Data-Aided Secure Massive MIMO Transmission Under the Pilot Contamination Attack

Yongpeng Wu®, Senior Member, IEEE, Chao-Kai Wen®, Member, IEEE, Wen Chen®, Shi Jin®, Senior Member, IEEE, Robert Schober, Fellow, IEEE, and Giuseppe Caire, Fellow, IEEE

Abstract—In this paper, we study the design of secure communication for time-division duplex multi-cell multi-user massive multiple-input-multiple-output (MIMO) systems with active eavesdropping. We assume that the eavesdropper actively attacks the uplink pilot transmission and the uplink data transmission before eavesdropping the downlink data transmission of the users. We exploit both the received pilot’s and the received data signals for uplink channel estimation. We show analytically that when both the number of transmit antennas and the length of the data vector tend to infinity, the signals of the desired user and the eavesdropper lie in different eigenspaces of the received signal matrix at the base station, provided their signal powers are different. This finding reveals that decreasing (instead of increasing) the desired user’s signal power might be an effective approach to combat a strong active attack from an eavesdropper. Inspired by this observation, we propose a data-aided secure downlink transmission scheme and derive an asymptotic achievable secrecy sum-rate expression for the proposed design. For the special case of a single-cell single-user system with independent and identically distributed fading, the obtained expression reveals that the secrecy rate scales logarithmically with the number of transmit antennas. This is the same scaling law as for the achievable rate of a single-user massive MIMO system in the absence of eavesdroppers. The numerical results indicate that the proposed scheme achieves significant secrecy rate gains compared with alternative approaches based on matched filter precoding with artificial noise generation and null space transmission.

Index Terms—Massive MIMO, pilot contamination attack, physical layer security.

I. INTRODUCTION

WIRELESS networks are widely used in civilian and military applications and have become an indispensable part of our daily lives. Therefore, secure communication is a critical issue for future wireless networks. As a complement to the conventional cryptographic techniques, new approaches to secure communication based on information theoretical concepts, such as the secrecy capacity of the propagation channel, have been developed and are collectively referred to as physical layer security [1]–[6].

Multiple-input multiple-output (MIMO) technology has been shown to be a promising means for providing multiplexing gains and diversity gains, leading to improved performance [7]–[12]. In particular, massive MIMO technology, which utilizes a very large number of antennas at the BS and simple signal processing to provide services for a comparatively small (compared to the number of antennas) number of active mobile users, is a promising approach for efficient transmission of massive amounts of information and is regarded as a key technology in 5G [13]. Pilot contamination is a major impairment in massive MIMO systems [14] and many approaches have been proposed to solve this problem [15]–[18]. For example, the authors of [18] proposed an approach based on Chu sequences, which efficiently reduces the effect of pilot contamination.

Most studies on physical layer security in massive MIMO systems assume that the eavesdropper is passive and does not attack the communication process of the system [19]–[23]. However, a smart eavesdropper can perform a pilot contamination attack to impair the channel estimation process at the base station [24]. Due to the channel hardening effect caused by large antenna arrays, it is difficult to exploit the statistical fluctuations of fading channels to safeguard the transmission. Then, the beamforming direction misled by the pilot contamination attack can significantly enhance the performance of...
the eavesdropper. This results in a serious secrecy threat in time division duplex (TDD)-based massive MIMO systems [24].

Prior works on the pilot contamination attack have studied mechanisms for enhancing the eavesdropper’s performance [25]–[28]. Other works propose various approaches for detecting the pilot contamination attack [29]–[33]. Although these schemes can detect a pilot contamination attack with high probability, [29]–[33] do not provide an effective transmission scheme in the presence of a pilot contamination attack. For secure communication under a pilot contamination attack, the authors of [34] propose a secret key agreement protocol for single-cell multi-user massive MIMO systems. An estimator for the base station (BS) is designed to evaluate the resulting information leakage. Then, the BS and the desired users perform secure communication by adjusting the length of the secret key based on the estimated information leakage. Other works have studied how to combat the pilot contamination attack. The authors of [35] investigate the pilot contamination attack problem for single-cell multi-user massive MIMO systems over independent and identically distributed (i.i.d.) fading channels. The eavesdropper is assumed to only know the pilot signal set whose size scales polynomially with the number of transmit antennas. For each transmission, the desired users randomly select certain pilot signals from this set, which are unknown to the eavesdropper. In this case, it is proved that the impact of the pilot contamination attack can be eliminated as the number of transmit antennas goes to infinity. Under the same pilot allocation protocol, the authors of [36] and [37] respectively propose a random channel training scheme and a jamming-resistant scheme employing an unused pilot sequence to combat the pilot contamination attack and to maintain secure communication. Moreover, by exploiting an additional random sequence, which is transmitted by the legitimate users but is unknown to the eavesdropper, an effective blind channel estimation method and a secure beamforming scheme are developed to realize reliable transmission in [38].

However, all the above-mentioned methods rely on a key assumption: some form of an additional pilot signal protocol which is unknown to the eavesdropper is needed to combat the pilot contamination attack. For the more pessimistic case where the eavesdropper knows the desired users’ exact pilot signal structure for each transmission, the secrecy threat caused by the pilot contamination attack in multi-cell multi-user massive MIMO systems over correlated fading channels is analyzed in [24]. Based on this analysis, three transmission strategies for combating the pilot contamination attack are proposed. Nevertheless, the designs in [24] are not able to guarantee a high (or not even a non-zero) secrecy rate for weakly correlated or i.i.d. fading channels when the power of the eavesdropper pilot signal is much larger than that of the users’ pilot signals.

In this paper, we investigate secure transmission for TDD multi-cell multi-user massive MIMO systems impaired by general correlated fading and a pilot contamination attack. We assume the considered system performs first uplink training followed by uplink and downlink data transmission phases. The eavesdropper jams the uplink training phase and the uplink data transmission phase and then eavesdrops the downlink data transmission. We utilize the data transmitted in the uplink to aid the channel estimation at the BS. Then, based on the estimated channels, the BS designs precoders for downlink transmission.

This paper makes the following key contributions:

1) We prove that when the number of transmit antennas and the amount of transmitted data both approach infinity, the desired users’ and the eavesdropper’s signals lie in different eigenspaces of the uplink received signal matrix provided that their pilot signal powers are different. Our results reveal that increasing the power gap between the desired users’ and the eavesdropper’s signals is beneficial for separating the desired users and the eavesdropper. This implies that when facing an active attack, decreasing (instead of increasing) the desired users’ signal power could be an effective approach for enabling secret communication.

2) Inspired by this observation, we propose a joint uplink and downlink data-aided transmission scheme to combat strong active attacks from an eavesdropper. Then, we derive an asymptotic expression for the corresponding achievable secrecy sum-rate. The derived expression indicates that the impact of an active attack on uplink transmission can be effectively eliminated by the proposed design.

3) We specialize the asymptotic achievable secrecy sum-rate expression to the case of i.i.d. fading channels. Particularly, for the classical MIMO eavesdropper wiretap model, the derived expression indicates that the secrecy rate exhibits a logarithmic growth with the number of transmit antennas. This is the same growth rate as that of the achievable rate of a typical point-to-point massive MIMO system without eavesdropping.

The remainder of this paper is organized as follows. In Section II, the basic system model is introduced and the uplink channel estimation is investigated. In Section III, the proposed secure downlink transmission scheme is presented and an asymptotic expression for the secrecy rate of the proposed design is derived. Section IV discusses the special case of i.i.d. fading in detail. Numerical results are provided in Section V, and conclusions are drawn in Section VI.

1We note that this case constitutes a worst-case scenario. Hence, if secure communication can be achieved for this worst case, then secure communication can also be achieved for more optimistic settings as considered in [36]–[38].

2We note that the pilot contamination attack presents a security threat only for the downlink. In fact, in the uplink, if an eavesdropper transmits a strong pilot signal in the uplink together with the legitimate users, it can at most jam the reception of some users, and therefore disrupt coherent detection, but it will not be able to improve its ability to eavesdrop the uplink traffic. Since this paper studies the pilot contamination attack, we focus on downlink data transmission. Secure uplink transmission is also relevant and is an interesting topic for future work (not dedicated to the pilot contamination attack) but is outside the scope of the present paper.

