entropy

MDPI

Article

Artificial Noise-Aided Physical Layer Security in Underlay Cognitive Massive MIMO Systems with Pilot Contamination

Hayder Al-Hraishawi [1,*], Gayan Amarasuriya Aruma Baduge [1] and Rafael F. Schaefer [2]

[1] Department of Electrical and Computer Engineering, Southern Illinois University, Carbondale, IL 62901, USA; gayan.baduge@siu.edu

[2] Information Theory and Applications Chair, Technische Universität Berlin, Berlin 10587, Germany; rafael.schaefer@tu-berlin.de

[*] Correspondence: hayder.a@siu.edu

Received: 2 June 2017; Accepted: 27 June 2017; Published: 10 July 2017

Abstract: In this paper, a secure communication model for cognitive multi-user massive multiple-input multiple-output (MIMO) systems with underlay spectrum sharing is investigated. A secondary (cognitive) multi-user massive MIMO system is operated by using underlay spectrum sharing within a primary (licensed) multi-user massive MIMO system. A passive multi-antenna eavesdropper is assumed to be eavesdropping upon either the primary or secondary confidential transmissions. To this end, a physical layer security strategy is provisioned for the primary and secondary transmissions via artificial noise (AN) generation at the primary base-station (PBS) and zero-forcing precoders. Specifically, the precoders are constructed by using the channel estimates with pilot contamination. In order to degrade the interception of confidential transmissions at the eavesdropper, the AN sequences are transmitted at the PBS by exploiting the excess degrees-of-freedom offered by its massive antenna array and by using random AN shaping matrices. The channel estimates at the PBS and secondary base-station (SBS) are obtained by using non-orthogonal pilot sequences transmitted by the primary user nodes (PUs) and secondary user nodes (SUs), respectively. Hence, these channel estimates are affected by intra-cell pilot contamination. In this context, the detrimental effects of intra-cell pilot contamination and channel estimation errors for physical layer secure communication are investigated. For this system set-up, the average and asymptotic achievable secrecy rate expressions are derived in closed-form. Specifically, these performance metrics are studied for imperfect channel state information (CSI) and for perfect CSI, and thereby, the secrecy rate degradation due to inaccurate channel knowledge and intra-cell pilot contamination is quantified. Our analysis reveals that a physical layer secure communication can be provisioned for both primary and secondary massive MIMO systems even with the channel estimation errors and pilot contamination.

Keywords: massive MIMO; pilot contamination; cognitive radio; physical layer security; artificial noise

1. Introduction

Massive multiple-input multiple-output (MIMO) is currently being investigated as one of the key enabling technologies for the 5th generation wireless standard [1]. Specifically, in massive MIMO systems, very large antenna arrays are used for aggressive spatial multiplexing and focusing radiated energy towards desired spatial directions [2,3]. Thereby, massive MIMO can potentially provide unprecedented gains in spectral and energy efficiencies compared to conventional MIMO.

Confidentiality of transmitted information is one of the key challenges for system designers of next generation wireless communication networks [4]. To protect confidential communication against intruders and eavesdropper attacks, the concept of physical layer security [5–9] has recently attracted significant interest to complement current cryptographic approaches on higher layers. These techniques realize secure communication directly at the physical layer by exploiting the noisiness and imperfection of the wireless communication channel for degrading the quality of signal reception at eavesdroppers, and thereby prevent them from eavesdropping upon the confidential information from the intercepted signals [4].

Another concept that promises significant gains in performance for wireless communication networks are so-called *cognitive radio networks*. These cognitive networks allow secondary systems to access the licensed spectrum of the primary systems by exploiting the underlay spectrum sharing techniques, and thereby, mitigating the spectrum under-utilization of current wireless systems and significantly improving the spectral efficiency [10]. In cognitive radio systems, where the primary spectrum is an open medium to be accessed and utilized by the secondary systems, achieving end-to-end security is a crucial challenge to the system designs and configurations. Information theoretic secrecy provisioning for cognitive radio networks has been investigated, e.g., in [11,12].

In the event that the eavesdroppers intercept confidential signals passively, they do not transmit in order to conceal their existence. Therefore, the acquisition of the channel state information (CSI) of the eavesdropping channels at the massive MIMO base-stations (BSs) will be difficult. Although the null-space beamforming techniques can be effectively used in conventional MIMO BS for provisioning of physical layer security, constructing such sophisticated precoders at the massive MIMO BSs will be prohibitively complicated. Alternatively, artificial noise (AN) sequences can be exploited for massive MIMO BSs. In this context, massive MIMO techniques can be used in cognitive radio systems for provisioning physical layer security by exploiting the large antenna arrays at the BSs to simultaneously transmit confidential signals towards the legitimate user nodes and AN sequences towards eavesdroppers for perturbing the intercepted signals.

Notwithstanding that the massive MIMO techniques have received significant interest recently, little research exists on securing massive MIMO systems by exploiting physical layer security strategies. Next, some of the important contributions to the development of physical layer provisioning in massive MIMO systems are summarized. In [13], a secure transmission scheme for single-hop massive MIMO systems is investigated by deriving the secrecy rates and secrecy outage probabilities for perfect and imperfect CSI. Furthermore, in [14], the effects of linear precoding of data and AN in secure massive MIMO downlink are studied. Specifically, in [14], linear precoders that are based on matrix polynomials are proposed for both data and AN precoding, and consequently, the corresponding polynomial coefficients are optimized to minimize the sum mean-squared error and the AN leakage to the user nodes. In [15], optimal power allocation with security constraints in multi-user massive MIMO systems with distributed antennas is investigated. Moreover, in [16], the physical layer security and energy efficiency aspects are investigated for massive MIMO-enabled heterogeneous cloud radio access networks.

