M_p}{M}\right) E_{h_1}\left[\log_2\left(1+\frac{N^2\mathcal{E}_s}{N_0}|h_1|^2\right)\right] \\ &\geq \left(\frac{M-M_p}{M}\right) E_{h_1}\left[\log_2\left(\frac{N^2\mathcal{E}_s}{N_0}|h_1|^2\right)\right]. \end{aligned} \tag{71}$$

Defining $\psi \triangleq \frac{4N^2}{\pi\sum_{i=1}^{N}\sum_{m=1}^{N}\sqrt{\Omega_{1,i}\Omega_{m,i}}}|h_1|^2$,

$$\begin{aligned} R_m \geq \left(\frac{M-M_p}{M}\right) \times \\ \left(\log_2\left(\frac{\pi}{4}\frac{\mathcal{E}_s}{N_0}\sum_{i=1}^{N}\sum_{m=1}^{N}\sqrt{\Omega_{1,i}\Omega_{m,i}}\right) + E[\log_2(\psi)]\right). \end{aligned} \tag{72}$$

Since ψ is the square of a weighted combination of Rayleigh random variables its distribution is not obtainable in a closed form for $N > 2$. Therefore, the term $E[\log_2(\psi)]$ cannot be computed in a closed form. However, since $\log_2(\psi) \geq \log_2(e)\left((\psi-1)-\frac{(\psi-1)^2}{2}\right)$,

$$E[\log_2(\psi)] \geq \log_2(e)\left(2E[\psi] - \frac{E[\psi^2]}{2} - \frac{3}{2}\right). \tag{73}$$

Now,

$$E[\psi] = \frac{4N^2}{\pi\sum_{i=1}^{N}\sum_{m=1}^{N}\sqrt{\Omega_{1,i}\Omega_{m,i}}}E[|h_1|^2] \tag{74}$$

and

$$E[\psi^2] = \frac{16N^4}{\pi^2\left(\sum_{i=1}^{N}\sum_{m=1}^{N}\sqrt{\Omega_{1,i}\Omega_{m,i}}\right)^2}E[|h_1|^4] \tag{75}$$

that can be simplified to (8) and (9) respectively. For identically distributed channels, these can further be simplified as, $E[\psi] = 1 + \frac{1}{N}\left(\frac{4}{\pi}-1\right)$ and

$$\begin{aligned} E[\psi^2] = \left(1+\frac{1}{N}\left(\frac{24}{\pi}-6\right)+\frac{1}{N^2}\left(29-\frac{72}{\pi}+\frac{24}{\pi^2}\right)\right. \\ \left.-\frac{1}{N^3}\left(24-\frac{48}{\pi}-\frac{48}{\pi^2}\right)\right). \end{aligned} \tag{76}$$

Consequently,

$$\begin{aligned} E[\log_2(\psi)] \geq \frac{-1}{N}\log_2(e)\left(\frac{4}{\pi}-1\right) \\ -\frac{1}{N^2}\log_2(e)\left(29-\frac{72}{\pi}+\frac{24}{\pi^2}\right) \approx \frac{-0.3944}{N} - \frac{4.24}{N^2}. \end{aligned} \tag{77}$$

Appendix B
Proof of Lemma 2

By the definition of g_1,

$$E[|g_1|^2] = \frac{1}{N^2}\sum_{i=1}^{N}E[b_{1,i}^2] = \frac{1}{N^2}\sum_{i=1}^{N}\Delta_{1,i}. \tag{78}$$

Defining $\Delta \triangleq \frac{1}{N}\sum_{i=1}^{N}\Delta_{1,i}$, we have $g_1 \sim \mathcal{CN}\left(0, \frac{\Delta}{N}\right)$, and the ergodic achievable rate of EVE's channel can be calculated as [33]

$$R_e = \left(\frac{M-M_p}{M}\right) E_{g_1}\left[\log_2\left(1+\frac{N^2\mathcal{E}_s}{N_0}|g_1|^2\right)\right]. \tag{79}$$

Using Jensen's inequality [37], we get

$$R_e \leq \left(\frac{M-M_p}{M}\right)\log_2\left(1+\frac{N^2\mathcal{E}_s}{N_0}E[|g_1|^2]\right), \tag{80}$$

leading to (10).