3We refer to a pilot contamination attack as a strong pilot contamination attack if the pilot signal power of the eavesdropper is much larger than that of the users.
II. UPLINK TRANSMISSION

Throughout the paper, we adopt the following transmission protocol. We assume the uplink transmission phase, comprising uplink training and uplink data transmission, is followed by a downlink data transmission phase.
pilot signal matrix $\mathbf{Y}_m^p \in \mathbb{C}^{N_t \times \tau}$ and the received data signal matrix $\mathbf{Y}_d^m \in \mathbb{C}^{N_t \times (T-\tau)}$ at the BS in cell $m$ are given by

$$
\mathbf{Y}_p^m = \sqrt{P_0} \sum_{k=1}^{K} \mathbf{h}_0^m \omega_k^T + \sum_{l=1}^{K} \sqrt{P_l} \mathbf{h}_l^m \omega_l^T + \sqrt{P_c} \mathbf{H}^m \mathbf{W}_e + \mathbf{N}_p^m,
$$

$$
\mathbf{Y}_d^m = \sqrt{P_0} \sum_{k=1}^{K} \mathbf{h}_0^d \omega_k^T + \sum_{l=1}^{K} \sqrt{P_l} \mathbf{h}_l^d \omega_l^T + \sqrt{P_c} \mathbf{H}^d \mathbf{A} + \mathbf{N}_d^m,
$$

where $P_0$, $\omega_k \in \mathbb{C}^{T \times 1}$, and $\mathbf{d}_{0k} \sim \mathcal{CN}(0,\mathbf{I}_{T})$ denote the average transmit power, the pilot sequence, and the uplink transmission data of the $k$th user in the cell of interest, respectively. For simplicity of notation, we assume that all users in a given cell use the same transmit power $[19]$. Using similar techniques as presented in this paper, our results can be easily extended to the case where the users in a cell have different transmit powers. We assume that the users in different cells have different powers. It is assumed that the same $K$ orthogonal pilot sequences are used in each cell where $\omega_k^T \omega_k = \tau$ and $\omega_l^T \omega_l = 0$, $k \neq l$. $\mathbf{W}_e$ is the pilot attack signal of the eavesdropper. $P_0$ and $\mathbf{d}_{0k}$ denote the average transmit power and the uplink transmission data of the $k$th user in the $l$th cell, respectively. $\mathbf{h}_{lk} \sim \mathcal{CN}(\mathbf{0}, \mathbf{R}_{lk}^p)$ denotes the channel between the $k$th user in the $l$th cell and the BS in the $p$th cell, where $\mathbf{R}_{lk}^p$ is the corresponding correlation matrix. $\mathbf{H}_l^d$ and $\mathbf{P}_c$ denote the channel between the eavesdropper and the BS in the $l$th cell and the average transmit power of the eavesdropper, respectively. $\mathbf{H}_l^d \sim \mathcal{CN}(\mathbf{0}, \mathbf{R}_{l,E,T}^d \otimes \mathbf{R}_{l,E,R}^d)$ represents the channel between the eavesdropper and the BS in the $l$th cell, where $\mathbf{R}_{l,E,T}^d$ and $\mathbf{R}_{l,E,R}^d$ are the corresponding transmit and receive correlation matrices of the eavesdropper. $\mathbf{N}_p^m \in \mathbb{C}^{N_t \times \tau}$ and $\mathbf{N}_d^m \in \mathbb{C}^{N_t \times (T-\tau)}$ are noise matrices whose columns are i.i.d. Gaussian distributed with $\mathcal{CN}(0,\mathbf{N}_e \mathbf{I}_{N_e})$.

During the training phase, the eavesdropper attacks all users in the cell of interest. In this paper, we adopt the worst-case assumption that for each transmission, the eavesdropper knows the exact pilot sequence $\omega_k$ of each user. Therefore, it uses pilot attack sequences $\mathbf{W}_e = \sum_{k=1}^{K} \mathbf{W}_k$ [35], where $\mathbf{W}_k = [\omega_k \cdots \omega_k]^T \in \mathbb{C}^{T \times \tau}$. In the uplink data transmission phase, the eavesdropper generates an artificial noise matrix $\mathbf{A} \in \mathbb{C}^{N_t \times T-\tau}$, whose elements follow an i.i.d. standard Gaussian distribution.

We define $\mathbf{Y}_0 = [\mathbf{Y}_p^0 \mathbf{Y}_d^0]$ and the eigenvalue decomposition $\frac{1}{T \tau^N} \mathbf{Y}_0 \mathbf{Y}_0^H = [\mathbf{\Sigma}_1, \cdots, \mathbf{\Sigma}_{N_e}] [\mathbf{\Sigma}_1, \cdots, \mathbf{\Sigma}_{N_e}]^H$, where the eigenvalues on the main diagonal of matrix $\mathbf{\Sigma}$ are organized in ascending order. For the proposed joint uplink and downlink transmission scheme and the corresponding asymptotic performance analysis.

---

Footnote 1: If the eavesdropper is only interested in a particular user, then he can perform a pilot contamination attack specifically for this user as in [24]. However, this pilot contamination precoding will not influence the proposed joint uplink and downlink transmission scheme and the corresponding asymptotic performance analysis.

Footnote 2: When the eavesdropper increases the pilot contamination attack power $P_e$, the users in the cell of interest can intentionally decrease their pilot signal power $P_0$ to achieve a significant power gap between $P_0$ and $P_0$ based on a power control mechanism. According to Appendix A, this is essential to eliminate the impact of the active eavesdropper. If the eavesdropper does not eavesdrop the signals in the cell in which it is located but the signals in one of the other cells, then a power control mechanism for $P_e$ and $P_I$ is required to combat the pilot contamination attack.
that a sufficient power gap between the BS and the WU: the coherence time spans several hundred symbol durations. This assumption can be justified based on the expression for the coherence time in [16, Eq. (1)]. For typical speeds of mobile users and typical symbol durations, the coherence time spans several hundred symbol durations.

Remark 4: The simulation results in Section V indicate that a sufficient power gap between $P_0$ and $P_e$ can guarantee a good secrecy performance when the number of transmit antennas and the coherence time of the channel are large but finite. We note that allocating a high power to the desired users to combat a strong active attack is not necessary. In contrast, a large gap between $P_0 \text{tr}(\mathbf{R}_{ok}^0)$ and $P_e \text{tr}(\mathbf{R}_{lk}^0)$ is essential to approach the channel estimation result in Theorem 1. This implies that decreasing the transmit power of the desired users can be an effective strategy to ensure secure transmission under a strong active attack. As shown in Figure 5 and Figure 6 in Section V, as long as $\rho = P_e/(P_0 K)$ is larger than 0 dB, the proposed design is able to achieve a good secrecy performance in all considered scenarios.

Based on Theorem 1, in the next section, we can design the precoders for downlink transmission.

III. DOWNLINK TRANSMISSION

In this section, we consider the downlink transmission phase. We assume that the BSs in all $L + 1$ cells perform channel estimation according to Theorem 1 by replacing $\hat{\mathbf{h}}_{eq,0k}$, $\mathbf{V}_eq$, by $\hat{\mathbf{h}}_{eq,tk}$, $\mathbf{V}_{eq}$, respectively. Then, the $l$th BS designs the transmit signal as follows

$$\mathbf{x}_l = \sqrt{P} \sum_{k=1}^{K} t_{lk} s_{lk}, \quad l = 0, \ldots, L,$$  

(6)

where $P$ is the downlink transmission power, $t_{lk} = (\mathbf{V}_eq^H \mathbf{h}_{eq,ltk})$ and $s_{lk}$ is the downlink transmitted signal for the $k$th user in the $l$th cell.

We note that unlike for the scheme in [24], for the proposed precoder design, the base station does not need to know the full statistical channel state information of the eavesdropper. As long as $P_0 \text{tr}(\mathbf{R}_{E,T}^0) \gg P_0 \text{tr}(\mathbf{R}_{ok}^0) \gg P_0 \text{tr}(\mathbf{R}_{lk}^0)$ holds, the base station can identify the relevant columns in $\mathbf{h}_{eq,ltk}$, $\mathbf{V}_{eq}^0$, respectively. For the legitimate users in the cell of interest, the BS needs to know their covariance matrices $\mathbf{R}_{ok}^0$ to perform channel estimation, see Theorem 1.

Because each user in the cell of interest has the risk of being eavesdropped, based on [39] and [24], the achievable ergodic (the codewords are sent over a large number of fading blocks) secrecy sum-rate can be expressed as

$$R_{sec} = \sum_{k=1}^{K} [R_k - C_k^{\text{eve}}]^+$$  

(7)

where $R_k$ and $C_k^{\text{eve}}$ denote an achievable ergodic rate between the BS and the $k$th user and the ergodic capacity between the BS and the eavesdropper seeking to decode the information of the $k$th user, respectively.

The received signal $y_{0k}$ at the $k$th user in the cell of interest is given by

$$y_{0k} = \sum_{l=0}^{L} (\mathbf{h}_{0k}^0)^H \mathbf{x}_l + n_d$$

(8)

where $n_d \sim C_N(0, N_{od})$ is the noise affecting the received downlink signal.

The achievable ergodic rate $R_k$ is given by

$$R_k = E[\log (1 + \gamma_k)],$$  

(9)

where

$$\gamma_k = \frac{1}{N_{od}} \left[ \sum_{l=1}^{K} \mathbf{g}_{0l,k}^H \mathbf{g}_{0l,k} + \sum_{l=1}^{L} \sum_{t=1}^{K} \mathbf{g}_{lt,k}^H \mathbf{g}_{lt,k} \right],$$  

(10)

and $\mathbf{g}_{0l,k} = \sqrt{P}(\mathbf{h}_{0k}^0)^H (\mathbf{V}_eq^H \mathbf{h}_{eq,ltk})$.

The ergodic capacity of the eavesdropper for decoding the information intended for user $k$, $C_k^{\text{eve}}$, is given by

$$C_k^{\text{eve}} = E[\log_2 (1 + P(t_{0k})^H \mathbf{H}_e^0 \mathbf{Q}_k^{-1} (\mathbf{H}_e^0)^H t_{0k})],$$  

(11)

where

$$\mathbf{Q}_k = (\mathbf{H}_o^0)^H \sum_{p=1}^{K} \mathbf{t}_{0l}(t_{ok})^H \mathbf{H}_e^p$$

$$+ \sum_{l=1}^{L} (\mathbf{H}_e^0)^H \sum_{k=1}^{K} t_{lk}(t_{lk})^H \mathbf{H}_e^l + N_{od} \mathbf{I}_{N_e}.$$  

(12)

Based on (7), (9), and (11), we obtain the following theorem.

