Secure Communication in Relay-Assisted Massive MIMO Downlink

Santosh Timilsina and Gayan Amarasuriya
Department of Electrical and Computer Engineering, Southern Illinois University, Carbondale, IL, USA 62901
Email: {santosh.timilsina, gayan.baduge}@siu.edu

Abstract—In this paper, secure transmission strategies for the relay-assisted massive multiple-input multiple-output (MIMO) downlink are investigated by using artificial noise (AN) generation and by exploiting the excess degrees-of-freedom through the random and null-space based precoders. The achievable rate expressions are derived for the estimated channel state information, and hence, the detrimental effects of channel estimation errors in designing precoders are quantified. Specifically, the achievable secrecy rate at the relayed user nodes is derived in closed-form, and thereby, the performance gap between the random and null-space based precoders is investigated. Our performance analysis reveals that the AN generation by using random precoders can be employed to design secure physical layer transmission strategies for the relay-assisted massive MIMO downlink systems. The AN generation can be useful in the finite antenna regime for guaranteeing physical layer security in the base-station-to-relay hop of the relay-assisted massive MIMO downlink. Although the AN generated at the base-station propagates to the relay-to-user hop via amplify-and-forward operation at the relay, sophisticated security provisions are needed to secure the end-to-end transmission when the relay is equipped with finitely many antennas. Consequently, the performance gap between the random and null-space based precoders gradually diminishes in the limit of infinitely many base-station antennas. Nevertheless, the achievable secrecy rate steadily vanishes with an increasing number of antennas at the passive eavesdropper.

I. INTRODUCTION

Establishing a secure communication over the wireless medium is a significant challenge due to its broadcast nature [1]–[3]. As a remedy, traditional cryptographic encryption methods have been widely adopted in higher layers to guarantee information security. However, most of these conventional cryptographic techniques have been designed based on the key assumption that the eavesdropper’s computational capability and resources will be inadequate for successful information intrusions. Moreover, with the recent proliferation of mobile Internet, Internet-of-things and enhanced signal/information processors, higher layer cryptographic techniques may be increasingly vulnerable and insufficient for guaranteeing information security over wireless channels [1]–[3]. Secure transmission strategies, which provision physical layer security, are currently being investigated as a practically viable complement to these traditional high-layer encryption techniques. In particular, secure transmission designs in physical layer exploit the key characteristics of wireless medium, and consequently, there have been several promising and established techniques to enhance wireless security. These techniques include secure channel codes [4]–[6], cooperative jamming [7], and artificial noise (AN) generation [8]. In this paper, secure transmission designs based on generation of AN sequences are investigated for the relay-assisted massive multiple-input multiple-output (MIMO) downlink.

Massive MIMO has a great potential to boost the physical layer performance through unprecedented spectral/energy efficiency gain and significantly enhances the link reliability. The combination of physical layer security and massive MIMO can boost the performance of physical-layer designs with highly confidential and mission critical transmissions. Some of the recent seminal research contributions to the development of physical layer security can be summarized as follows: All these contributions are based on the wiretap channel model investigated by Wyner [4]. In [8], it has been shown that the achievable secrecy rate can be gained by generating AN, which can significantly degrade the eavesdropper’s channel quality. In [9], it is shown that by generating AN from the cooperative relays, everlasting secrecy can be obtained even when the number of uniformly distributed eavesdroppers is larger than the number of user nodes. In [10], secrecy rate optimization techniques are investigated for a conventional MIMO channel by employing a multi-antenna cooperative jammer to improve secure communication in the presence of a multi-antenna eavesdropper.

Recently, physical layer security for the single-hop massive MIMO systems in the presence of passive and active eavesdroppers has been studied. In [11], the effects of passive and active eavesdropper attacks with their detection schemes have been investigated. Similarly, the references [12]–[14] investigate the secure data transmission designs in massive MIMO systems in the presence of passive eavesdroppers. In [15], the effects of co-located and distributed eavesdroppers are explored with a single legitimate user, and the average secrecy rate is maximized even in the worst-case design by using AN-aided jamming. In [13], the effects of active eavesdropping in multi-cell multi-user massive MIMO have been investigated by using the matched-filter precoding and AN generation in order to combat the multi-antenna active eavesdropper for enhancing the achievable secrecy rate. In [14], secrecy rates and secrecy outage probabilities for both perfect and imperfect channel state information (CSI) for single-hop massive MIMO systems are studied.

All aforementioned contributions [11]–[14] investigate physical layer security for single-hop massive MIMO systems. Recently, in [16], reliable secure communication in single-cell multi-user massive MIMO relaying network with a multi-antenna passive eavesdropper has been studied by deriving the achievable asymptotic secrecy rate. The system model of [16] consists of a massive MIMO enabled relay, which assists the end-to-end transmission between the spatially distributed user nodes and a destination with finitely many antennas in the presence of a multiple-antenna eavesdropper. In particular,
I. System, channel and signal model

In this section, the system, channel, and signal models are presented.