Although there is a symbiotic relationship between massive MIMO and cognitive radio networks to achieve a groundbreaking spectral and energy efficiencies for future wireless systems, facilitating secrecy at the physical layer of cognitive massive MIMO systems has not yet received any attention in the existing studies in the literature. To fill this gap, in this paper, a secure downlink transmission strategy is investigated for cognitive massive MIMO systems with underlay spectrum sharing in the presence of a passive multi-antenna eavesdropper. To this end, a secondary massive MIMO system is allowed to access the licensed spectrum of a primary massive system subject to an interference temperature constraint, which is the maximum tolerable co-channel interference (CCI) power at the primary system. Consequently, the secondary transmit power is constrained such that the CCI inflicted at the primary system due to secondary concurrent transmission is maintained below this interference temperature. The motive of the eavesdropper is to intercept the confidential transmissions of the primary or secondary systems. By assuming that the eavesdropper's CSI is unavailable, AN sequences are generated at the primary base-station (PBS) for provisioning physical layer security by exploiting the additional degrees-of-freedom offered by its massive antenna array. The construction of null-space-based AN shaping precoders at the PBS is prohibitively complicated due to its massive antenna array, and hence, random AN shaping matrices are advocated. Furthermore, zero-forcing (ZF) based precoders are used at the PBS and the secondary base-station (SBS).

The uplink channels of the primary and secondary systems are estimated at the corresponding BSs by using pilots transmitted by the primary user nodes (PUs) and secondary user nodes (SUs), respectively. The number of orthogonal pilot sequences is limited and depends on the coherence interval of the wireless channels [2]. Hence, the same pilot sequence is shared among both PUs and SUs for minimum mean square error (MMSE) channel estimation. Nevertheless, a normalized pseudo-inverse of a complex Gaussian random matrix is used for AN shaping at the PBS, and thereby, the burden of estimating the eavesdropper's channels is avoided.

The performance of the aforementioned system set-up is investigated by deriving the achievable secrecy rates in closed-form for both imperfect and perfect channel state information (CSI) cases. The impacts of the numbers of PBS and SBS antennas are investigated in the context of provisioning physical layer secure transmission for cognitive massive MIMO systems. Furthermore, the detrimental effects of intra-cell secondary interference, channel estimation errors, intra-cell pilot contamination, and AN leakage into the desired signals at the PUs and SUs are investigated for the imperfect and perfect CSI cases. Thereby, the achievable secrecy rate degradation due to intra-cell pilot contamination and inaccurate channel estimation is quantified.

Notation: $\mathbf{A}^*$, $\mathbf{A}^T$, $\mathbf{A}^H$, and $[\mathbf{A}]_{k,l}$ denote the conjugate, transpose, Hermitian-transpose, and the (k,l)th element of a matrix $\mathbf{A}$, respectively. $\mathbb{E}[\cdot]$ is the expectation and the operator $\otimes$ denotes the Kronecker product.

2. System, Channel, and Signal Models

In this section, the system, channel, and signal models of a cognitive multi-user massive MIMO system are presented.

2.1. System and Channel Model

We consider a cognitive multi-user MIMO network with underlay spectrum sharing (see Figure 1). A multi-user secondary MIMO system is underlaid within a primary multi-user MIMO system. The secondary system shares the same licensed frequency spectrum of the primary system by exploiting the concepts of cognitive underlay spectrum sharing [10]. The primary system consists of an N_P-antennas PBS and K single-antenna PUs. In the secondary system, M single-antenna SUs are served by an N_S-antenna SBS. The ratio between the numbers of BS antennas at the primary and secondary systems is defined as $\beta = N_P/N_S$. The numbers of antennas at the PBS and SBS can grow without limit compared to the numbers of PUs and SUs, ($N_P \gg K$) and ($N_S \gg M$), while keeping a fixed ratio $\beta = N_P/N_S$. Moreover, an N_E-antenna eavesdropper seeks passively to eavesdrop upon the information transmitted to user nodes, either in the primary or secondary system.

Let $\mathbf{F}^T \in \mathbb{C}^{(K\times N_P)}$ be the channel matrix between the PBS and PUs, and $\mathbf{G}^T \in \mathbb{C}^{(M\times N_S)}$ is the channel matrix between the SBS and SUs. Here, $\mathbf{V}^T \in \mathbb{C}^{(K\times N_S)}$ and $\mathbf{U}^T \in \mathbb{C}^{(M\times N_P)}$ are the interference channel matrices between the SBS and PUs and between the PBS and SUs, respectively. Moreover, $\mathbf{H}_P^T \in \mathbb{C}^{(N_E\times N_P)}$ is the channel matrix between the PBS and the eavesdropper, and $\mathbf{H}_S^T \in \mathbb{C}^{(N_E\times N_S)}$ is the channel matrix between the SBS and the eavesdropper. For the sake of the brevity of exposition, all the aforementioned channels can be correspondingly defined in the following general expression:

$$\mathbf{C} = \mathbf{D}_C^{1/2}\tilde{\mathbf{C}}, \tag{1}$$

where $\mathbf{C} \in \{\mathbf{F}, \mathbf{G}, \mathbf{V}, \mathbf{U}, \mathbf{H}_P, \mathbf{H}_S\}$, $\tilde{\mathbf{C}} \sim \mathcal{CN}_{P\times Q}\left(\mathbf{0}_{P\times Q}, \mathbf{I}_P \otimes \mathbf{I}_Q\right)$ models the independent small-scale Rayleigh fading, and diagonal matrix $\mathbf{D}_C = \mathrm{diag}(\zeta_{C_1}, \cdots, \zeta_{C_Q})$ captures the path-loss.