**Theorem 2:** For the considered multi-cell multi-user massive MIMO system, an asymptotic achievable secrecy sum-rate for the transmit signal design in (6) is given by

$$R_{sec, ach} = \sum_{k=1}^{K} \mathbf{N}_{i,k} \log (1 + \gamma_k),$$  

(13)

It should be noted that here we consider the practical scenario where the eavesdropper is not able to decode and cancel the signals of the intra-cell and inter-cell users from the received signal. For a more pessimistic setting, where the eavesdropper has access to the data of all intra-cell and inter-cell interfering users, we can also obtain a lower bound on the ergodic secrecy rate as in [24]. However, the two expressions exhibit no difference as far as the subsequent analysis is concerned since the eavesdropper’s rate will be suppressed to zero based on the proposed data-aided transmission scheme.
where
\[
\gamma_k = \frac{P_0^0N_{t,k}G_k}{a_{0,k,1}^0 + P_0^0\sum_{t=1}^{K} b_{t,k}^0 + P \sum_{t=1}^{K} \sum_{l=1}^{K} c_{t,k}^1},
\]
(14)
\[
d_{l,t,1} = \frac{P_0^0 \left[ \sum_{p=1}^{K} A_{l,t,4,p} \right] tr(R_{l,t}R_{l,p})}{\sum_{p=1, p \neq t}^{K} A_{l,t,4,p} tr(R_{l,t})} + N_0 \sum_{p=1}^{K} \left[ A_{l,t,4,p} \right] tr(R_{l,k}) ,
\]
(15)
\[
A_{l,t,4} = A_{l,t,3} - \sum_{k=1}^{L} \left( A_{l,t,2} \right)^2, \quad A_{l,t,2} = \left( N_0 I + \tau P_0 A_{l,t,1} \right)^{-1},
\]
(16)
\[
A_{l,t,1} = \left( \frac{tr(R_{l,t}R_{l,t})}{\sum_{k=1}^{K} tr(R_{l,t}R_{l,k})} \right), \quad l = 0, 1, \ldots, L, \quad t = 1, \ldots, K,
\]
(17)
\[
a_{0,k,2} = P_0^0 \left( \sum_{l=1}^{K} A_{l,k,5} \right) tr(R_{0,k}),
\]
(18)
\[
A_{l,t,5} = A_{l,t,2} A_{l,t,1} diag(tr(R_{0,t})), \quad l = 0, 1, \ldots, L, \quad t = 1, \ldots, K,
\]
(19)
\[
b_{0,t,k} = \left( P_0^0 \left| (A_{0,t,5}^0) \right|_k \right) tr(R_{0,k} R_{0,k}),
\]
(20)
\[
c_{t,k} = P_t^0 \left[ \sum_{p=1}^{K} A_{l,t,5}^0 \right] tr(R_{0,k} R_{l,p}) tr(R_{l,p}),
\]
(21)
\[
N_0 + P \sum_{t=1}^{K} a_{2kt,1,1} + P \sum_{l=1}^{K} \sum_{p=1}^{K} a_{3lt,1,1},
\]
(24)
\[
R_{sec, iid} \rightarrow \infty \sum_{k=1}^{K} \log (1 + \gamma_k),
\]
(25)
\[
R_{sec, iid} = \frac{P_{a_{1k,1}}}{N_0 + \sum_{t=1}^{K} \sum_{k=1}^{K} a_{2kt,1,1} + \sum_{l=1}^{K} \sum_{p=1}^{K} a_{3lt,1,1}},
\]
(26)
\[
\beta_{0,k} \rightarrow \beta_{0,k}^0(N_t + K - 1 + K N_0),
\]
(27)
\[
\beta_{0,k} = \frac{P_0^0 \left( \begin{array}{c} \beta_{0,k}^0 \\ \beta_{0,k}^0 (N_t + K - 1) + K N_0 \end{array} \right)}{P_0^0 \beta_{0,k}^0 (N_t + K - 1 + K N_0)}.
\]
Proposition 3 states that the secrecy rate is a monotonically increasing function of the signal-to-noise ratio (SNR) SNR = P/N_0 even in the presence of an active eavesdropper. This behavior is in sharp contrast with the results in [24, Theorem 3], for which the secrecy rate decreases for increasing SNR in the high SNR range.

Remark 7: It is important to note that the proposed scheme does not require joint channel estimation and data detection or an additional pilot sequence hopping mechanism. In fact, the uplink data only has to be exploited to generate matrix V^{eq}_0. Then, simply projecting the transmit signal along the eigenspace, V^{eq}_0, is enough to effectively combat the strong pilot contamination attack without any further computational operations or extra resources.

IV. THE I.I.D. FADEING CASE

In order to obtain more insightful results, in this section, we analyze the asymptotic achievable secrecy rate of massive MIMO systems for the i.i.d. fading case. For general multi-cell multi-user massive MIMO systems, we have the following theorem.

Theorem 3: For multi-cell multi-user massive MIMO systems with i.i.d. fading where R_{lk}^p = \beta_{lk}^0 I_{N_t},^9 the asymptotic achievable secrecy sum-rate for the transmit signal design in (6) is given by

\[
R_{sec, iid} \rightarrow \infty \sum_{k=1}^{K} \log (1 + \gamma_k),
\]
(23)
\[
\gamma_k = \frac{P_0^0N_{t,k}G_k}{a_{0,k,1}^0 + P_0^0\sum_{t=1}^{K} b_{t,k}^0 + P \sum_{t=1}^{K} \sum_{l=1}^{K} c_{t,k}^1},
\]
(24)
\[
A_{l,t,4} = A_{l,t,3} - \sum_{k=1}^{L} \left( A_{l,t,2} \right)^2, \quad A_{l,t,2} = \left( N_0 I + \tau P_0 A_{l,t,1} \right)^{-1},
\]
(25)
\[
A_{l,t,1} = \left( \frac{tr(R_{l,t}R_{l,t})}{\sum_{k=1}^{K} tr(R_{l,t}R_{l,k})} \right), \quad l = 0, 1, \ldots, L, \quad t = 1, \ldots, K,
\]
(26)
\[
a_{0,k,2} = P_0^0 \left( \sum_{l=1}^{K} A_{l,k,5} \right) tr(R_{0,k}),
\]
(27)
\[
A_{l,t,5} = A_{l,t,2} A_{l,t,1} diag(tr(R_{0,t})), \quad l = 0, 1, \ldots, L, \quad t = 1, \ldots, K,
\]
(28)
\[
b_{0,t,k} = \left( P_0^0 \left| (A_{0,t,5}^0) \right|_k \right) tr(R_{0,k} R_{0,k}),
\]
(29)
\[
c_{t,k} = P_t^0 \left[ \sum_{p=1}^{K} A_{l,t,5}^0 \right] tr(R_{0,k} R_{l,p}) tr(R_{l,p}),
\]
(30)

Proof: The theorem can be proved by substituting R_{lk}^p = \beta_{lk}^0 I_{N_t} into (13) and performing some simplifications.

Remark 8: Theorem 3 indicates that the secrecy rate is a monotonically increasing function of the signal-to-noise ratio (SNR) SNR = P/N_0 even in the presence of an active eavesdropper. This behavior is in sharp contrast with the scheme proposed in [24, Theorem 3], for which the secrecy rate decreases for increasing SNR in the high SNR range.

Remark 6: Although the rigorous theoretical analysis in Theorem 2 requires that both N_t and T tend to infinity, our simulation results in Section V indicate that even for short packet communication (e.g., T = 128) and a finite number of transmit antennas (e.g., N_t = 64), the proposed joint uplink and downlink transmission approach is adopted.
regime if all the available power at the BS is allocated to the information-carrying signals. For the proposed data-aided secure massive MIMO transmission, \( \mathbf{V}_eq^0 \) naturally forms an asymptotic orthogonal space to the eavesdropper’s channel. As a result, the null space of the transmit correlation matrix of the eavesdropper’s channel [24] is not essential anymore to combat the strong pilot contamination attack. The proposed joint uplink and downlink transmission scheme can guarantee reliable secure communication even for i.i.d. fading channels.

To provide more insights into the impact of the proposed scheme on secure communication in massive MIMO systems, we simplify the system model further to the single-cell single-user case. Based on Theorem 3 and [40, Corollary 1], we have the following corollary.

**Corollary 1:** For a single-cell single-user system \((L = 0, K = 1)\) with i.i.d. fading, the asymptotic achievable secrecy rate for the transmit signal design in (6) is given by

\[
R_{sc_{, \text{id, single}}} = \log \left(1 + \frac{P N_{0d} \rho_i}{N_0} + o(N_i)\right).
\]

**Proof:** By setting \(L = 0, K = 1\) in (23) and considering the asymptotic case, we obtain (28). \(\square\)

**Remark 9:** The asymptotic secrecy rate in (28) grows logarithmically with the number of transmit antennas. This is identical to the growth rate of the asymptotic rate for single-user massive MIMO systems without eavesdropper. This is in sharp contrast to the conclusions in [24, Theorem 9], where secure communication is unachievable for the single-cell single-user i.i.d. fading case for high pilot contamination attack powers. Corollary 1 reveals that by exploiting the uplink transmission data, we can find a promising solution that facilitates secure communication for i.i.d. fading massive MIMO systems with active eavesdropper.