A. System and channel model

We consider a relay-assisted massive MIMO downlink in which an $N_T$-antenna BS provisions secure communication to $K$ spatially distributed single-antenna user nodes ($U_k$) for $k \in \{1, \cdots, K\}$ through an $N_R$-antenna amplify-and-forward (AF) relay node ($R$). A passive $N_E$-antenna eavesdropper solicits to spy on the information transmitted to the user nodes. It is assumed that the number of antennas at the relay is greater than the number of user nodes, whereas the number of BS antennas can grow without bound (i.e. $N_T > N_R > K$).

The channel between the BS and relay is denoted by $\mathbf{F}$. Similarly, $\mathbf{G}$ represents the channel between the relay and user nodes, and $\mathbf{E}$ denotes the channel between BS and eavesdropper. The channel between the relay and eavesdropper is denoted by $\mathbf{H}$. The aforementioned channels can be modeled in a uniform manner as follows:

$$\mathbf{A} = \mathbf{D}_A^{1/2} \tilde{\mathbf{A}},$$

where $\tilde{\mathbf{A}} \sim CN_{m \times n}(0_{m \times n}, \mathbf{I}_m \otimes \mathbf{I}_n)$ captures the independent, frequency-flat small-scale Rayleigh fading. The matrix dimension $(m, n)$ corresponding to the channel matrices $\mathbf{F}, \mathbf{G}, \mathbf{E}, \mathbf{H}$ are given by $(N_R, N_T), (K, N_R), (N_E, N_T)$ and $(N_R, N_R)$, respectively. Furthermore, the $m \times n$ diagonal matrix $\mathbf{D}_A$ accounts the path-loss having $|\mathbf{D}_A|_{k,k} = \zeta_{Ak}$ as the $k$th diagonal element where $A \in \{\mathbf{F}, \mathbf{G}, \mathbf{E}, \mathbf{H}\}$. Since the BS and relay antenna arrays are collocated, the diagonal matrix $\mathbf{D}_F$ is modeled as $\mathbf{D}_F = \zeta_{F} \mathbf{I}_{N_R}$.

B. Acquisition of channel state information

In this subsection, the CSI acquisition technique is presented. In massive MIMO, the estimation of the downlink channel at the user nodes is impractical due to the very large number of the BS antennas and the short coherence interval of the respective wireless channels [18]. To this end, the uplink channel $\mathbf{F}^T$ is estimated at the BS, and $\mathbf{G}^T$ is estimated at the relay by using pilot sequences transmitted from each of the relay antennas and the user nodes, respectively. The downlink channel estimates are obtained via the channel reciprocity in time division duplexing (TDD) mode of operation [18]. Thus, the minimum mean square error estimates (MMSE) of $\mathbf{F}$ and $\mathbf{G}$ can be derived as [19].
\[\alpha^2_R = P_r / \left( P_t \mathbb{E} \left[ \text{Tr} \left( \mathbf{F} \mathbf{W} \left( \mathbf{F} \mathbf{W}^H \right)^T \right) \right] + P_n \sigma_n^2 \mathbb{E} \left[ \text{Tr} \left( \mathbf{F} \mathbf{V}_n \left( \mathbf{F} \mathbf{V}_n^H \right)^T \right) \right] + N_R \sigma_R^2 \right), \] (10)

\[y_{U_k} = \alpha_R \sqrt{P_t} \mathbf{g}_k \mathbf{F} \bar{\mathbf{w}}_k x_{s_k} + \sum_{i=1, i \neq k}^{K} \alpha_R \sqrt{P_t} \mathbf{g}_i x_{s_i} + \alpha_R \sqrt{P_t} \mathbf{g}_k \mathbf{F} \mathbf{V}_n z_n + \alpha_R \mathbf{g}_k \mathbf{n}_k + n_{U_k}, \] (12)

\[y_{E_{k,2}} = \alpha_R \sqrt{P_t} \mathbf{h}_k \mathbf{F} \bar{\mathbf{w}}_k x_{s_k} + \sum_{i=1, i \neq k}^{K} \alpha_R \sqrt{P_t} \mathbf{h}_i x_{s_i} + \alpha_R \sqrt{P_t} \mathbf{h}_k \mathbf{F} \mathbf{V}_n z_n + \alpha_R \mathbf{h}_k \mathbf{n}_k + n_{E_k}, \] (16)