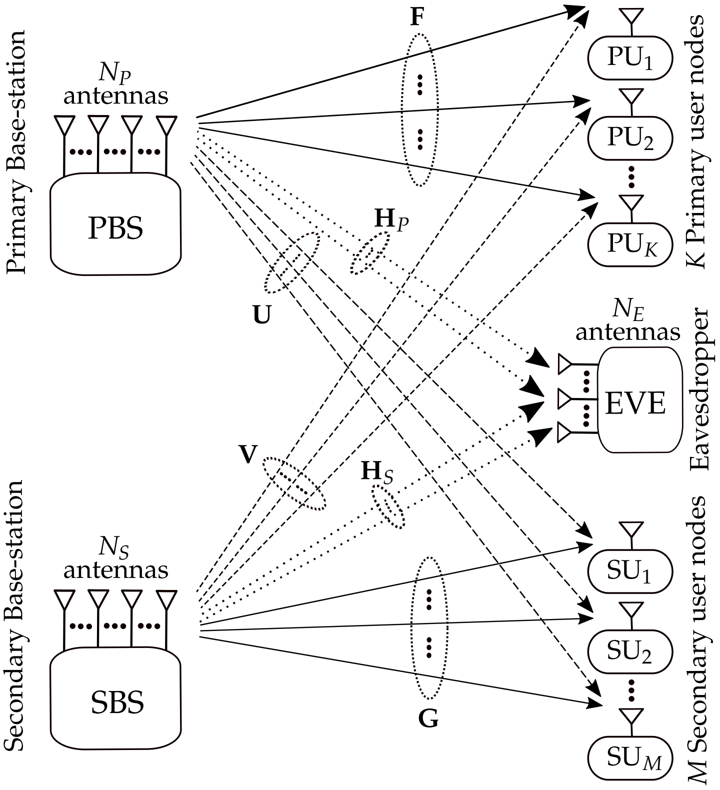

Figure 1. System model for a multi-user cognitive massive multiple-input multiple-output (MIMO) network in the presence of a multi-antenna eavesdropper. PBS: primary base station; SBS: secondary base station; PU: primary user node; SU: secondary user node.

2.2. Uplink Training and Channel Estimation

In massive MIMO systems, the uplink CSI is estimated at the BS from the uplink pilot sequences transmitted by the user nodes during the training period of the coherence interval (T). Then, the downlink channel is obtained from the uplink CSI by exploiting the channel reciprocity in time-division duplex (TDD) mode of operation. Here, for the sake of exposition, we assume that the numbers of PUs and SUs are the same ($K = M$). Therefore, all the PUs and SUs transmit simultaneously (τ) symbols of T as pilot sequences. The received pilot signals at the PBS and SBS are given by:

$$\mathbf{Y}_P = \sqrt{\tau P_U}\mathbf{F}\mathbf{\Phi}_P + \sqrt{\tau P_U}\mathbf{U}\mathbf{\Phi}_S + \mathbf{Z}_P, \tag{2a}$$

$$\mathbf{Y}_S = \sqrt{\tau P_U}\mathbf{G}\mathbf{\Phi}_S + \sqrt{\tau P_U}\mathbf{V}\mathbf{\Phi}_P + \mathbf{Z}_S, \tag{2b}$$

respectively, where P_U is the average transmit power of each pilot symbol, $\mathbf{\Phi}_P$ is a $K \times \tau$ pilot symbol matrix transmitted by the PUs, where $\mathbf{\Phi}_P^H$ is a $\tau \times K$ unitary matrix ($\tau \geq K$) satisfying $\mathbf{\Phi}_P\mathbf{\Phi}_P^H = \mathbf{I}_K$, and $\mathbf{\Phi}_S$ is an $K \times \tau$ pilot symbol matrix transmitted by the SUs, where $\mathbf{\Phi}_S^H$ is a $\tau \times K$ unitary matrix ($\tau \geq K$) satisfying $\mathbf{\Phi}_S\mathbf{\Phi}_S^H = \mathbf{I}_K$. Furthermore, $\mathbf{Z}_P$ and $\mathbf{Z}_S$ are additive white Gaussian noise (AWGN) matrices at the PBS and SBS with independent and identically distributed (i.i.d.) $\mathcal{CN}(0,1)$ elements, respectively. In (2), all pilot sequences are non-orthogonal, i.e., the primary and secondary systems share the same pilot sequences, i.e., $\mathbf{\Phi}_P = \mathbf{\Phi}_S = \mathbf{\Phi}$, which practically represents the worst-case scenario. Thus, the uplink channel estimates at the PBS and SBS are affected by pilot contamination, then the MMSE channel estimate of $\mathbf{F}$ can be derived as [3]:

$$\begin{aligned}\hat{\mathbf{F}} &= \frac{1}{\sqrt{\tau P_U}}\mathbf{Y}_P\mathbf{\Phi}_P\left(\mathbf{D}_F+\mathbf{D}_U+\frac{\mathbf{I}_K}{\tau P_U}\right)^{-1}\mathbf{D}_F \\ &= \left(\mathbf{F}+\mathbf{U}+\frac{\mathbf{Z}_F}{\sqrt{\tau P_U}}\right)\left(\mathbf{D}_F+\mathbf{D}_U+\frac{\mathbf{I}_K}{\tau P_U}\right)^{-1}\mathbf{D}_F, \end{aligned} \tag{3}$$

where $\mathbf{Z}_F = \mathbf{Z}_P\mathbf{\Phi}_P$ is an estimation noise matrix consisting of i.i.d. $\mathcal{CN}(0,1)$ elements. In (3), $\mathbf{F}$ and $\mathbf{Z}_F$ are statistically independent. Let $\boldsymbol{\mathcal{E}}_F$ be the estimation error matrix of $\mathbf{F}$. By using MMSE properties, the channel can be decomposed as:

$$\mathbf{F} = \hat{\mathbf{F}} + \boldsymbol{\mathcal{E}}_F. \tag{4}$$

From the property of MMSE estimation, $\hat{\mathbf{F}}$ and $\boldsymbol{\mathcal{E}}_F$ are independent. Furthermore, the rows of $\hat{\mathbf{F}}$ and $\boldsymbol{\mathcal{E}}_F$ are mutually independent and distributed as $\mathcal{CN}(\mathbf{0},\hat{\mathbf{D}}_F)$ and $\mathcal{CN}(\mathbf{0},\mathbf{D}_F-\hat{\mathbf{D}}_F)$, respectively, where $\hat{\mathbf{D}}_F$ is a diagonal matrix, whose k-th diagonal element is:

$$\sigma^2_{\hat{F}_k} = \frac{\tau P_U \zeta^2_{F_k}}{\tau P_U\left(\zeta_{F_k}+\zeta_{U_k}\right)+1}. \tag{5}$$

Next, by applying steps similar to those used for deriving (3), the MMSE channel estimate of $\mathbf{G}$ can be derived as follows:

$$\hat{\mathbf{G}} = \left(\mathbf{G}+\mathbf{V}+\frac{\mathbf{Z}_G}{\sqrt{\tau P_U}}\right)\left(\mathbf{D}_G+\mathbf{D}_V+\frac{\mathbf{I}_M}{\tau P_U}\right)^{-1}\mathbf{D}_G, \tag{6}$$

where $\mathbf{Z}_G = \mathbf{Z}_S\mathbf{\Phi}_S$ is a noise matrix with i.i.d. $\mathcal{CN}(0,1)$ random variables. Both $\mathbf{G}$ and $\mathbf{Z}_G$ in (6) are statistically independent. The estimation error matrix of $\mathbf{G}$ at SBS is denoted by $\boldsymbol{\mathcal{E}}_G$, where the channel can be decomposed as:

$$\mathbf{G} = \hat{\mathbf{G}} + \boldsymbol{\mathcal{E}}_G. \tag{7}$$

Again, $\hat{\mathbf{G}}$ and $\boldsymbol{\mathcal{E}}_G$ are independent. Also, the rows of $\hat{\mathbf{G}}$ and $\boldsymbol{\mathcal{E}}_G$ are mutually independent and distributed as $\mathcal{CN}(\mathbf{0},\hat{\mathbf{D}}_G)$ and $\mathcal{CN}(\mathbf{0},\mathbf{D}_G-\hat{\mathbf{D}}_G)$, respectively, where $\hat{\mathbf{D}}_G$ is a diagonal matrix whose m-th diagonal element is given by:

$$\sigma^2_{\hat{G}_m} = \frac{\tau P_U \zeta^2_{G_m}}{\tau P_U\left(\zeta_{G_m}+\zeta_{V_m}\right)+1}. \tag{8}$$

2.3. Signal Model

In this section, the signal model is presented, and thereby the signal-to-interference-plus-noise ratios (SINRs) are derived.

2.3.1. Transmit Power Constraint for the SBS

In underlay spectrum sharing cognitive systems, the power of the secondary transmissions is constrained such that the total interference power inflicted at the primary receivers is less than a predefined interference temperature [10]. Therefore, the transmit power of the SBS is constrained as follows:

$$P_S = \min\left(P_{S_{\max}}, \frac{I_P}{\mathbb{E}\left[\mathrm{Tr}\left(\mathbf{V}^T\hat{\mathbf{W}}_S\hat{\mathbf{W}}_S^H\mathbf{V}^*\right)\right]}\right), \tag{9}$$

where $P_{S_{\max}}$ is the maximum transmit power at the SBS. Furthermore, I_P is the primary interference temperature, which is the maximum tolerable interference level that the PUs can endure without compromising the quality-of-service. In (9), $\hat{\mathbf{W}}_S$ is the ZF precoder at the SBS and is defined as:

$$\hat{\mathbf{W}}_S = \alpha_S \hat{\mathbf{G}}^* \left(\hat{\mathbf{G}}^T \hat{\mathbf{G}}^*\right)^{-1}, \tag{10}$$

where α_S is a power normalization factor at the SBS and is defined as [17]:

$$\alpha_S = \left(\mathbb{E}\left[\mathrm{Tr}\left(\hat{\mathbf{G}}^T \hat{\mathbf{G}}^*\right)^{-1}\right]\right)^{1/2} = \sqrt{\frac{N_S - M}{\sum_{m=1}^{M} \sigma_{\hat{G}_m}^{-2}}}. \tag{11}$$