V. NUMERICAL RESULTS

In this section, we present numerical results to evaluate the proposed scheme and the obtained analytical results. To the best of our knowledge, although there has been a large amount of research on active eavesdropping in the past few years [35]–[38], most of these schemes require some additional pilot signal protocol which is unknown to the eavesdropper to combat the pilot contamination attack. These schemes are not compatible with the assumptions in our paper, where the eavesdropper perfectly knows the desired users’ exact pilot signal structure for each transmission. Hence, we compare the proposed scheme with matched filter precoding and AN generation (we refer to this design as MF-AN scheme) and the null space scheme in [24], which both also do not require a modified pilot protocol.

We define SNR = \(P/N_{0d}\) and set \(P_0 = P_1 = \ldots = P_K\). Also, we define \(\rho = P_e/(P_0 K)\). We consider both correlated fading channels and i.i.d. fading channels. For correlated fading channels, a uniform linear array is used at the BS with half a wavelength antenna spacing. The angle of arrival (AoA)

\(\rho = P_e/(P_0 K)\).

Figure 2 shows the normalized mean squared error (MSE)

\[
\sum_{k=1}^{K} \frac{\| \mathbf{h}_{eq,k} - \mathbf{V}_eq^0 \mathbf{h}_{eq,k}^0 \|_2^2}{\| \mathbf{V}_eq^0 \mathbf{h}_{eq,k}^0 \|_2^2} \text{ versus (vs.) } T
\]

for the MMSE estimation scheme in Theorem 1 for \(L = 3, K = 5, N_t = 128, \rho = 0 \text{ dB}, \tau = 64, N_0 = 1\), correlated fading with \(\theta_b = \pi\), and different \(P_0\). We observe from Figure 2 that the MSE is below \(10^{-3}\) for all considered \(P_0\) and \(T\). This demonstrates that the proposed data-aided estimation method is an effective approach to distinguish the actual channel of each user from the eavesdropper’s channel under the pilot contamination attack.

Figure 3 shows the secrecy rate performance vs. SNR for the proposed scheme for \(L = 3, K = 5, T = 1024, \tau = 64,\)

\(\rho\), and set \(P_0 = P_1 = \ldots = P_K\). Also, we define \(\rho = P_e/(P_0 K)\). We consider both correlated fading channels and i.i.d. fading channels. For correlated fading channels, a uniform linear array is used at the BS with half a wavelength antenna spacing. The angle of arrival (AoA)

\[\rho = P_e/(P_0 K)\].
TABLE I
VALUES OF MAIN PARAMETERS USED IN SIMULATIONS

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Fig. 2</th>
<th>Fig. 3</th>
<th>Fig. 4</th>
<th>Fig. 5</th>
<th>Fig. 6</th>
<th>Fig. 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>K</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Nt</td>
<td>128</td>
<td>128</td>
<td>64</td>
<td>64</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>T</td>
<td>1024</td>
<td>1024</td>
<td>1024</td>
<td>1024</td>
<td>1024</td>
<td>1024</td>
</tr>
<tr>
<td>τ</td>
<td>64</td>
<td>64</td>
<td>64</td>
<td>64</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>P0</td>
<td>1, 10, 100</td>
<td>1, 10, 100</td>
<td>1, 10, 100</td>
<td>1, 10, 100</td>
<td>1, 10, 100</td>
<td>1, 10, 100</td>
</tr>
<tr>
<td>N0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>ρ</td>
<td>1 dB, 20 dB</td>
<td>20 dB, 20 dB</td>
<td>0-20 dB, 0-20 dB</td>
<td>0-20 dB, 10 dB</td>
<td>0-20 dB, 10 dB</td>
<td>0-20 dB, 10 dB</td>
</tr>
<tr>
<td>SNR</td>
<td>None</td>
<td>-20-26 dB, 10, 20 dB, 20 dB, 20 dB, 15 dB</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>θb</td>
<td>π, π/2</td>
<td>Random, π/2, None, π/2, None, π/2</td>
<td>Random</td>
<td>Random</td>
<td>Random</td>
<td>Random</td>
</tr>
<tr>
<td>σ</td>
<td>0.1</td>
<td>0.1</td>
<td>0.1</td>
<td>0.1</td>
<td>0.1</td>
<td>0.1</td>
</tr>
<tr>
<td>β</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>β'</td>
<td>0.1</td>
<td>0.1</td>
<td>0.1</td>
<td>0.1</td>
<td>0.1</td>
<td>0.1</td>
</tr>
<tr>
<td>Nc</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Fig. 3. Secrecy rate vs. SNR for $L = 3$, $K = 5$, $T = 1024$, $τ = 64$, $ρ = 20$ dB, $P_0 = 10$, $N_0 = 1$, correlated fading with $θ_b = π$, and different $N_t$.

Fig. 4. Secrecy rate vs. $N_t$ for $L = 0$, $K = 1$, $ρ = 20$ dB, $P_0 = 10$, $N_0 = 1$, i.i.d. fading, and different SNRs.

$ρ = 20$ dB, $P_0 = 10$, $N_0 = 1$, correlated fading with $θ_b = π$, and different $N_t$. We observe from Figure 3 that the asymptotic secrecy rates in Theorem 2 provide a good approximation for the exact secrecy rates. The accuracy of the approximation increases with the number of transmit antennas as expected. Also, we observe from Figure 3 that the secrecy rate is a monotonically increasing function of the SNR even under a strong pilot contamination attack.

Figure 4 shows the secrecy rate performance of the proposed scheme vs. $N_t$ for $L = 0$, $K = 1$, $ρ = 20$ dB, $P_0 = 10$, $N_0 = 1$, i.i.d. fading, and different SNRs. We set $τ = 64$ and $T = 16 N_t$. We observe from Figure 4 that the secrecy rates scale logarithmically with the number of transmit antennas, as predicted by Corollary 1. Figure 4 also shows that the theoretical secrecy rates provide good approximations for the exact secrecy rates for the i.i.d. fading case.

Figure 5 shows the exact secrecy rate performance vs. $ρ$ for the proposed scheme and the null space (NS) scheme [24] for $L = 3$, $K = 5$, $N_t = 128$, $ρ = 20$ dB, $P_0 = 10$, $N_0 = 1$, SNR = 20 dB, correlated fading with $θ_b = π$, and different $T$. We observe from Figure 5 that even for short packet communication when $T = 128$, the proposed scheme can achieve an obvious secrecy performance gain compared to the null space scheme. Also, we observe from Figure 5 that when the power of the active attack is strong, the null space scheme maintains an almost constant secrecy rate. However, as $ρ$ increases, the gap between $P_0 R_{0,k}$ and $P_e \Lambda_i$ increases. Therefore, the secrecy rates of the proposed scheme increase with $ρ$. Moreover, Figure 5 reveals that increasing $T$ is beneficial for the secrecy performance of the proposed scheme.

Figure 6 shows the exact secrecy rate performance vs. $ρ$ for the proposed scheme and the MF-AN scheme [24] for $L = 3$, $K = 5$, $N_t = 128$, $ρ = 20$ dB, $P_0 = 10$, $N_0 = 1$, SNR = 20 dB, i.i.d. fading, and different $T$. We observe from Figure 6 that when the power of the active attack is strong, the MF-AN scheme cannot provide a non-zero secrecy rate. However, our proposed scheme performs well in the entire considered range of $ρ$. When the power of the active attack is close to the power of the desired user’s pilot signal where $ρ$ is small, the asymptotic estimation error in Theorem 1 increases. As a result, our proposed scheme suffers a slight performance loss comparing to the MF-AN scheme.
Appendix A

Proof of Theorem 1

We define \( \Omega_0 = [\omega_1, \cdots, \omega_K]^T \), \( D_0 = \sqrt{P_0}d_0 \), \( \Omega_L = [\sqrt{P_1} \Omega_0^T, \cdots, \sqrt{P_K} \Omega_0^T]^T \), \( D_L = [\sqrt{P_1}d_1, \cdots, \sqrt{P_K}d_K]^T \), \( X_0 = \left[ \sqrt{P_0} \Omega_0 D_0 \right]^T \), \( X_L = \left[ \sqrt{P_L} \Omega_L D_L \right]^T \), \( X_e = \left[ \sqrt{P_{e,L}} \sum_{k=1}^K W_k \right]^T \).

Based on (1) and (2), the received signal \( Y_0 \) can be re-expressed as

\[
Y_0 = H_0 X_0 + H_t X_L + H^0_e X_e + N \tag{30}
\]

where \( N = [N_p^0, N_d^0]^T \).