where \( \mathbf{g}_n \) is the additive white Gaussian noise (AWGN) vector at relay satisfying \( \mathbb{E} \left[ \mathbf{n}_R \mathbf{n}_R^H \right] = \sigma_n^2 \mathbf{I}_N_R \). Then, the relay amplifies this received signal by applying an amplification factor \( (\alpha_R) \). Thus, the transmitted signal by the relay can be written as follows:

\[x_R = \alpha_R y_R = \alpha_R \left( \sqrt{P_t} \mathbf{F} \bar{\mathbf{W}} \mathbf{x}_s + \sqrt{P_t} \mathbf{F} \mathbf{V}_n z_n + \mathbf{n}_R \right), \] (9)

where \( \mathbf{n}_R \) is given in (10) at the top of the page, and \( P_t \) represents the transmit power of the relay. In the second time-slot, the relay forwards the amplified signal towards the user nodes. The received signal at the user nodes can be written as

\[y_U = \alpha_R \sqrt{P_t} \mathbf{G} \mathbf{F} \bar{\mathbf{W}} \mathbf{x}_s + \alpha_R \sqrt{P_t} \mathbf{G} \mathbf{F} \mathbf{V}_n z_n + \alpha_R \mathbf{G} \mathbf{n}_n + \mathbf{n}_U, \] (11)

where \( \mathbf{n}_U \) is the AWGN vector at user nodes satisfying \( \mathbb{E} \left[ \mathbf{n}_U \mathbf{n}_U^H \right] = \sigma_n^2 \mathbf{I}_N_E \). Thereby, the received signal at the kth user node can be written as (12) at the top of the page. Meanwhile, the eavesdropper seeks to intercept the information received from the signals transmitted by the BS and relay during the first and second time-slots, respectively. The received signal at the eavesdropper during the first time-slot can be written as

\[y_{E,1} = \sqrt{P_t} \mathbf{E} \mathbf{W} \mathbf{x}_s + \sqrt{P_t} \mathbf{E} \mathbf{V}_n \mathbf{z}_n + \mathbf{n}_E. \] (13)

C. Signal model

In this subsection, the signal models for the user nodes and the eavesdropper are presented. The end-to-end transmission for the relay channel is performed in two orthogonal time-slots as the relay is a half-duplex terminal. In the first time-slot, the BS transmits the signal towards the relay by using a ZF precoder. Since, the eavesdropper’s CSI is not available at the BS, it transmits an AN sequence for degrading the eavesdropper’s ability to intercept the transmitted signals. In this context, the transmitted signal vector at the BS can be written as

\[y_T = \sqrt{P_t} \bar{\mathbf{W}} x_T + \sqrt{P_t} \mathbf{V}_n z_n, \] (5)

where \( P_t \) and \( P_n \) are the transmit power allocated for the user symbols and AN sequence at the BS, respectively. Furthermore, \( \bar{\mathbf{W}} \) is the ZF precoder, \( x_T \) is the transmit symbol vector satisfying \( \mathbb{E} \left[ \mathbf{x}_T \mathbf{x}_T^H \right] = \mathbf{I}_K \), and \( \mathbf{V}_n \in \mathcal{C} \mathcal{N}(\mathbf{0}, \mathbf{I}_N_R) \) is the AN shaping matrix at the BS. Moreover, \( z_n \) is the AN vector and can be defined as \( z_n \sim \mathcal{C} \mathcal{N}(\mathbf{0}, \mathbf{I}_N_R, \sigma_n^2 \mathbf{I}_N_R) \). The ZF precoder is constructed by using the cascaded relay channel as

\[\bar{\mathbf{W}} = \beta_1 \left( \mathbf{G} \mathbf{F} \right)^H \left( \mathbf{G} \mathbf{F} \left( \mathbf{G} \mathbf{F}^H \right)^{-1} \right)^{-1}. \] (6)

where \( \beta_1 \) is the power normalization factor defined as

\[\beta_1 = \left( \mathbb{E} \left[ \text{Tr} \left( \mathbf{G} \mathbf{F} \left( \mathbf{G} \mathbf{F}^H \right)^{-1} \right) \right] \right)^{-1/2}. \] (7)

The received signal at the relay can be written as

\[y_R = \sqrt{P_t} \mathbf{F} \bar{\mathbf{W}} x_s + \sqrt{P_t} \mathbf{F} \mathbf{V}_n z_n + \mathbf{n}_R, \] (8)

The received signal at the eavesdropper through the relay’s transmission during the second time-slot can be written as

\[y_{E,2} = \sqrt{P_t} \mathbf{F} \mathbf{H} \bar{\mathbf{W}} x_s + \alpha_R \sqrt{P_t} \mathbf{F} \mathbf{H} \mathbf{V}_n z_n + \alpha_R \mathbf{H} \mathbf{n}_R + \mathbf{n}_{E,2}. \] (14)

Next, the kth user’s information leaked into the eavesdropper during the second time-slot can be written as (16) at the top of the page.