APPENDIX C
PROOF OF LEMMA 3

The signal received at the FC can be written as

$$y[n] = N\sqrt{\mathcal{E}_s}\hat{h}_1 s[n] + N\sqrt{\mathcal{E}_s}\tilde{h}_1 s[n] + w[n], \quad (81)$$

where $\hat{h}_1 = \frac{1}{N}\sum_{i=1}^{N}\sqrt{\frac{\xi\Omega_{1,i}}{1+\xi\Omega_{1,i}}}\hat{\alpha}_{1,i}$ and $\tilde{h}_1 = \frac{1}{N}\sum_{i=1}^{N}\sqrt{\frac{\Omega_{1,i}}{1+\xi\Omega_{1,i}}}\tilde{a}_{1,i}e^{-j\hat{\theta}_{1,i}}$.

Now, $E[\tilde{h}_1] = 0$, $E[|\tilde{h}_1|^2] = \frac{1}{N^2}\sum_{i=1}^{N}\frac{\Omega_{1,i}}{1+\xi\Omega_{1,i}}$, $E[\hat{h}_1] = \frac{1}{N}\sum_{i=1}^{N}\sqrt{\frac{\pi}{4}}\sqrt{\frac{\xi\Omega_{1,i}^2}{1+\xi\Omega_{1,i}}}$, and

$$E[|\hat{h}_1|^2] = \frac{1}{N^2}\sum_{i=1}^{N}\frac{\xi\Omega_{1,i}^2}{1+\xi\Omega_{1,i}} + \frac{\pi}{4N^2}\sum_{i=1}^{N}\sum_{k=1;k\neq i}^{N}\sqrt{\frac{\xi\Omega_{1,i}^2}{1+\xi\Omega_{1,i}}}\sqrt{\frac{\xi\Omega_{1,k}^2}{1+\xi\Omega_{1,k}}} \quad (82)$$

for non identically distributed channels. When the channels are i.i.d.,

$$E[\hat{h}_1] = \sqrt{\frac{\pi}{4}}\sqrt{\frac{\xi\Omega^2}{1+\xi\Omega}}, \quad (83)$$

$$E[|\hat{h}_1|^2] = \left(\frac{1}{N} + \frac{\pi}{4}\frac{N-1}{N}\right)\frac{\xi\Omega^2}{1+\xi\Omega}. \quad (84)$$

At the FC, an accurate estimate of the effective DCP channel $\bar{h}_1 = \hat{h}_1 + \tilde{h}_1$ is required for data decoding. Using the fact that the $\bar{h}_1$ has a positive real part with high probability, it has been shown in [16] that it can be accurately estimated at the FC using the data symbols transmitted by the SNs. That is, the channel estimation at the FC is blind, i.e., it does not require transmission of pilot symbols from the SNs. Defining

$$\bar{\psi} = \frac{4}{\pi}\frac{N^2}{\sum_{i=1}^{N}\sum_{k=1}^{N}\sqrt{\frac{\xi\Omega_{1,i}^2}{1+\xi\Omega_{1,i}}}\sqrt{\frac{\xi\Omega_{1,k}^2}{1+\xi\Omega_{1,k}}}}|\bar{h}|^2, \quad (85)$$

we can use an approach similar to the one discussed in Appendix A to obtain (16) and (17).

APPENDIX D
PROOF OF LEMMA 4

The diagonal and off diagonal entries of $\mathbf{H}$ follow different distributions, and their individual statistics are required to evaluate (35). Looking at diagonal entries first, we have

$$h_{kk} = \frac{1}{N}\sum_{i=1}^{N}\alpha_{k,i}, \quad (86)$$

consequently,

$$E[h_{kk}] = \frac{1}{N}\sum_{i=1}^{N}\sqrt{\frac{\pi}{4}\Omega_{ki}}, \quad (87)$$

$$E[h_{kk}^2] = \frac{1}{N^2}\sum_{i=1}^{N}\Omega_{ki} + \frac{\pi}{4N^2}\sum_{i=1}^{N}\sum_{m=1;m\neq i}^{N}\sqrt{\Omega_{km}\Omega_{ki}}, \quad (88)$$