For massive MIMO with correlated fading, when \( N_t \to \infty \), we have

\[
\frac{1}{N_t} H_0^H H_0 = \frac{1}{N_t} \begin{bmatrix}
(h_0^0)^H h_0^0 & \cdots & (h_{0,K}^0)^H h_0^0 \\
\vdots & \ddots & \vdots \\
(h_0^0)^H h_{0,K}^0 & \cdots & (h_{0,K}^0)^H h_{0,K}^0
\end{bmatrix}
\tag{31}
\]
Similarly, we have
\[
\frac{1}{N_t} \mathbf{H}^H_0 \mathbf{H}_0 \xrightarrow{N_t \to \infty} \mathbf{R}_0 \frac{1}{N_t} \begin{bmatrix} \text{tr} \left( \mathbf{R}_{0,1}^0 \right) & 0 & \cdots & 0 \\ 0 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \text{tr} \left( \mathbf{R}_{0,K}^0 \right) \end{bmatrix}
\]
(32)

Similarly, we have
\[
\frac{1}{N_t} \mathbf{H}^H_I \mathbf{H}_I \xrightarrow{N_t \to \infty} \mathbf{R}_I \frac{1}{N_t} \begin{bmatrix} \text{tr} \left( \mathbf{R}_{0,1}^0 \right) & 0 & \cdots & 0 \\ 0 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \text{tr} \left( \mathbf{R}_{L,K}^0 \right) \end{bmatrix}
\]
(33)

Also, based on [42, Eq. (102)], we have
\[
\frac{1}{N_t} [\mathbf{H}^H I e^e]_{ij} = \frac{1}{N_t} (h_{0,i})^H h_{E,j} = e_i^H \mathbf{R}_{E,R}^{1/2} (g_{0}^H)^H (\mathbf{R}_{E,T}^H)^{1/2} X_i^H \text{tr} (\mathbf{R}_{0,E}^0) \text{tr} (\mathbf{R}_{E,T})
\]
(34)

where \( h_{0,i}^H \) denotes the \( i \)th column of matrix \( \mathbf{H}_e \), \( g_{0}^H \sim \mathcal{CN}(0, \mathbf{I}_{N_{eq}} \otimes \mathbf{I}_{N_e}) \), and \( e_i \) is a \( N_t \times 1 \) vector with the \( i \)th element being one and the other elements being zero.

As a result, we have
\[
\frac{1}{N_t} \mathbf{H}^H e \xrightarrow{N_t \to \infty} \frac{1}{N_t} \mathbf{R}_{E,R}^{1/2} \text{tr} (\mathbf{R}_{0,E,T}^0) = \frac{1}{N_t} \mathbf{R}_E.
\]
(35)

When \( T \to \infty \), based on [40, Corollary 1], we have
\[
\frac{1}{T} \mathbf{X}_0 \mathbf{X}_0^H \xrightarrow{T \to \infty} \mathbb{E} \mathbf{X}_0 \mathbf{X}_0^H \mathbf{X}_I \mathbf{X}_I^H \xrightarrow{T \to \infty} \mathbb{E} \mathbf{X}_I \mathbf{X}_I^H \mathbf{X}_0 \mathbf{X}_0^H \mathbf{X}_L \mathbf{X}_L^H \xrightarrow{T \to \infty} \mathbb{E} \mathbf{X}_L \mathbf{X}_L^H
\]
(36)

Then, we obtain (39), given at the top of the next page.

Based on [40, Corollary 1], we obtain (40), given at the top of next page from (39).

Now, we re-write (40) as (41), given at the top of the next page.

We define
\[
\mathbf{U}_Y = \begin{bmatrix} \mathbf{U}_W & \mathbf{H}_I \mathbf{R}_I^{-1/2} \mathbf{H}_e \mathbf{R}_e^{-1/2} \mathbf{H}_0 \mathbf{R}_0^{-1/2} \end{bmatrix}
\]
(42)

where \( \mathbf{U}_W \in \mathbb{C}^{N_t \times (N_t - M)} \) has orthogonal columns.

Based on (32)–(35), we know
\[
\frac{1}{N_t} \mathbf{U}_Y^H \mathbf{Y} \xrightarrow{N_t \to \infty} \mathbf{I}_{N_t}.
\]
(43)

From (39)–(43), we know that for \( T \to \infty, N_t \to \infty \), \( \mathbf{U}_Y \) is the right singular matrix of \( \mathbf{Y} \). Therefore, we obtain
\[
\mathbf{Z}_{op} = \frac{1}{\sqrt{T N_t}} \mathbf{V}_p^0 (\mathbf{V}_p^0)^H \xrightarrow{N_t \to \infty} \frac{1}{\sqrt{T N_t}} \mathbf{F}_0 \mathbf{D}_0 \mathbf{X}_0 + \frac{1}{\sqrt{T N_t}} (\mathbf{V}_p^0)^H \mathbf{N}_p^0.
\]
(44)

Define \( \mathbf{z} = \text{vec} (\mathbf{Z}_{op}) \), where \( \mathbf{Z}_{op} \) is defined in Theorem 1. From (44), we can re-express the equivalent received signal during the pilot transmission phase as follows
\[
\mathbf{z} = \sqrt{T} \sum_{i=1}^{K} (\omega_k \otimes \mathbf{I}_K) \mathbf{h}_{eq,0i} + \mathbf{n}
\]
(45)

where
\[
\mathbf{n} = \begin{bmatrix} (\mathbf{V}_p^0)^H \mathbf{n}^0_p \end{bmatrix}
\]
(46)

and \( \mathbf{n}_p^0 \) in (46) is the \( i \)th column of \( \mathbf{N}_p^0 \).

Based on (45), the MMSE estimate of \( \mathbf{h}_{eq,0k} \) is given by
\[
\mathbf{h}_{eq,0k} = \sqrt{T} \mathbf{V}_p \mathbf{V}_p^0 (\mathbf{V}_p^0)^H (\mathbf{X}_{eq,0} \otimes \mathbf{I}_K)^H
\]
\[
\times \left( \mathbf{N}_0 \mathbf{I}_K + \tau P_0 \mathbf{V}_p \mathbf{V}_p^0 \mathbf{V}_p^H \right)^{-1}
\]
\[
\times \left( \sqrt{T} \mathbf{V}_p \mathbf{V}_p^0 \mathbf{V}_p^H (\mathbf{X}_{eq,0} \otimes \mathbf{I}_K)^H \right) \mathbf{z}
\]
(47)

For the noise term in (47), we have
\[
(\mathbf{X}_{eq,0} \otimes \mathbf{I}_K)^H \mathbf{n} = (\mathbf{V}_p^0)^H \sum_{i=1}^{K} \omega_k^* \mathbf{n}_p^i
\]
(48)

where \( \omega_k^* \) is the \( i \)th element of \( \mathbf{w}_k \).

Combining (47) and (48) completes the proof.

**APPENDIX B**

**PROOF OF THEOREM 2**

From (40), we know
\[
(\mathbf{V}_p^0)^H = \mathbf{H}_e \mathbf{R}_e^{-1/2} = [h_{0,1}^0, \ldots, h_{0,K}^0] \mathbf{R}_0^{-1/2},
\]
(49)

\[
(\mathbf{V}_p^i)^H = \mathbf{H}_e \mathbf{R}_e^{-1/2} = [h_{0,1}^i, \ldots, h_{0,K}^i] \mathbf{R}_0^{-1/2}.
\]
(50)

First, we consider
\[
|\mathbf{g}_{0,k}^0|^2 = \frac{P}{\mathbf{H}_0^H \mathbf{H}_0} (\mathbf{V}_p^i)^H \mathbf{h}_{eq,0k} \mathbf{h}_{eq,0k}^H (\mathbf{V}_p^0)^H \mathbf{n}_{eq}.
\]
(51)
Based on (4), we have
\[
\|\hat{\mathbf{n}}_{eq,0k}\|^2 = P_0 \left( \sqrt{P_0} \mathbf{v}_{eq}^H \mathbf{h}_{0k}^0 + \mathbf{v}_{eq}^H \hat{\mathbf{n}}_{eq} \right)^H \\
\times \left( \mathbf{N}_k + \tau P_0 \mathbf{v}_{eq}^0 \mathbf{R}_{0k}^0 \left( \mathbf{v}_{eq}^0 \right)^H \right)^{-1} \mathbf{v}_{eq}^0 \mathbf{R}_{0k}^0 \left( \mathbf{v}_{eq}^0 \right)^H \\
\times \left( \mathbf{F}_0 \mathbf{v}_{eq}^H \mathbf{h}_{0k}^0 + \mathbf{v}_{eq}^H \hat{\mathbf{n}}_{eq} \right).
\] (52)

Based on (49) and (40, Corollary 1), we have
\[
\frac{1}{N_t} \mathbf{v}_{eq}^0 \mathbf{R}_{0k}^0 \left( \mathbf{v}_{eq}^0 \right)^H = \frac{1}{N_t} \mathbf{R}_{0k}^{1/2} \mathbf{h}_{0k,1, \ldots, 0} \mathbf{R}_{0k}^{1/2} \mathbf{R}_{0k}^{1/2} \mathbf{R}_{0k}^{1/2} \mathbf{R}_{0k}^{1/2} \mathbf{R}_{0k}^{1/2} \mathbf{R}_{0k}^{1/2},
\] (53)