D. Precoder designs for transmission of AN sequences

In this subsection, two precoder designs for securing the downlink transmissions of the relay-assisted massive MIMO system are presented.

1) Random AN Precoder: A random AN precoder can be constructed by using a pseudo-inverse of a random matrix as

\[\mathbf{V}_n = \frac{\mathbf{R}_n^H \left( \mathbf{R}_n \mathbf{R}_n^H \right)^{-1} \mathbf{n}_n}{\sqrt{\mathbb{E} \left[ \text{Tr} \left( \mathbf{R}_n \mathbf{R}_n^H \right) \right]}}. \] (17)

where \( \mathbf{R}_n \sim \mathcal{C} \mathcal{N}(\mathbf{0}, \mathbf{I}_N_R, \mathbf{I}_N_R \otimes \mathbf{I}_N_T) \) and the elements of \( \mathbf{R}_n \) are independent and identically distributed random variables [14].
2) Null-space based AN Precoder: The null-space based AN precoder at the BS can be constructed such that the transmitted signal power lies in the null-space of the cascaded relay channel. The useful signal power leaked into the eavesdropper can be minimized. To this end, the null-space based precoder can be designed as [12]

\[
V_n = U \sqrt{E[\text{Tr}(UU^H)]},
\]

where \( U \) is defined as

\[
U = I_{NT} - (\hat{G}\hat{F})^H (\hat{G}\hat{F}(\hat{G}\hat{F})^H)^{-1} \hat{G}\hat{F}.
\]

The null-space based precoder in (18) is designed for the cascaded relay channel GF. Thus, the channels \( G \) and \( F \) need to be estimated, and hence, it is constructed based on the estimated/imperfect CSI.

III. ACHIEVABLE RATE DEFINITIONS

In this section, the achievable rate definitions are presented.

A. Achievable rate definitions

Since the user nodes do not have access to the estimated CSI, the worst-case Gaussian approximation technique is used for the achievable rate analysis [20]. To this end, the received signal at the \( k \)th user node can be decomposed into the desired signal and the uncorrelated noise as follows:

\[
y_{U_k} = \alpha_R \sqrt{P_t} \mathbb{E}[g_k \hat{F} \hat{w}_k] x_{U_k} + \bar{n}_k,
\]

where \( \bar{n}_k \) is the effective noise signal and can be defined as

\[
\bar{n}_k = \alpha_R \sqrt{P_t} (g_k \hat{F} \hat{w}_k - E[g_k \hat{F} \hat{w}_k]) x_{U_k} + \sum_{i=1, i \neq k}^K \alpha_R \sqrt{P_t} g_k \hat{F} \hat{w}_i x_{U_i}
\]

\[+ \alpha_R \sqrt{P_t} g_k \hat{F} \hat{V}_n z_n + \alpha_R g_k \hat{H} R + n_u_k.
\]

Noting that the desired signal component is uncorrelated with the effective noise components and each noise term is pairwise uncorrelated, the achievable rate at the \( k \)th user node can be defined by treating the noise as uncorrelated worst-case Gaussian noise as follows:

\[
\mathcal{R}_{U_k} = \min(T_{c_1} - T_{p_1} - T_{c_2} - T_{p_2}) \log \left( 1 + \frac{\alpha_R^2 P_t \mathbb{E}[\|g_k \hat{F} \hat{w}_k\|^2]}{\sum_{j=1}^K P_{l_j} + \sigma_n^2} \right)
\]

where \( T_{c_1} \) and \( T_{c_2} \) are the coherence times intervals from relay to BS and user nodes to relay, and the interference power terms \( P_{l_j} \)'s for \( j \in \{1, \ldots, 4\} \) are defined as

\[
P_{l_1} = \alpha_R^2 P_t \mathbb{V}[g_k \hat{F} \hat{w}_k],
\]

\[
P_{l_2} = \sum_{i=1, i \neq k}^K \alpha_R^2 P_t \mathbb{E}[\|g_k \hat{F} \hat{w}_i\|^2],
\]

\[
P_{l_3} = \alpha_R^2 \sigma_n^2 P_t \mathbb{E}[\|g_k \hat{F} \hat{V}_n\|^2],
\]

\[
P_{l_4} = \alpha_R^2 \mathbb{E}[\|g_k \hat{H} R\|^2].
\]