For a finite number of antennas at the SBS, the transmit power constraint can be re-written as:

$$P_S = \min\left(P_{S_{\max}}, \frac{I_P}{\Delta}\right), \tag{12}$$

where Δ is approximated as (see Appendix A.1 for derivation):

$$\begin{aligned} \Delta \approx\ & \alpha_S^2 \mathrm{Tr}\left(\left(\mathbf{D}_V^T + \mathbf{I}_M/\tau P_U\right)^2 \mathbf{D}_G^{-2}\right) + \frac{N_S - M}{N_S} \mathrm{Tr}\left(\mathbf{D}_G - \hat{\mathbf{D}}_G\right) \\ & + \frac{(N_S - M)}{N_S \tau P_U} \left(2\mathrm{Tr}\left(\mathbf{D}_G^T \left(\mathbf{D}_G^T + \mathbf{D}_V^T + \frac{\mathbf{I}_M}{\tau P_U}\right)^{-1}\right) - 1\right). \end{aligned} \tag{13}$$

Next, the asymptotic transmit power constraint at the secondary system for infinitely many BS antenna can be derived by letting N_S go to infinity in (12) as follows:

$$\min_{N_S \to \infty} P_S = P_{S_{\max}}. \tag{14}$$

Remark 1. *As $N_S \to \infty$, the secondary transmit power constraint (12) asymptotically becomes independent of the interference temperature of the primary system. Consequently, the secondary system with underlay spectrum sharing can be operated independent of the primary system, and hence, the secondary system can be asymptotically operated at its maximum transmit power level.*

2.3.2. Signal Model for the Primary System

It is assumed that the eavesdropper's CSI is unavailable at both PBS and SBS. Consequently, the PBS transmits an AN sequence for degrading the eavesdropper's ability to decode the signals transmitted to its PUs. To this end, the $N_P - K$ additional degrees-of-freedom offered by the large antenna array at the PBS are used to transmit this AN. Thus, the PBS transmits both confidential data and AN by using linear precoders in the downlink. In this context, the transmitted signal vector at the PBS can be written as:

$$\mathbf{x}_{P_t} = \sqrt{P_P} \hat{\mathbf{W}}_P \mathbf{x}_P + \sqrt{P_n} \mathbf{W}_n \mathbf{a}_n, \tag{15}$$

where P_P and P_n are the transmit powers allocated for confidential data and AN, respectively. In (15), $\hat{\mathbf{W}}_P$ is the precoder used for pre-processing the confidential data at the PBS. Furthermore, $\mathbf{W}_n \in \mathbb{C}^{N_P \times (N_P - K)}$ is the AN shaping matrix at the PBS, and $\mathbf{a}_n$ is the AN vector and defined as $\mathbf{a}_n \sim \mathcal{CN}_{(N_P-K)\times 1}\left(\mathbf{0}_{N_P-K}, \sigma_A^2 \mathbf{I}_{N_P-K}\right)$. In particular, $\hat{\mathbf{W}}_P$ is designed based on the ZF criterion as:

$$\hat{\mathbf{W}}_P = \alpha_P \hat{\mathbf{F}}^* \left(\hat{\mathbf{F}}^T \hat{\mathbf{F}}^*\right)^{-1}, \tag{16}$$

where α_P is a normalization constant, and is defined as:

$$\alpha_p = \left(\mathbb{E}\left[\mathrm{Tr}\left(\hat{\mathbf{F}}^T\hat{\mathbf{F}}^*\right)^{-1}\right]\right)^{1/2} = \sqrt{\frac{N_P - K}{\sum_{k=1}^{K}\sigma_{\hat{\mathbf{f}}_k}^{-2}}}. \tag{17}$$

The construction of the AN shaping matrix can be described as follows: In conventional MIMO systems, the AN shaping matrix ($\mathbf{W}_n$) can be constructed by computing the null space of the desired channel matrix ($\mathbf{F}$). In this context, the performance degradation due to the leakage of AN into desired signals can be mitigated. However, for a massive MIMO PBS, the computation of the null space based precoders is prohibitively complicated. Hence, $\mathbf{W}_n$ can be constructed as the pseudo-inverse of a random matrix with mutually independent Gaussian random vectors. To this end, the AN shaping matrix can be defined as follows:

$$\mathbf{W}_n = \alpha_n \mathbf{R}_n^* \left(\mathbf{R}_n^T\mathbf{R}_n^*\right)^{-1}, \tag{18}$$

where $\mathbf{R}_n^T \sim \mathcal{CN}_{(N_P-K)\times N_P}\left(\mathbf{0}_{(N_P-K)\times N_P}, \mathbf{I}_{N_P-K}\otimes \mathbf{I}_{N_P}\right)$, $\mathbf{W}_n \in \mathbb{C}^{N_P\times(N_P-K)}$, and α_n is defined as:

$$\alpha_n = \left(\mathbb{E}\left[\mathrm{Tr}\left(\mathbf{R}_n^T\mathbf{R}_n^*\right)^{-1}\right]\right)^{1/2} = \sqrt{\frac{K}{(N_P-K)}}. \tag{19}$$

In particular, $\mathbf{W}_n$ is designed as a normalized version of the pseudo-inverse of $\mathbf{R}_n$. Therefore, the aforementioned choice (18) facilitates the mathematical tractability of the asymptotic analysis.