and

$$\text{var}(h_{kk}) = \frac{1}{N^2}\left(1-\frac{\pi}{4}\right)\sum_{i=1}^{N}\Omega_{ki} \quad (89)$$

for i.n.d. channels, and

$$E[h_{kk}] = \sqrt{\frac{\pi}{4}\Omega}, \quad (90)$$

$$E[h_{kk}^2] = \frac{\pi}{4}\Omega + \frac{1}{N}\left(1-\frac{\pi}{4}\right)\Omega, \quad (91)$$

and

$$\text{var}(h_{kk}) = \frac{1}{N}\left(1-\frac{\pi}{4}\right)\Omega \quad (92)$$

for i.i.d. channels.

Also, the off-diagonal entries of $\mathbf{H}$, h_{km}, $k \neq m$, are the sum of ZMCSCG r.v.s and therefore are ZMCSCG, such that, $E[|h_{k,m}|^2] = \frac{1}{N}\sum_{i=1}^{N^2}\Omega_{ki}$, for i.n.d. channels, and $E[|h_{km}|^2] = \frac{1}{N}\Omega$. for i.i.d. channels.

Since the matrix $\mathbf{H}^H\mathbf{H}$ is positive semidefinite, we can lower bound (35) as,

$$R_m \geq \left(\frac{M-KM_p}{M}\right)E\left[\log_2\left(\det\left(\frac{N^2\mathcal{E}_s}{KN_0}\mathbf{H}^H\mathbf{H}\right)\right)\right]. \quad (93)$$

Defining the matrices, $\boldsymbol{\Psi}$ and $\mathbf{D}$ as (37) and (38), we can write

$$R_m \geq \left(\frac{M-KM_p}{M}\right)\times \left(\log_2\left(\det\left(\frac{N^2\mathcal{E}_s}{KN_0}\mathbf{D}\right)\right) + E\left[\log_2\left(\det\left(\boldsymbol{\Psi}\right)\right)\right]\right). \quad (94)$$

This can be simplified as (36).

APPENDIX E
PROOF OF LEMMA 5

The vector signal received across all the eavesdroppers is $\mathbf{z}[n] = N\sqrt{\frac{\mathcal{E}_s}{K}}\mathbf{G}\mathbf{s}[n] + \mathbf{v}[n]$, where $\mathbf{G}$ denotes the effective channel with (l,k)th entry g_{lk}. The achievable rate over the EVEs' channel becomes [33]

$$\begin{aligned} R_e &= E\left[\log_2\left(\det\left(\mathbf{I}_K + \frac{N^2\mathcal{E}_s}{KN_0}\mathbf{G}^H\mathbf{G}\right)\right)\right] \\ &\overset{(a)}{\leq} E\left[\sum_{k=1}^{K}\log_2\left(1+\frac{N^2\mathcal{E}_s}{KN_0}\|\mathbf{g}_k\|^2\right)\right] \\ &\overset{(b)}{\leq} \sum_{k=1}^{K}\log_2\left(1+\frac{N^2\mathcal{E}_s}{KN_0}E\left[\|\mathbf{g}_k\|^2\right]\right) \\ &= \sum_{k=1}^{K}\log_2\left(1+\frac{\mathcal{E}_s}{KN_0}\sum_{l=1}^{L}\sum_{i=1}^{N}\Delta_{li}\right) \\ &= K\log_2\left(1+\frac{NL\mathcal{E}_s\Delta}{KN_0}\right). \end{aligned} \quad (95)$$

In the above, inequality (a) is the result of the upper bound on the $\log\det(.)$ function [38], and the inequality (b) is due to Jensen's inequality [37].