B. Rate leaked into eavesdropper

Since the BS and relay transmit in two orthogonal time-slots, the eavesdropper has two opportunities of intercepting the information intended for the \( k \)th user node. Thus, the rate leaked into the eavesdropper during the first time-slot can be defined as

\[
\mathcal{R}_{E_k,1} = \log \left( \frac{P_t \mathbb{E}[\|e_k \hat{w}_l\|^2]}{\sum_{i=1, i \neq k}^K P_{l_i} \mathbb{E}[\|e_k \hat{w}_i\|^2] + \sigma_n^2 + \sigma_E^2} \right)
\]

Similarly, the rate leaked into the eavesdropper during the second time-slot can be defined as

\[
\mathcal{R}_{E_k,2} = \log \left( 1 + \frac{\alpha_R^2 P_t \mathbb{E}[\|e_k \hat{w}_l\|^2]}{\sum_{i=1, i \neq k}^K P_{l_i} + \sigma_E^2} \right),
\]

where \( P_{l_i} \)'s for \( i \in \{1, 2, 3\} \) are given by

\[
P_{l_1} = \sum_{i=1, i \neq k}^K \alpha_R^2 P_t \mathbb{E}[\|e_k \hat{w}_i\|^2],
\]

\[
P_{l_2} = \alpha_R^2 \mathbb{E}[\|e_k \hat{V}_n\|^2],
\]

\[
P_{l_3} = \alpha_R^2 \mathbb{E}[\|e_k \hat{H} R\|^2].
\]

Then, the cumulative information leakage rate into the eavesdropper during two time-slots can be written as

\[
\mathcal{R}_{E_k} = \frac{1}{2} (\mathcal{R}_{E_k,1} + \mathcal{R}_{E_k,2}).
\]

For the worst-case scenario, we can assume that the eavesdropper is able to cancel the inter-pair terms. This case leads to an upper bound on the rate leaked into the eavesdropper. Hence, the average rates leaked into the eavesdropper during the first and second time-slots can alternatively written as [12]

\[
\mathcal{R}_{E_k,1} = \mathbb{E} \left[ \log \left( 1 + P_t \hat{w}_l^H \hat{E} \hat{H}^H \hat{C}_1^{-1} \hat{E} \hat{w}_k \right) \right],
\]

\[
\mathcal{R}_{E_k,2} = \mathbb{E} \left[ \log \left( 1 + \alpha_R^2 P_t \mathbb{E}[\|e_k \hat{V}_n\|^2] \right) \right],
\]

where \( \mathbb{C}_1 \) and \( \mathbb{C}_2 \) are effective noise correlation matrices and defined as

\[
\mathbb{C}_1 = \sigma_n^2 \mathbb{E}[\hat{V}_n \hat{V}_n^H] + \sigma_E^2 \mathbb{I}_{N_E},
\]

\[
\mathbb{C}_2 = \alpha_R^2 \sigma_n^2 \mathbb{E}[\hat{V}_n \hat{V}_n^H] + \alpha_R^2 \mathbb{H}^H \mathbb{H}^H + \sigma_E^2 \mathbb{I}_{N_E}.
\]

C. Secrecy rate definition

The achievable secrecy rate can be defined as

\[
\mathcal{R}_{S_k} = \mathbb{R}_{U_k} - \mathbb{R}_{E_k},
\]

where \( [\lambda]^+ = \max(0, \lambda) \).

IV. ACHIEVABLE RATE ANALYSIS

In this section, the achievable rates are derived for an unlimited number of BS antennas, while keeping the number of relay antennas and number of user nodes fixed at finite values.

A. Achievable rate analysis for the \( k \)th user node

The transmit power of the BS is scaled inversely proportional to the square-root of the number of BS antennas as \( P_t = E_t / \sqrt{N_T} \). Then by letting \( N_T \to \infty \), the achievable rate at the \( k \)th user node can be derived by using (22) as shown in (32) at the top of the next page (see Appendix A for the derivation). In (32), \( P_{l_1}^\infty \) and \( P_{l_2}^\infty \) are defined as

\[
P_{l_1}^\infty = \alpha_R^2 P_t E_t \mathbb{E}[\hat{G}_l^2] \left( \zeta_{G_k} - \zeta_{G_l} \right) \zeta_{G_k}^{-1},
\]

\[
P_{l_2}^\infty = \sum_{i=1, i \neq k}^K \alpha_R^2 P_t E_t \mathbb{E}[\hat{G}_l^2] \left( \zeta_{G_k} - \zeta_{G_l} \right) \zeta_{G_k}^{-1}.
\]

In (32), (33), and (34), \( \sigma_R^2 \) is given by

\[
\sigma_R^2 = P_t / (E_t P_t E_t \mathbb{E}[\hat{G}_l^2] + N_T \sigma_R^2).
\]
where $P_{N} = 8$, $K = 8$, and $N_{R} = 10$. $T_{p1} = N_{R}$, $T_{p2} = K$ and $T_{c1} = T_{c2} = 196$. NS = null-space and ED = eavesdropper.