The received signal vector at the PUs can be written as:

$$\mathbf{y}_P = \sqrt{P_P}\mathbf{F}^T\hat{\mathbf{W}}_P\mathbf{x}_P + \sqrt{P_S}\mathbf{V}^T\hat{\mathbf{W}}_S\mathbf{x}_S + \sqrt{P_n}\mathbf{F}^T\mathbf{W}_n\mathbf{a}_n + \mathbf{z}_P, \tag{20}$$

where $\mathbf{x}_P$ and $\mathbf{x}_S$ are the transmitted signal vectors of the PBS and SBS satisfying $\mathbb{E}\left[\mathbf{x}_P\mathbf{x}_P^H\right] = \mathbf{I}_K$ and $\mathbb{E}\left[\mathbf{x}_S\mathbf{x}_S^H\right] = \mathbf{I}_M$, respectively. Furthermore, $\mathbf{z}_P$ is the AWGN vector at the PUs satisfying $\mathbb{E}\left[\mathbf{z}_P\mathbf{z}_P^H\right] = \mathbf{I}_K\sigma_P^2$. In (20), the first term accounts for the desired signal transmitted towards the PUs. The second term captures the intra-cell interference due to the concurrent secondary transmissions in the same frequency band. Moreover, the third term represents the AN leakage into the PUs.

Then, the received signal at the k-th PU (i.e., the k-th element of $\mathbf{y}_P$) can be expressed as:

$$y_{P_k} = \sqrt{P_P}\mathbf{f}_k^T\hat{\mathbf{w}}_{P_k}x_{P_k} + \sum_{j=1,j\neq k}^{K}\sqrt{P_P}\mathbf{f}_k^T\hat{\mathbf{w}}_{P_j}x_{P_j} + \sqrt{P_S}\mathbf{v}_k^T\hat{\mathbf{W}}_S\mathbf{x}_S + \sqrt{P_n}\mathbf{f}_k^T\mathbf{W}_n\mathbf{a}_n + z_{P_k}, \tag{21}$$

where $\hat{\mathbf{w}}_{P_k}$ and $\mathbf{f}_k$ are the k-th columns of $\hat{\mathbf{W}}_P$ and $\mathbf{F}$, respectively, and x_{P_k} and z_{P_k} are the k-th element of $\mathbf{x}_P$ and $\mathbf{z}_P$, respectively.

2.3.3. Signal Model for the Secondary System

The SUs are served by the SBS, where the received signal at the SUs is:

$$\mathbf{y}_S = \sqrt{P_S}\mathbf{G}^T\hat{\mathbf{W}}_S\mathbf{x}_S + \sqrt{P_P}\mathbf{U}^T\hat{\mathbf{W}}_P\mathbf{x}_P + \sqrt{P_n}\mathbf{U}^T\mathbf{W}_n\mathbf{a}_n + \mathbf{z}_S, \tag{22}$$

where the first term represents the desired signal at the SUs. The second term captures the intra-cell interference from the concurrent primary transmissions. The third term accounts for the AN leakage into the SU's reception. Moreover, $\mathbf{z}_S$ models the AWGN vector at the SUs satisfying $\mathbb{E}\left[\mathbf{z}_S\mathbf{z}_S^H\right] = \mathbf{I}_M\sigma_S^2$. The received signal at the m-th SU can be written as:

$$y_{S_m} = \sqrt{P_S}\mathbf{g}_m^T\hat{\mathbf{w}}_{S_m}x_{S_m} + \sum_{j=1,j\neq m}^{M}\sqrt{P_S}\mathbf{g}_m^T\hat{\mathbf{w}}_{S_j}x_{S_j} + \sqrt{P_S}\mathbf{u}_m^T\hat{\mathbf{W}}_P\mathbf{x}_P + \sqrt{P_n}\mathbf{u}_m^T\mathbf{W}_n\mathbf{a}_n + z_{S_m}, \tag{23}$$

where $\hat{\mathbf{w}}_{S_m}$ and $\mathbf{g}_m$ are the m-th columns of $\hat{\mathbf{W}}_S$ and $\mathbf{G}$, respectively, and x_{S_m} and z_{S_m} are the m-th element of $\mathbf{x}_S$ and $\mathbf{z}_S$, respectively.

2.3.4. Signal Model for the Eavesdropper

The eavesdropper is interested in eavesdropping upon the confidential data transmitted to either PUs or SUs. For the sake of completeness, two cases, in which the eavesdropper intercepts (1) the k-th PU's signal and (2) the m-th SU's signal, are investigated. To this end, a generic expression for the received signal at the eavesdropper can be written as:

$$\mathbf{y}_E = \sqrt{P_P}\mathbf{H}_P^T\hat{\mathbf{W}}_P\mathbf{x}_P + \sqrt{P_n}\mathbf{H}_P^T\mathbf{W}_n\mathbf{a}_n + \sqrt{P_S}\mathbf{H}_S^T\hat{\mathbf{W}}_S\mathbf{x}_S + \mathbf{z}_E \tag{24}$$

where $\mathbf{z}_E$ is the AWGN vector at the eavesdropper satisfying $\mathbb{E}\left[\mathbf{z}_E\mathbf{z}_E^H\right] = \mathbf{I}_{N_E}\sigma_E^2$. In (24), the first term corresponds to the signal transmitted by the PBS, the second term accounts for the AN leakage, and the third term captures the signal transmitted by the SBS. Then, the k-th PU signal intercepted at the eavesdropper can be re-written as:

$$y_{E_k} = \sqrt{P_P}\mathbf{h}_P^T\hat{\mathbf{w}}_{P_k}x_{P_k} + \sum_{j=1,j\neq k}^{K}\sqrt{P_P}\mathbf{h}_P^T\hat{\mathbf{w}}_{P_j}x_{P_j} + \sqrt{P_n}\mathbf{h}_P^T\mathbf{W}_n\mathbf{a}_n + \sqrt{P_S}\mathbf{h}_S^T\hat{\mathbf{W}}_S\mathbf{x}_S + z_{E_k}. \tag{25}$$