By substituting (54) into (52) and simplifying, we have
\[
\frac{1}{N_t} \|\hat{\mathbf{n}}_{eq,0k}\|^2 = \frac{1}{N_t} P_0 \left( \sqrt{P_0} \mathbf{v}_{eq}^H \mathbf{h}_{0k}^0 + \mathbf{v}_{eq}^H \hat{\mathbf{n}}_{eq} \right)^H A_{0k,3}^0 \\
\times \left( \sqrt{P_0} \mathbf{v}_{eq}^H \mathbf{h}_{0k}^0 + \mathbf{v}_{eq}^H \hat{\mathbf{n}}_{eq} \right) \\
\times \left( \mathbf{N}_k \rightarrow \frac{1}{N_t} P_0 \left( \sqrt{P_0} \mathbf{v}_{eq}^H \mathbf{h}_{0k}^0 + \mathbf{v}_{eq}^H \hat{\mathbf{n}}_{eq} \right) A_{0k,3}^0 \mathbf{h}_{0k}^0 \\
+ \left( \hat{\mathbf{n}}_{eq} \right)^H \left( \mathbf{v}_{eq}^0 \right)^H A_{0k,3}^0 \mathbf{v}_{eq} \hat{\mathbf{n}}_{eq} \right),
\] (55)

where \(A_{0k,3}^0\) is defined in (17).
For the second term on the right hand side of (55), we obtain
\[
\frac{1}{N_t} (h_{0k}^0)^H (V_{eq})^H A_{0k,3}^0 V_{eq} h_{0k}^0
\]
\[
= \frac{1}{N_t} (h_{0k}^0)^H [h_{01}, \ldots, h_{0K}]^T R_0^{-1/2} A_{0k,3}^0
\]
\[
\times R_0^{-1/2} [h_{01}, \ldots, h_{0K}]^T H^0 h_{0k}
\]
\[
= \frac{1}{N_t} \sum_{t=1, t \neq k}^K (h_{0k}^0)^H h_{0t}^0 [A_{0k,4}^0]_{tt} (h_{0t}^0)^H h_{0k}
\]
\[
+ (h_{0k}^0)^H h_{0k}^0 [A_{0k,4}^0]_{kk} (h_{0k}^0)^H H^0 h_{0k},
\]
where \(A_{0k,4}^0\) is defined in (17).

Based on [40, Corollary 1], we obtain
\[
\frac{1}{N_t} (h_{0k}^0)^H (V_{eq})^H A_{0k,3}^0 V_{eq} h_{0k}
\]
\[
\xRightarrow{N_t \to \infty} \frac{1}{N_t} \left[ \sum_{t=1, t \neq k}^K [A_{0k,4}^0]_{tt} \text{tr} \left( R_{0k}^0 h_{0t}^0 (h_{0t}^0)^H R_{0k}^0 \right) \right]
\]
\[
+ [A_{0k,4}^0]_{kk} \text{tr}^2 (R_{0k}^0)
\]
\[
\xRightarrow{N_t \to \infty} \frac{1}{N_t} \left[ \sum_{t=1, t \neq k}^K [A_{0k,4}^0]_{tt} \text{tr} (R_{0k}^0 R_{0t}^0) \right]
\]
\[
+ [A_{0k,4}^0]_{kk} \text{tr}^2 (R_{0k}^0)
\]
(57)

For the second term on the right hand side of (55), we have
\[
\frac{1}{N_t} (\tilde{n}_{eq})^H (V_{eq})^H A_{0k,3}^0 V_{eq} \tilde{n}_{eq}
\]
\[
\xRightarrow{N_t \to \infty} \frac{1}{N_t} (V_{eq})^H A_{0k,3}^0 (V_{eq})
\]
\[
= \frac{1}{N_t} \sum_{t=1, t \neq k}^K [A_{0k,4}^0]_{tt} \text{tr} (h_{0t}^0 (h_{0t}^0)^H)
\]
\[
= \frac{1}{N_t} \sum_{t=1, t \neq k}^K [A_{0k,4}^0]_{tt} \text{tr} (R_{0t}^0).
\]
(60)

Combining (55)–(60) yields
\[
\frac{1}{N_t} \left\| \tilde{n}_{eq,0k} \right\|^2 \xRightarrow{N_t \to \infty} \frac{1}{N_t} a_{0k,1}^0
\]
(61)

where \(a_{0k,1}^0\) is defined in (15).

For the numerator in (51), we have (62), given at the top of the next page, where \(A_{0k,1}^0\) and \(A_{0k,2}^0\) are defined in (18) and (17), respectively.

According to the definition of \(V_{eq}^0\) in (49), we obtain
\[
\frac{1}{N_t} (h_{0k}^0)^H (V_{eq})^H A_{0k,2}^0 V_{eq} h_{0k}
\]
\[
= \frac{1}{N_t} (h_{0k}^0)^H [h_{01}, \ldots, h_{0K}] R_0^{-1/2} A_{0k,2}^0 h_{0k}
\]
\[
\times R_0^{-1/2} [h_{01}, \ldots, h_{0K}] H^0 h_{0k}
\]
\[
= \frac{1}{N_t} \sum_{t=1}^K (h_{0k}^0)^H h_{0t}^0 [A_{0k,5}^0]_{tt} (h_{0t}^0)^H H^0 h_{0k}
\]
\[
= \frac{1}{N_t} \sum_{t=1}^K (h_{0k}^0)^H h_{0t}^0 [A_{0k,5}^0]_{tt} \text{tr} (h_{0t}^0) H^0 h_{0k}
\]
\[
\xrightarrow{N_t \to \infty} \frac{1}{N_t} \sum_{t=1}^K (h_{0k}^0)^H h_{0t}^0 [A_{0k,5}^0]_{tt} \text{tr}^2 (R_{0k}^0) + \frac{1}{N_t} \sum_{t=1}^K [A_{0k,5}^0]_{tt} \text{tr} (R_{0k}^0 R_{0t}^0).
\]
(63)

We can further simplify (63) as follows:
\[
\frac{1}{N_t} (h_{0k}^0)^H (V_{eq})^H A_{0k,2}^0 V_{eq} h_{0k}
\]
\[
\xrightarrow{N_t \to \infty} \frac{1}{N_t} (V_{eq})^H A_{0k,2}^0 V_{eq} h_{0k}
\]
\[
\xrightarrow{N_t \to \infty} \frac{1}{N_t} \sum_{t=1}^K (A_{0k,5}^0)_{tt} \text{tr}^2 (R_{0k}^0)\]
\[
\xrightarrow{N_t \to \infty} \frac{1}{N_t} \sum_{t=1, t \neq k}^K [A_{0k,5}^0]_{tt} \text{tr}^2 (R_{0k}^0).
\]
(64)

Then, we have
\[
\frac{1}{N_t} (h_{0k}^0)^H (V_{eq})^H A_{0k,2}^0 V_{eq} h_{0k}
\]
\[
\xrightarrow{N_t \to \infty} \frac{1}{N_t} \sum_{t=1, t \neq k}^K [A_{0k,5}^0]_{tt} \text{tr}^2 (R_{0k}^0) + \frac{1}{N_t} \sum_{t=1}^K [A_{0k,5}^0]_{tt} \text{tr} (R_{0k}^0 R_{0t}^0).
\]
(65)

Also, we have
\[
\frac{1}{N_t} (\tilde{n}_{eq,0k})^H (V_{eq})^H A_{0k,2}^0 V_{eq} h_{0k}
\]
\[
\xrightarrow{N_t \to \infty} \frac{1}{N_t} \sum_{t=1, t \neq k}^K [A_{0k,5}^0]_{tt} \text{tr}^2 (R_{0k}^0) + \frac{1}{N_t} \sum_{t=1}^K [A_{0k,5}^0]_{tt} \text{tr} (R_{0k}^0 R_{0t}^0).
\]
(66)

Substituting (65) and (66) into (62), we obtain
\[
\frac{1}{N_t} (h_{0k}^0)^H (V_{eq})^H A_{0k,2}^0 V_{eq} h_{0k}
\]
\[
\xrightarrow{N_t \to \infty} \frac{1}{N_t} P_0 (P_0) \left( [A_{0k,5}^0]_{tt} \text{tr}^2 (R_{0k}^0) + \frac{1}{N_t} \sum_{t=1}^K [A_{0k,5}^0]_{tt} \text{tr} (R_{0k}^0 R_{0t}^0) + \frac{1}{N_t} \sum_{t=1}^K [A_{0k,5}^0]_{tt} \text{tr} (R_{0k}^0 R_{0t}^0) \right) + \frac{1}{N_t} P_0 N_0 R_0^0
\]
\[
\times \left( [A_{0k,4}^0]_{kk} \text{tr}^2 (R_{0k}^0) + \sum_{t=1}^K [A_{0k,4}^0]_{tt} \text{tr} (R_{0k}^0 R_{0t}^0) \right)
\]
(67)