**B. Information rate leakage into the eavesdropper**

As $N_{T} \to \infty$, the information rate that is leaked into the eavesdropper during the first and second time-slots can be derived as (see Appendix B for the derivation)

$$R_{E_{k,1}}^\infty = 0,$$

$$R_{E_{k,2}}^\infty = \log \left( 1 + \frac{\alpha_{R}^{2} E_{R} T_{p1} E_{R1} (N_{R} - K) \zeta_{k}^{2}}{\sum_{j=1}^{2} P_{j1}^{\infty} + \left[ \alpha_{R}^{2} N_{R} K \zeta_{k} \sigma_{R}^{2} + \sigma_{E}^{2} \right] \text{Tr} \left( D_{G}^{-1} \right) } \right).$$

(36a)

where $P_{j1}^{\infty}$ is given by

$$P_{j1}^{\infty} = \sum_{i=1,i \neq j}^{K} \alpha_{R}^{2} E_{R} T_{p1} E_{R1} \zeta_{k} \zeta_{i} \hat{G}_{k}. \zeta_{i}^{-1}.$$ (36b)

Then the total information rate that is leaked into the eavesdropper can be written as

$$R_{E_{k}}^\infty = \frac{1}{2} \log \left( 1 + \frac{\alpha_{R}^{2} E_{R} T_{p1} E_{R1} \zeta_{k} \zeta_{k} \hat{G}_{k} \zeta_{k}^{-1}}{P_{j1}^{\infty} + \left[ \alpha_{R}^{2} N_{R} K \zeta_{k} \sigma_{R}^{2} + \sigma_{E}^{2} \right] \text{Tr} \left( D_{G}^{-1} \right) } \right).$$ (38)

**Remark IV.1:** As per (36a), during the first time-slot, the rate leaked into the eavesdropper vanishes as $N_{T} \to \infty$. Nevertheless, during the second time-slot, it can be seen from (36b) that a non-zero rate is leaked into the eavesdropper even in the asymptotic BS antenna regime. Thus, the overall rate leaked into the eavesdropper is indeed non-zero as given in (38). This non-zero rate leakage is due to the fact that the eavesdropper is capable of intruding the secure transmissions during the second time-slot as the relay is equipped with finitely many antennas. Nevertheless, cooperative jamming can be employed as the BS remains silent during the second time-slot. In this context, the BS can transmit a jamming signal to weaken the useful signal interception at the eavesdropper during the second time-slot. Cooperative jamming with the massive MIMO BS will be investigated in an extended version of this paper.

**C. Secrecy rate analysis**

The secrecy rate of the $k$th user node can be derived by using (31), (32) and (38) as (39) at the top of this page.

**V. Numerical Results**

In this section, the performance of the proposed secure transmission designs is investigated via numerical results. The channels $F$, $E$, $H$ and $G$ are modeled as independently distributed Rayleigh fading. The pathloss is modeled as $P_{L} \propto \left( d_{m,n}/d_{0} \right)^{\nu}$, where $d_{0}$, $d_{m,n}$ and $\nu$ are reference distance, distance between the node $m$ and node $n$, and pathloss exponent, respectively.

In Fig. 2, the achievable rates for (i) the $k$th user node, (ii) the rate leaked into the eavesdropper, and (iii) the corresponding secrecy rate are plotted as a function of the average first hop SNR. The achievable rate curves relevant to the theoretical analysis are plotted by using (32), (38) and (39). In particular, in Fig. 2, the achievable secrecy rates for (i) random AN precoding and (ii) null-space based AN precoding techniques are compared. The Fig. 2 clearly depicts that the null-space based precoding technique provides a slightly higher secrecy rate in...
the low-to-moderate SNR regime. However, in the high SNR regime, the achievable secrecy rates of both these techniques approach the same. Moreover, Fig. 2 clearly shows that even the null-space based AN precoding does not guarantee full secrecy when the the precoder is designed by using estimated CSI with channel estimation errors. This observation is partly due to the unsecured transmission in the second time-slot. In Fig. 3, the achievable secrecy rate for the $k$th user node is plotted against the number of antennas at the eavesdropper, while keeping the numbers of antenna at relay and BS fixed, by using (32) and (28). Fig. 3 reveals that the achievable secrecy rate gradually decreases with increasing number of eavesdropper antennas. When $N_E > 10$, the achievable rate at the $k$th user node drops below the rate leaked into the eavesdropper and consequently yielding a zero secrecy rate at the $k$th user node. This observation is due to the fact that the eavesdropper’s capability of intercepting the secure transmission of the $k$th user node enhances with the increasing number of degrees-of-freedom available at the eavesdropper.