Whereas, the m-th SU signal intercepted at the eavesdropper can be re-written as:

$$y_{E_m} = \sqrt{P_S}\mathbf{h}_S^T\hat{\mathbf{w}}_{S_m}x_{S_m} + \sum_{j=1,j\neq m}^{M}\sqrt{P_S}\mathbf{h}_S^T\hat{\mathbf{w}}_{S_j}x_{S_j} + \sqrt{P_n}\mathbf{h}_P^T\mathbf{W}_n\mathbf{a}_n + \sqrt{P_P}\mathbf{h}_P^T\hat{\mathbf{W}}_P\mathbf{x}_P + z_{E_m}. \tag{26}$$

2.4. Achievable Rate Analysis

In this subsection, the achievable rate expressions at the PUs and SUs are derived by using the worst-case Gaussian noise approximation technique. This technique is widely used in sum rate analysis in wireless systems [17,18], and basically represents a lower bound of what can be achieved in practice. Accordingly, by using (21), the received signal at the k-th PU can be re-written as:

$$y_{P_k} = \sqrt{P_P}\mathbf{f}_k^T\hat{\mathbf{w}}_{P_k}x_{P_k} + \tilde{n}_{P_k}, \tag{27}$$

where the first term accounts for the desired signal and $\tilde{n}_{P_k}$ represents the effective noise, which is given by:

$$\begin{aligned}\tilde{n}_{P_k} = {} & \sqrt{P_P}\left(\mathbf{f}_k^T\hat{\mathbf{w}}_{P_k} - \mathbb{E}\left[\mathbf{f}_k^T\hat{\mathbf{w}}_{P_k}\right]\right)x_{P_k} + \sum_{j=1,j\neq k}^{K}\sqrt{P_P}\mathbf{f}_k^T\hat{\mathbf{w}}_{P_j}x_{P_j} + \sqrt{P_S}\mathbf{v}_k^T\hat{\mathbf{W}}_S\mathbf{x}_S \\ & + \sqrt{P_n}\mathbf{f}_k^T\mathbf{W}_n\mathbf{a}_n + z_{P_k}.\end{aligned} \tag{28}$$

In (27), the desired signal and the effective noise are uncorrelated. The worst-case uncorrelated additive noise is independent Gaussian noise having the same variance, hence, the achievable rate at the k-th PU can be derived as:

$$\mathcal{R}_{P_k} = \log_2\left(1 + \frac{\left|\mathbb{E}\left[\sqrt{P_P}\mathbf{f}_k^T\hat{\mathbf{w}}_{P_k}\right]\right|^2}{P_P\mathbb{V}\mathrm{ar}(\mathbf{f}_k^T\hat{\mathbf{w}}_{P_k}) + I_{P_k} + I_{S_k} + AN_k + \sigma_P^2}\right), \tag{29}$$

where I_{P_k}, I_{S_k}, and AN_k account for the primary inter-user interference, intra-cell interference due to concurrent secondary transmissions, and the AN leakage towards the k-th PU, respectively, and they are defined as:

$$I_{P_k} = \sum_{j=1,j\neq k}^{K} P_P \mathbb{E}\left[\left|\mathbf{f}_k^T \hat{\mathbf{w}}_{P_j}\right|^2\right], \tag{30a}$$

$$I_{S_k} = P_S \mathbb{E}\left[\left\|\mathbf{v}_k^T \hat{\mathbf{W}}_S\right\|^2\right], \tag{30b}$$

$$AN_k = P_n \mathbb{E}\left[\left\|\mathbf{f}_k^T \mathbf{W}_n\right\|^2\right]. \tag{30c}$$

Similarly, by using (23), the received signal at the m-th SU can be re-written as:

$$y_{S_m} = \sqrt{P_S}\mathbf{g}_m^T \hat{\mathbf{w}}_{S_m} x_{S_m} + \tilde{n}_{S_m}, \tag{31}$$

where the first term represents the desired signal and $\tilde{n}_{S_m}$ is the effective noise, and is given by:

$$\tilde{n}_{S_m} = \sqrt{P_S}\left(\mathbf{g}_m^T \hat{\mathbf{w}}_{S_m} - \mathbb{E}\left[\mathbf{g}_m^T \hat{\mathbf{w}}_{S_m}\right]\right) x_{S_m} + \sum_{j=1,j\neq m}^{M} \sqrt{P_S}\mathbf{g}_m^T \hat{\mathbf{w}}_{S_j} x_{S_j} + \sqrt{P_S}\mathbf{u}_m^T \hat{\mathbf{W}}_P \mathbf{x}_P$$
$$+ \sqrt{P_n}\mathbf{u}_m^T \mathbf{W}_n \mathbf{a}_n + z_{S_m}. \tag{32}$$