APPENDIX F
PROOF OF LEMMA 6

It can be shown that

$$E[\hat{h}_{kk}] = \frac{1}{N}\sum_{i=1}^{N}\sqrt{\frac{\pi}{4}\Omega_{ki}}\sqrt{\frac{\xi\Omega_{ki}}{1+\xi\Omega_{ki}}}, \tag{96}$$

$$E[|\hat{h}_{kk}|^2] = \frac{1}{N}\sum_{i=1}^{N}\frac{\xi\Omega_{ki}^2}{1+\xi\Omega_{ki}} + \frac{\pi}{4N^2}\sum_{i=1}^{N}\sum_{m=1;m\neq i}^{N}\sqrt{\frac{\xi\Omega_{ki}^2}{1+\xi\Omega_{ki}}}\sqrt{\frac{\xi\Omega_{km}^2}{1+\xi\Omega_{km}}}, \tag{97}$$

$$E[\tilde{h}_{kk}] = 0,\ E[|\tilde{h}|^2] = \frac{1}{N^2}\sum_{i=1}^{N}\frac{\Omega_{ki}}{1+\xi\Omega_{ki}}. \tag{98}$$

Therefore,

$$E[\bar{h}_{kk}] = \frac{1}{N}\sum_{i=1}^{N}\sqrt{\frac{\pi}{4}\frac{\xi\Omega_{k,i}^2}{1+\xi\Omega_{ki}}}, \tag{99}$$

$$E[|\bar{h}_{kk}|^2] = \frac{1}{N^2}\sum_{i=1}^{N}\Omega_{ki} + \frac{\pi}{4N^2}\sum_{i=1}^{N}\sum_{m=1;m\neq i}^{N}\sqrt{\frac{\xi\Omega_{ki}^2}{1+\xi\Omega_{ki}}}\sqrt{\frac{\xi\Omega_{km}^2}{1+\xi\Omega_{km}}} \tag{100}$$

for i.n.d. channels, and

$$E[\bar{h}_{kk}] = \sqrt{\frac{\pi}{4}\frac{\xi\Omega^2}{1+\xi\Omega}}, \tag{101}$$

$$E[|\bar{h}_{kk}|^2] = \frac{\Omega}{N} + \frac{\pi}{4}\frac{N-1}{N}\frac{\xi\Omega^2}{1+\xi\Omega} \tag{102}$$

for i.i.d. channels.

We have shown in [17] that the effective channel matrix $\bar{\mathbf{H}}$ contains positive real numbers on its main diagonal with high probability, and can be blindly estimated at the FC using covariance based channel estimation. Defining $\mathbf{D}$ and $\boldsymbol{\Psi}$ as (51) and (52), the above results can be used to obtain Lemma 7.

APPENDIX G
PROOF OF LEMMA 7

Since the phase of h_{km} is uniformly distributed, $E[h_{km}] = 0 \quad m \neq k$, and

$$E[h_{kk}] = \frac{1}{N}\sum_{i=1}^{N}E\left[\frac{\alpha_{ki}^2}{\|\boldsymbol{\alpha}_i\|_2}\right] \overset{(a)}{=} \sqrt{\Omega}\frac{\Gamma(K+\frac{1}{2})}{\Gamma(K+1)}. \tag{103}$$

A proof for (a) is given in [39]. Further,

$$E[|h_{km}|^2] = \frac{1}{N^2}\sum_{i=1}^{N}E\left[\frac{\alpha_{ki}^2\alpha_{mi}^2}{\|\boldsymbol{\alpha}_i\|_2^2}\right]. \tag{104}$$

For $K = 2$, it can be shown that [40]

$$E[|h_{km}|^2] = {}_2F_1\left(1,2;\frac{3}{2};-\frac{1}{2}\right)\frac{\Omega}{N} \tag{105}$$

where ${}_2F_1(\cdot,\cdot;\cdot;\cdot)$ is the Gauss hypergeometric function [41]. For $K \geq 3$, $E[|h_{km}|^2]$ cannot be evaluated in closed form. However, when K is large, $\frac{\alpha_{ki}^2}{\|\boldsymbol{\alpha}_i\|_2}$ and $\frac{\alpha_{mi}^2}{\|\boldsymbol{\alpha}_i\|_2}$ can be treated as being approximately independent. Under this approximation, we have:

$$E[|h_{km}|^2] \approx \frac{\Omega}{N}\left(\frac{\Gamma(K+\frac{1}{2})}{\Gamma(K+1)}\right)^2. \tag{106}$$