\[
\text{tr} (R_{0k}^0 R_{0t}^0)
\]
(68)
\[
\frac{1}{N_t} (\hat{h}_{0k}^0) H (V_{eq}^0)^H \hat{h}_{eq,0k} (\hat{h}_{eq,0k}) H V_{eq}^0 h_{0k}^0 \\
= \frac{1}{N_t} (h_{0k}^0) H (V_{eq}^0) H \sqrt{P_0} V_{eq}^0 R_{0k}^0 (V_{eq}^0) H (N_0 I_K + \tau P_0 V_{eq}^0 R_{0k}^0 (V_{eq}^0))^{-1} \left( \sqrt{P_0} V_{eq}^0 h_{0k}^0 + V_{eq}^0 \tilde{n}_{eq} \right) \\
\times \sqrt{P_0} (\sqrt{P_0} V_{eq}^0 h_{0k}^0 + V_{eq}^0 \tilde{n}_{eq}) H (N_0 I_K + \tau P_0 V_{eq}^0 R_{0k}^0 (V_{eq}^0))^{-1} V_{eq}^0 R_{0k}^0 (V_{eq}^0) H V_{eq}^0 h_{0k}^0 \\
= \frac{1}{N_t} P_0 (\sqrt{P_0} V_{eq}^0 h_{0k}^0 + V_{eq}^0 \tilde{n}_{eq}) H (N_0 I_K + \tau P_0 V_{eq}^0 R_{0k}^0 (V_{eq}^0))^{-1} V_{eq}^0 R_{0k}^0 (V_{eq}^0) H V_{eq}^0 h_{0k}^0 \\
\times (h_{0k}^0) H (V_{eq}^0) H V_{eq}^0 R_{0k}^0 (V_{eq}^0) H (N_0 I_K + \tau P_0 V_{eq}^0 R_{0k}^0 (V_{eq}^0))^{-1} (\sqrt{P_0} V_{eq}^0 h_{0k}^0 + V_{eq}^0 \tilde{n}_{eq}) \\
\times (h_{0k}^0) H (V_{eq}^0) H V_{eq}^0 R_{0k}^0 (V_{eq}^0) H (N_0 I_K + \tau P_0 V_{eq}^0 R_{0k}^0 (V_{eq}^0))^{-1} (\sqrt{P_0} V_{eq}^0 h_{0k}^0 + V_{eq}^0 \tilde{n}_{eq}) \\
\rightarrow \frac{1}{N_t} P_0 \left( \sqrt{P_0} V_{eq}^0 h_{0k}^0 + V_{eq}^0 \tilde{n}_{eq} \right) H (N_0 I_K + \tau P_0 A_{00,1})^{-1} A_{00,1} V_{eq}^0 h_{0k}^0 \\
\times (h_{0k}^0) H (V_{eq}^0) H A_{00,1} \left( N_0 I_K + \tau P_0 A_{00,1} \right)^{-1} \left( \sqrt{P_0} V_{eq}^0 h_{0k}^0 + V_{eq}^0 \tilde{n}_{eq} \right) \\
\times (h_{0k}^0) H (V_{eq}^0) H A_{00,1} A_{00,2} V_{eq}^0 h_{0k}^0 + (h_{0k}^0) H (V_{eq}^0) H A_{00,1} A_{00,2} V_{eq}^0 \tilde{n}_{eq} \right),
\]

(62)

Substituting (65) and (68) into (61), we obtain

\[
\frac{1}{N_t} \left| g_{0,k}^0 \right|^2 \rightarrow \frac{1}{N_t} \left| \tilde{h}_{eq,0}^0 \right|^2 \rightarrow \frac{1}{N_t} \left| P \tilde{A}_{00,2} \frac{1}{N_t} \tilde{A}_{00,1} \right|^2.
\]

(69)

For \( g_{0,k}^0 \), we obtain

\[
\left| g_{0,k}^0 \right|^2 = P (h_{0k}^0) H (V_{eq}^0) H \tilde{h}_{eq,0}^0 \left| \tilde{h}_{eq,0}^0 \right|^2 V_{eq}^0 h_{0k}^0.
\]

(70)

Following a similar approach as in (52)–(61), the denominator of (76) is given by

\[
\frac{1}{N_t} \left| \tilde{h}_{eq,0}^0 \right|^2 = \frac{1}{N_t} P_0 \left( P_0 \tau^2 \sum_{p=1, p \neq t}^K A_{0,t,4}^0 A_{0,t,4}^0 \tau^2 (R_{0p}^0 R_{0p}^0) + [A_{0,t,4}^0]_{tt} \tau^2 (R_{0p}^0) + \tau N_0 \sum_{p=1}^K A_{0,t,4}^0 A_{0,t,4}^0 \tau^2 (R_{0p}^0) \right) = a_{0,t,1}^0.
\]

(71)

For the numerator of (76), we have (72), given at the top of the next page.

Substituting the expression for \( V_{eq}^0 \) in (49) into (72), we obtain (73), given at the top of the next page.

By applying [40, Corollary 1] to \( h_{0k}^0 \) \( h_{01}^0 \ldots h_{0K}^0 \), we have

\[
\frac{1}{N_t} (h_{0k}^0) H (V_{eq}^0) H \tilde{h}_{eq,0k} (\tilde{h}_{eq,0k}) H V_{eq}^0 h_{0k}^0 \\
\rightarrow \frac{1}{N_t} (P_0 \tau)^2 tr (R_{0k}^0) [A_{0,t,5}^0]_{kk} e_k^H h_{0k}^0 \ldots h_{0k}^0] H h_{0k}^0 \\
\times (h_{0k}^0) H h_{0k}^0 \ldots h_{0k}^0) e_k tr (R_{0k}^0) [A_{0,t,5}^0]_{kk} \\
+ \frac{1}{N_t} P_0 tr (R_{0k}^0) [A_{0,t,5}^0]_{kk} e_k^H h_{0k}^0 \ldots h_{0k}^0] H \tilde{n}_{eq} \\
\times (\tilde{n}_{eq}) H h_{0k}^0 \ldots h_{0k}^0)_{0k}^{1/2} e_k tr (R_{0k}^0) [A_{0,t,5}^0]_{kk},
\]

(74)

which can be simplified further as

\[
\frac{1}{N_t} (h_{0k}^0) H (V_{eq}^0) H \hat{h}_{eq,lt} (\hat{h}_{eq,lt}) H V_{eq}^0 h_{0k}^0 \\
= \frac{1}{N_t} \left( P_0 \tau tr (R_{0k}^0) [A_{0,t,5}^0]_{kk} \right)^2 (h_{0k}^0) H h_{0k}^0 \ldots h_{0k}^0] H h_{0k}^0 \\
+ \frac{1}{N_t} P_0 tr (R_{0k}^0) [A_{0,t,5}^0]_{kk}^2 (h_{0k}^0) H \tilde{n}_{eq} \tilde{n}_{eq}^H h_{0k}^0 \\
\rightarrow \frac{1}{N_t} \left( P_0 \tau N_0 \tau^3 tr (R_{0k}^0) [A_{0,t,5}^0]_{kk} \right)^2 \\
= b_{0,t,k}^0.
\]

(75)

By combining (69), (71), and (75), we obtain

\[
\frac{1}{N_t} \left| g_{lt,k}^0 \right|^2 \rightarrow \frac{1}{N_t} \left| \tilde{h}_{eq,lt}^0 \right|^2 \rightarrow \frac{1}{N_t} \left| P \tilde{A}_{lt,1} \right|^2.
\]

(76)

Then, we consider \( g_{lt,k}^0 \), which leads to

\[
\frac{P}{N_t} \left| g_{lt,k}^0 \right|^2 = \frac{P}{N_t} (h_{lt,k}^0) H (V_{eq}^0) H \hat{h}_{eq,lt} (\hat{h}_{eq,lt}) H V_{eq}^0 h_{lt,k}^0.
\]

(77)

Following a similar approach as in (52)–(61), the denominator of (77) is obtained as

\[
\frac{1}{N_t} \left| \tilde{h}_{eq,lt}^0 \right|^2 \rightarrow \frac{1}{N_t} \left| P \tau^2 \sum_{p=1, p \neq t}^K [A_{lt,4}^l]_{pp} tr (R_{lt}^l R_{lt}^l) \\
+ [A_{lt,4}^l]_{tt} \tau^2 (R_{lt}^l) \right| \\
+ \tau N_0 \sum_{p=1}^K [A_{lt,4}^l]_{pp} tr (R_{lt}^l) \\
= a_{lt,1}^l.
\]

(78)
Based on (50), we can re-express (79) as (80), given at the top of the next page.

For the numerator of (77), we have (79), given at the top of the next page.

Substituting (81) and (82) into (80), we obtain

\[
\frac{1}{N_t} \left( h_{0k}^0 \right)^H (V_{eq}^0)^H \hat{h}_{eq,0l} \hat{h}_{eq,0l}^H V_{eq}^0 h_{0k}^0 = \frac{1}{N_t} \left( h_{0k}^0 \right)^H (V_{eq}^0)^H \hat{h}_{eq,0l} \hat{h}_{eq,0l}^H V_{eq}^0 h_{0k}^0 = \frac{1}{N_t} \left( h_{0k}^0 \right)^H (V_{eq}^0)^H \hat{h}_{eq,0l} \hat{h}_{eq,0l}^H V_{eq}^0 h_{0k}^0 \]

\[
= \frac{1}{N_t} \left( h_{0k}^0 \right)^H (V_{eq}^0)^H \left( \frac{\sqrt{P_t} V_{eq}^0 R_{l,t}^i (V_{eq}^0)^H}{N_0 I_K + \tau P_t V_{eq}^0 R_{l,t}^i (V_{eq}^0)^H} \right)^{-1} \left( \sqrt{P_t} V_{eq}^0 h_{lt}^i + V_{eq}^0 \tilde{n}_{eq} \right) \hat{h}_{eq,0l} \hat{h}_{eq,0l}^H V_{eq}^0 h_{0k}^0 \]

\[
N_t \rightarrow \infty \frac{1}{N_t} \left( h_{0k}^0 \right)^H (V_{eq}^0)^H \hat{h}_{eq,0l} \hat{h}_{eq,0l}^H V_{eq}^0 h_{0k}^0 \]

For the numerator of (77), we have (79), given at the top of the next page.