VI. CONCLUSION

Secure transmission strategies for the relay-assisted massive MIMO downlink have been investigated by exploiting the generation of AN to minimize the information leakage to the multi-antenna eavesdropper. The achievable secrecy rate expression for the AN generation through a random precoder has been derived and compared against the conventional and more complicated null-space based precoding. The performance of the proposed secure communication model is investigated for estimated CSI, and thereby, the adverse impacts of channel estimation errors have been studied. Our analysis reveals that the computationally efficient random precoders can be used for transmission of AN sequences instead of more complicated precoders based on the null-space of the cascaded relay channel with gradually diminishing information leakage into the eavesdroppers with increasing number of BS antennas.

APPENDIX A

DERIVATION OF (32)

In this appendix, the derivation of the $k$th user’s achievable rate (32) is outlined. To begin with, we invoke the asymptotic channel orthogonality from [21]: As $M \to \infty$, the column vectors of $\hat{A}$ become orthogonal [21]:

$$\lim_{M \to \infty} \frac{[\hat{A}]_i^H [\hat{A}]_j}{M} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases} \quad \text{and} \quad \lim_{M \to \infty} [\hat{A}]_i^H [\hat{A}]_j = D_A.$$ (40)

By using (2a), (6), (40) and by letting $P_{R_1} = E_{R_1}/\sqrt{N_T}$, $\hat{W}$ can be asymptotically approximated as

$$\lim_{N_T \to \infty} \sqrt{N_T} \hat{W} = \frac{\zeta_F^2}{T_{R_1} E_{R_1}} \beta_1 \left( \hat{G} \right)^H \left( \hat{G} \right)^{-1}. \quad (41)$$

By substituting (2a) into (7), an asymptotic expression for $\beta_1^2/\sqrt{N_T}$ can be derived as in (42) at the top of this page. In deriving (42), the identity from random matrix theory [21]

$$E \left[ \text{Tr} \left( \left( \hat{G} \hat{G}^H \right)^{-1} \right) \right] = \text{Tr} \left( \hat{D}_G^{-1} \right) / (N_R - K). \quad (43)$$

has been invoked. Similarly, by using (40) and (41), the asymptotic expressions for $\hat{F} \hat{W}$ and $\hat{F} \hat{V}_n$ can be derived as shown in (44) and (45) at the top of this page. By first substituting (44) and (45) into (10) and then by letting $N_T \to \infty$, an asymptotic expression for $\alpha_R$ can be derived as in (35). By substituting (44) into (22), the desired signal power $P_S$ and the interference-plus-noise power terms $P_I$’s can be re-written as

$$P_S = \alpha_R^2 E_{R_1} \frac{E_1}{\sqrt{N_T}} |E[g_k \hat{z}_k]|^2, \quad (46a)$$

$$P_{I_1} = \alpha_R^2 E_{R_1} \frac{E_1}{\sqrt{N_T}} \text{Var}[g_k \hat{z}_k], \quad (46b)$$

$$P_{I_2} = \sum_{i=1, i \neq k}^K \alpha_R^2 E_{R_1} \frac{E_1}{\sqrt{N_T}} E\left[ |g_k \bar{z}_i|^2 \right], \quad (46c)$$

$$P_{I_3} = \alpha_R^2 \frac{E_1}{\sqrt{N_T}} E\left[ |g_k \hat{F} \hat{V}_n|^2 \right], \quad (46d)$$

$$P_{I_4} = \alpha_R^2 E\left[ |g_k \hat{F} \hat{V}_n|^2 \right], \quad (46e)$$

where $\hat{Z}$ is defined in (44).

1) Compute $E[g_k \hat{z}_k]$ : By substituting $\hat{Z}$, $g_k \hat{z}_k$ can be computed as follows:

$$g_k \hat{z}_k = \left( \hat{G} + E \bar{G} \right) \hat{z}_k \left( \hat{G} \hat{G}^H \right)^{-1} = 1 + E \bar{G} \hat{z}_k. \quad (47)$$

where $E \bar{G}_k$ is the $k$th row of $E \bar{G}$. Since $\bar{z}_k$ and $E \bar{G}_k$ are independent, $E[\bar{G}_k \hat{z}_k] = 0$ and $E[\bar{G}_k \hat{z}_k] = 0$. Thus, we have

$$E[g_k \hat{z}_k] = 1. \quad (48)$$

2) Compute $\text{Var}[g_k \hat{z}_k]$ : Similarly, by using (47), $\text{Var}[g_k \hat{z}_k]$ can be computed as $\text{Var}[g_k \hat{z}_k] = \text{Var}[\bar{G}_k \hat{z}_k]$. By substituting $\hat{z}_k$ and by using (43), $\text{Var}[\bar{G}_k \hat{z}_k]$ can be computed as