Also, from [39]

$$E[h_{kk}^2] = \frac{1}{N}E\left[\frac{\alpha_{ki}^4}{\|\boldsymbol{\alpha}_i\|_2^2}\right] + \frac{(N-1)}{N}E^2\left[\frac{\alpha_{ki}^2}{\|\boldsymbol{\alpha}_i\|_2}\right] = \frac{\Omega}{N}\left(\frac{2}{K-1} + (N-1)\left(\frac{\Gamma(K+\frac{1}{2})}{\Gamma(K+1)}\right)^2\right). \tag{107}$$

REFERENCES

[1] J. Voas, "Demystifying the internet of things," *Computer*, vol. 49, pp. 80–83, June 2016.

[2] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for internet of things: A survey," *IEEE Internet of Things Journal*, vol. 3, pp. 70–95, Feb. 2016.

[3] J. Chamberland and V. Veeravalli, "Wireless sensors in distributed detection applications," *IEEE Signal Process. Mag.*, vol. 24, pp. 16–25, May 2007.

[4] Y.-S. Tu and G. Pottie, "Coherent cooperative transmission from multiple adjacent antennas to a distant stationary antenna through AWGN channels," in *Proc. VTC (Spring)*, pp. 130–134, May 2002.

[5] F. Jameel, S. Wyne, and I. Krikidis, "Secrecy outage for wireless sensor networks," *IEEE Wireless Commun. Lett.*, vol. 21, pp. 1565–1568, July 2017.

[6] J. Zhu, Y. Zou, and B. Zheng, "Physical-layer security and reliability challenges for industrial wireless sensor networks," *IEEE Access*, vol. 5, pp. 5313–5320, 2017.

[7] R. Mudumbai, D. Brown, U. Madhow, and H. Poor, "Distributed transmit beamforming: challenges and recent progress," *IEEE Commun. Mag.*, vol. 47, pp. 102–110, Feb. 2009.

[8] R. Mudumbai, G. Barriac, and U. Madhow, "On the feasibility of distributed beamforming in wireless networks," *IEEE Trans. Wireless Commun.*, vol. 6, pp. 1754–1763, May 2007.

[9] R. Mudumbai, J. Hespanha, U. Madhow, and G. Barriac, "Distributed transmit beamforming using feedback control," *IEEE Trans. Inf. Theory*, vol. 56, pp. 411–426, Jan. 2010.

[10] K. Chaythanya, R. Annavajjala, and C. Murthy, "Comparative analysis of pilot-assisted distributed cophasing approaches in wireless sensor networks," *IEEE Trans. Signal Process.*, vol. 59, pp. 3722–3737, Aug. 2011.

[11] M. M. U. Rahman, R. Mudumbai, and S. Dasgupta, "Consensus based carrier synchronization in a two node networks," in *18th IFAC World Congress*, pp. 10038–10043, June 2011.

[12] S. Zhou and G. Giannakis, "How accurate channel prediction needs to be for transmit-beamforming with adaptive modulation over rayleigh MIMO channels?," *IEEE Trans. Wireless Commun.*, vol. 3, pp. 1285–1294, July 2004.

[13] P. Fertl, A. Hottinen, and G. Matz, "Perturbation-based distributed beamforming for wireless relay networks," in *Proc. Globecom*, pp. 1–5, Nov. 2008.

[14] C. Lin, V. Veeravalli, and S. Meyn, "A random search framework for convergence analysis of distributed beamforming with feedback," *IEEE Trans. Inf. Theory*, vol. 56, pp. 6133–6141, Dec. 2010.

[15] M. K. Banavar, A. D. Smith, C. Tepedelenlioglu, and A. Spanias, "On the effectiveness of multiple antennas in distributed detection over fading MACs," *IEEE Trans. Wireless Commun.*, vol. 11, pp. 1744–1752, May 2012.

[16] A. Manesh, C. Murthy, and R. Annavajjala, "Physical layer data fusion via distributed co-phasing with general signal constellations," *IEEE Trans. Signal Process.*, vol. 63, pp. 4660–4672, Sept. 2015.