Based on (50), we can re-express (79) as (80), given at the top of the next page.

For the first term on the right hand side of (80), we have (81), given at the top of the next page.

For the second term on the right hand side of (80), we have (82), given at the top of the next page.
By combining (77), (78), and (83), we obtain
\[
\frac{1}{N_t} (h_{lk}^H V_{eq}^H)^H \hat{n}_{eq,lt}^H V_{eq}^H V_{lk}^0
\]
\[
= \frac{1}{N_t} P_l \left( \sqrt{P_l} \tau \sum_{\ell=1}^{\tau} e_{\ell}^H V_{eq}^H V_{eq}^H A_{lt,1}^H A_{lt,2}^H R_{lk}^{-1/2} [h_{l1}^l, \ldots, h_{lK}^l]^H R_{lk}^0 [h_{l1}^l, \ldots, h_{lK}^l] R_{lk}^{-1/2} \right)
\times A_{lt,1}^H A_{lt,2}^H \left( \sqrt{P_l} \tau \sum_{\ell=1}^{\tau} e_{\ell}^H V_{eq}^H V_{eq}^H \right)
\times \left( \sqrt{P_l} \tau \sum_{\ell=1}^{\tau} e_{\ell}^H V_{eq}^H V_{eq}^H \right)
\Rightarrow N_t \rightarrow \infty \frac{1}{N_t} P_l \tau^2 \left( h_{lt}^H (V_{eq}^H)^H A_{lt,1}^H A_{lt,2}^H R_{lk}^{-1/2} [h_{l1}^l, \ldots, h_{lK}^l]^H R_{lk}^0 [h_{l1}^l, \ldots, h_{lK}^l] R_{lk}^{-1/2} A_{lt,1}^H A_{lt,2}^H V_{eq}^H h_{lt}
\right.
\left. + \frac{1}{N_t} P_l (\tilde{n}_{eq})^H (V_{eq}^H)^H A_{lt,1}^H A_{lt,2}^H R_{lk}^{-1/2} [h_{l1}^l, \ldots, h_{lK}^l]^H R_{lk}^0 [h_{l1}^l, \ldots, h_{lK}^l] R_{lk}^{-1/2} A_{lt,1}^H A_{lt,2}^H V_{eq}^H \tilde{n}_{eq}. \right)

(80)

Substituting (69), (76), (77), and (85) into (7) completes the proof.

REFERENCES

Chao-Kai Wen (S’00–M’04) received the Ph.D. degree from the Institute of Communications Engineering, National Tsing Hua University, Taiwan, in 2004. He was with the Industrial Technology Research Institute, Hsinchu, Taiwan, and MediaTek Inc., Hsinchu, from 2004 to 2009, where he was involved in broadband digital transceiver design. Since 2009, he has been with the Institute of Communications Engineering, National Sun Yat-sen University, Kaohsiung, Taiwan, where he is currently a Professor. His research interest includes the optimization in wireless multimedia networks.

Wen Chen is currently a Professor of wireless communications with Shanghai Jiao Tong University. His area of expertise covers massive access, network coding, and MIMO-OFDM. In these areas, he has published 95 papers in IEEE journals and more than 100 papers in IEEE conferences. Dr. Chen received the Ariyama Memorial Research Award in 1997, the JSPS Fellowship in 1999, and the PIMS Fellowship in 2001. He received the Honors of New Century Excellent Scholar in China in 2006 and the Pujiang Excellent Scholar in Shanghai in 2007. He received the Shanghai Excellent Master Thesis Supervision Award and the Best Paper Award of Chinese Information Theory Society in 2013, the Best Service Award of the Chinese Institute of Electronics and the Best Presentation Paper Awards of the Chinese Information Theory Society in 2014, the Innovate 5G Competition Award and the IEEE WCSP Best Paper Award in 2015, the IEEE APCC Keynote Speaker Appreciation in 2016, the Excellent Ph.D. Thesis Supervision Award of the Chinese Institute of Communications in 2018, and the Excellent Researcher Award of the Chinese Institute of Electronics in 2019. He received the IEEE VTS 2018 Chapter-of-the-Year Award. He is an IEEE Distinguished Lecturer of the Communications Society. He is the Shanghai Chapter Chair of the IEEE Vehicular Technology Society. He is an Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON COMMUNICATIONS, and the IEEE ACCESS.

Shi Jin (S’06–M’07–SM’17) received the B.S. degree in communications engineering from the Guilin University of Electronic Technology, Guilin, China, in 1996, the M.S. degree from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2003, and the Ph.D. degree in information and communications engineering from Southeast University, Nanjing, in 2007. From 2007 to 2009, he was a Research Fellow with Adas-tral Park Research Campus, University College Lon-don, London, U.K. He is currently with the faculty of the National Mobile Communications Research Laboratory, Southeast Uni-versity. His research interests include space–time wireless communications, random matrix theory, and information theory. He and his coauthors received the 2011 IEEE Communications Society Stephen O. Rice Prize Paper Award in the field of communication theory and the 2010 Young Author Best Paper Award from the IEEE Signal Processing Society. He serves as an Associate Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE COMMUNICATIONS LETTERS, and the IET Communications.

Robert Schober (S’98–M’01–SM’08–F’10) was born in Neuenetdettelsau, Germany, in 1971. He received the Diplom (Univ.) and Ph.D. degrees in electrical engineering from the University of Erlangen-Nuernberg in 1997 and 2000, respectively. From 2001 to 2002, he was a Post-Doctoral Fellow with the University of Toronto, Canada, sponsored by the German Academic Exchange Service (DAAD). Since 2002, he has been with The University of British Columbia (UBC), Vancouver, Canada, where he is currently a Full Professor. Since 2012, he has been an Alexander von Humboldt Professor and the Chair for Digital Communication at Universität Erlangen-Nürnberg (FAU), Erlangen, Germany. His research interests fall into the broad areas of communication theory, wireless communications, and statistical signal processing.

Dr. Schober is a fellow of the Canadian Academy of Engineering and the Engineering Institute of Canada. He received several awards for his work, including the 2002 Heinz Maier-Leibnitz Award of the German Science Foundation (DFG), the 2004 Innovations Award of the Vodafone Foundation for Research in Mobile Communications, the 2006 UBC Killam Research Prize, the 2007 Wilhelm Friedrich Bessel Research Award of the Alexander von Humboldt Foundation, the 2008 Charles McDowell Award for Excellence in Research from UBC, the 2011 Alexander von Humboldt Professorship, and the 2012 NSERC E.W.R. Steacie Fellowship. In addition, he received the Best Paper Awards from the German Information Technology Society (ITG), the European Association for Signal, Speech and Image Processing (EURASIP), the IEEE WCNC 2012, the IEEE Globecom 2011, the IEEE ICUWB 2006, the International Zurich Seminar on Broadband Communications, and European Wireless 2000. From 2012 to 2015, he was the Editor-in-Chief of the IEEE TRANSACTIONS ON COMMUNICATIONS. He currently serves as a Member-at-Large on the Board of Governors of the IEEE Communication Society and the Chair of the IEEE TRANSACTIONS ON MOLECULAR, BIOLOGICAL AND MULTISCALE COMMUNICATIONS.

Giuseppe Caire (S’92–M’94–SM’03–F’05) was born in Torino in 1965. He received the B.Sc. degree in electrical engineering from the Politecnico di Torino in 1990, the M.Sc. degree in electrical engineering from Princeton University in 1992, and the Ph.D. degree from the Politecnico di Torino in 1994. He has been a Post-Doctoral Research Fellow with the European Space Agency (ESTEC), Noordwijk, The Netherlands, from 1994 to 1995, an Assistant Professor in telecommunications with the Politecnico di Torino, an Associate Professor with the University of Parma, Italy, a Professor with the Department of Mobile Communications, the Eurecom Institute, Sophia-Antipolis, France, and a Professor of electrical engineering with the Viterbi School of Engineering, University of Southern California, Los Angeles, CA, USA. He is currently an Alexander von Humboldt Professor with the Faculty of Electrical Engineering and Computer Science, Technical University of Berlin, Germany. His main research interests include communications theory, information theory, and channel and source coding with particular focus on wireless communications.

Dr. Caire was a recipient of the Jack Neubauer Best System Paper Award from the IEEE Vehicular Technology Society in 2003, the IEEE Communications Society and Information Theory Society Joint Paper Award in 2004 and 2011, the Okawa Research Award in 2014, the Vodafone Innovation Prize in 2015, and the ERC Advanced Grant in 2018. He has served in the Board of Governors of the IEEE Information Theory Society from 2004 to 2007, and as an Officer from 2008 to 2013. He was the President of the IEEE Information Theory Society in 2011.