$$\text{Var}[\bar{G}_k \hat{z}_k] = E\left[ \bar{G}_k \hat{z}_k \hat{z}_k^H \bar{G}_k^H \right] = E\left[ \bar{G}_k \bar{G}_k^H \right] E\left[ \text{Tr} \left( \hat{Z} \hat{Z}^H \right) \right] = (\zeta_k - \zeta_k) \zeta_k^{-1} / (N_R - K). \quad (49)$$
3) Compute \( \mathbb{E}[\|g_k \hat{z}_k\|^2] \): By using steps similar to those in (49), \( \mathbb{E}[\|g_k \hat{z}_k\|^2] \) can be computed as
\[
\mathbb{E}[\|g_k \hat{z}_k\|^2] = \left( \zeta_{G_k} - \zeta_{G_k} \right) \zeta_{G_k}^{-1}(N_R - K). \tag{50}
\]

4) Compute \( \mathbb{E}[\|g_k FV_n\|^2] \): Since, \( F, G, \) and \( V_n \) are pairwise independent, we can compute \( \mathbb{E}[\|g_k FV_n\|^2] \) using (45) as
\[
\mathbb{E}[\|g_k FV_n\|^2] = 0. \tag{51}
\]

5) Compute \( \mathbb{E}[\|\hat{g}_k n_R\|^2] \): Since the noise and the channel are independent, we can compute
\[
\mathbb{E}[\|\hat{g}_k n_R\|^2] = \sigma_R^2 \mathbb{E}[\|g_k\|^2] = N_R \zeta_{G_k} \sigma_R^2. \tag{52}
\]

By substituting (48), (49), (50), (51), and (52) into (46), and by letting \( N_T \to \infty \), the desired asymptotic achievable rate at the 4th user node can be derived as (32).

**APPENDIX B**

**DERIVATION OF (38)**

In this appendix, the derivation of (38) is outlined. Since, \( F, \) and \( N_F \) are pairwise independent, by using (40), we can show that
\[
\lim_{N_T \to \infty} \mathbb{E} F^H / N_T = 0, \quad \text{and} \quad \lim_{N_T \to \infty} \mathbb{E} F^H / N_T = 0. \tag{53}
\]

By using (41) and (53), asymptotic expressions for \( \mathbb{E} \hat{W} \) and \( \mathbb{E} V_n \) are derived as shown in (54) and (55), respectively, at the top of this page. By substituting (54) and (55) into (24), the asymptotic rate leaked into the eavesdropper in first time-slot can be derived as shown in (36a).

Similarly, by letting \( N_T \to \infty \) and by substituting (44) into (26), the desired signal power \( P_J \), and interference-plus-noise power terms \( P_J \) can be re-written as
\[
P_J \beta_2 = \alpha_R \beta_2 E_{\|h_k z_k\|^2}, \quad P_J = \sum_{i=1}^{K} \alpha_R \beta_2 E_{\|h_k z_k\|^2}, \tag{56a}
\]
\[
P_J \beta_2 = \alpha_R \beta_2 P_{\|h_k FV_n\|^2}, \quad \text{and} \quad P_J = \alpha_R \beta_2 E_{\|h_k n_R\|^2}. \tag{56b}
\]

1) Compute \( \mathbb{E}[\|h_k z_k\|^2] \): By using steps similar to those in (49), \( \mathbb{E}[\|h_k z_k\|^2] \) can be computed as
\[
\mathbb{E}[\|h_k z_k\|^2] = \zeta_{H_k} \zeta_{G_k}^{-1}/(N_R - K). \tag{57}
\]

2) Compute \( \mathbb{E}[\|h_k \hat{z}_k\|^2] \): Similar to above, it can be shown that
\[
\mathbb{E}[\|h_k \hat{z}_k\|^2] = \zeta_{H_k} \zeta_{G_k}^{-1}/(N_R - K). \tag{58}
\]

3) Compute \( \mathbb{E}[\|h_k FV_n\|^2] \): By using (45), it can be shown that
\[
\mathbb{E}[\|h_k FV_n\|^2] = 0. \tag{59}
\]

4) Compute \( \mathbb{E}[\|h_k n_R\|^2] \): One can readily show that
\[
\mathbb{E}[\|h_k n_R\|^2] = N_R \zeta_{H_k} \sigma_R. \tag{60}
\]

By substituting (57), (58), (59) and (60) into (56), and by letting \( N_T \to \infty \) the desired asymptotic rate leaked into the eavesdropper during the second time-slot can be derived as shown in (38).