[17] R. Chopra, C. R. Murthy, and R. Annavajjala, "Multistream distributed cophasing," *IEEE Trans. Signal Process.*, vol. 65, pp. 1042–1057, Feb. 2017.

[18] R. Chopra, R. Annavajjala, and C. R. Murthy, "Distributed cophasing with autonomous constellation selection," *IEEE Trans. Signal Process.*, vol. 65, pp. 5798–5811, Nov. 2017.

[19] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, pp. 4033–4039, Sept. 2009.

[20] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H. H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Communications Surveys Tutorials*, vol. 19, pp. 1027–1053, Secondquarter 2017.

[21] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, pp. 1355–1387, Oct. 1975.

[22] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in miso systems with partial channel information," *IEEE Trans. Inf. Forensics Security*, vol. 7, pp. 704–716, Apr. 2012.

[23] M. Soltani and H. Arslan, "Randomized beamforming with generalized selection transmission for security enhancement in MISO wiretap channels," *IEEE Access*, vol. 6, pp. 5589–5595, 2018.

[24] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Lett.*, vol. 19, pp. 71–74, Feb. 2012.

[25] N. S. Ferdinand, D. B. da Costa, A. L. F. de Almeida, and M. Latva-aho, "Physical layer secrecy performance of tas wiretap channels with correlated main and eavesdropper channels," vol. 3, pp. 86–89, Feb. 2014.

[26] P. Zhao, M. Zhang, H. Yu, H. Luo, and W. Chen, "Robust beamforming design for sum secrecy rate optimization in mu-miso networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, pp. 1812–1823, Sept. 2015.

[27] X. Chen and H. Chen, "Physical layer security in multi-cell MISO downlinks with incomplete csia unified secrecy performance analysis," *IEEE Trans. Signal Process.*, vol. 62, pp. 6286–6297, Dec. 2014.

[28] Q. Xiong, Y. Gong, Y. Liang, and K. H. Li, "Achieving secrecy of miso fading wiretap channels via jamming and precoding with imperfect channel state information," vol. 3, pp. 357–360, Aug. 2014.

[29] M. R. A. Khandaker, C. Masouros, and K. Wong, "Constructive interference based secure precoding: A new dimension in physical layer security," *IEEE Trans. Inf. Forensics Security*, vol. 13, pp. 2256–2268, Sept. 2018.

[30] A. Zappone, P. Lin, and E. A. Jorswieck, "Energy-efficient secure communications in miso-se systems," in *Proc. Asilomar Conf. on Signals, Syst., and Comput.*, pp. 1001–1005, Nov 2014.

[31] J. Li and A. P. Petropulu, "On ergodic secrecy rate for gaussian MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, pp. 1176–1187, Apr. 2011.

[32] J. Li and A. P. Petropulu, "Ergodic secrecy rate for multiple-antenna wiretap channels with rician fading," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 861–867, 2011.

[33] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. New York, NY, USA: Cambridge University Press, 2005.

[34] E. Tekin and A. Yener, "The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2735–2751, June 2008.

[35] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, pp. 2180–2189, June 2008.

[36] W. Wang, K. C. Teh, and K. H. Li, "Artificial noise aided physical layer security in multi-antenna small-cell networks," *IEEE Trans. Inf. Forensics Security*, vol. 12, pp. 1470–1482, June 2017.

[37] T. M. Cover and J. A. Thomas, *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. Wiley-Interscience, 2006.

[38] A. F. Molisch, M. Z. Win, Y.-S. Choi, and J. H. Winters, "Capacity of MIMO systems with antenna selection," *IEEE Trans. Wireless Commun.*, vol. 4, pp. 1759–1772, July 2005.

[39] C. Feng and Y. Jing, "Modified mrt and outage probability analysis for massive MIMO downlink under per-antenna power constraint," in *2016 IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pp. 1–6, July 2016.

[40] M. O. Hasna and M. S. Alouini, "End-to-end performance of transmission systems with relays over rayleigh-fading channels," *IEEE Trans. Wireless Commun.*, vol. 2, pp. 1126–1131, Nov. 2003.

[41] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*. New York: Dover, ninth dover printing, tenth gpo printing ed., 1964.