Hence, the achievable rate at the m-th SU can be derived as:

$$\mathcal{R}_{S_m} = \log_2\left(1 + \frac{\left|\mathbb{E}\left[\sqrt{P_S}\mathbf{g}_m^T \hat{\mathbf{w}}_{S_m}\right]\right|^2}{P_S \mathbb{V}\text{ar}(\mathbf{g}_m^T \hat{\mathbf{w}}_{S_m}) + I_{S_m} + I_{P_m} + AN_m + \sigma_S^2}\right), \tag{33}$$

where I_{S_m}, I_{P_m}, and AN_m represent the secondary inter-user interference, the CCI from SBS transmissions, and the AN leakage towards the m-th SU, respectively, and they are defined as:

$$I_{S_m} = \sum_{j=1,j\neq m}^{M} P_S \mathbb{E}\left[\left|\mathbf{g}_m^T \hat{\mathbf{w}}_{S_j}\right|^2\right], \tag{34a}$$

$$I_{P_m} = P_P \mathbb{E}\left[\left\|\mathbf{u}_m^T \hat{\mathbf{W}}_P\right\|^2\right], \tag{34b}$$

$$AN_m = P_n \mathbb{E}\left[\left\|\mathbf{u}_m^T \mathbf{W}_n\right\|^2\right]. \tag{34c}$$

3. Secrecy Rate Analysis

An achievable secrecy rate of the k-th PU is given by the difference between channel capacities of the PBS to PU channel and the PBS to eavesdropper channel. Thus, the achievable secrecy rate at the k-th PU is:

$$\mathcal{R}_{P_k}^{\text{sec}} = \left[\mathcal{R}_{P_k} - \mathcal{R}_k^{\text{eve}}\right]^+, \tag{35}$$

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

A lower bound for the achievable rate at the k-th PU can be derived from (29) as (see Appendix A.2 for the derivation):

$$\mathcal{R}_{P_k} \approx \left(\tfrac{T-\tau}{T}\right) \log_2 \Bigg(1+ \frac{P_P(N_P-K)\sum_{j=1}^{K}\sigma^2_{\hat{F}_j}}{P_P\left(\zeta_{F_k}-\sigma^2_{\hat{F}_k}\right)+P_S(N_S-M)\left(\sum\limits_{j=1}^{M}\sigma^2_{\hat{G}_j}\left(\zeta^{-1}_{Gm}(\zeta_{V_k}+\frac{1}{\tau P_U})\right)^2+\frac{1}{N_S}\left(\frac{2\zeta_{Gm}/\tau P_U}{\zeta_{Gm}+\zeta_{V_k}+1/\tau P_U}-\frac{1}{\tau P_U}+\zeta_{Gm}-\sigma^2_{\hat{G}m}\right)\right)+P_n\frac{K\zeta_{F_k}}{N_P-K}+\sigma^2_P} \Bigg). \tag{36}$$

The eavesdropper's rate, on the other hand, cannot be lower bounded, since in that case the obtained secrecy rate is no longer a lower bound. Thus, the ergodic rate of the k-th PU signal leaked into the eavesdropper is computed as $\mathcal{R}^{\text{eve}}_k = \mathbb{E}\left[\log_2(1+\gamma_{E_k})\right]$, where γ_{E_k} is a closed-form expression for the SINR of the k-th PU signal intercepted at the eavesdropper, which is derived from (24) as (by assuming eavesdropper is able to mitigate inter-pair interference [13]):

$$\gamma_{E_k} = \frac{\left|\sqrt{P_P}\mathbf{h}^T_{P_k}\hat{\mathbf{w}}_{P_k}\right|^2}{P_S\left[\mathbf{H}^T_S\hat{\mathbf{W}}_S\hat{\mathbf{W}}^H_S\mathbf{H}^*_S\right]_{k,k}+P_n\left[\mathbf{H}^T_P\mathbf{W}_n\mathbf{W}^H_n\mathbf{H}^*_P\right]_{k,k}+\sigma^2_E}. \tag{37}$$

Similarly, the achievable secrecy rate of the m-th SU is:

$$\mathcal{R}^{\text{sec}}_{S_m} = \left[\mathcal{R}_{S_m}-\mathcal{R}^{\text{eve}}_m\right]^+, \tag{38}$$

where $\mathcal{R}_{S_m}$ is an achievable rate of the m-th SU and its lower bound is derived by following steps similar to those used for deriving (36) as:

$$\mathcal{R}_{S_m} \approx \left(\tfrac{T-\tau}{T}\right) \log_2 \Bigg(1+ \frac{P_S(N_S-M)\sum_{j=1}^{M}\sigma^2_{\hat{G}_j}}{P_S\left(\zeta_{Gm}-\sigma^2_{\hat{G}m}\right)+P_P(N_P-K)\left(\sum\limits_{j=1}^{K}\sigma^2_{\hat{F}_j}\left(\zeta^{-1}_{F_k}(\zeta_{Um}+\frac{1}{\tau P_U})\right)^2+\frac{1}{N_P}\left(\frac{2\zeta_{F_k}/\tau P_U}{\zeta_{F_k}+\zeta_{Um}+1/\tau P_U}-\frac{1}{\tau P_U}+\zeta_{F_k}-\sigma^2_{\hat{F}_k}\right)\right)+P_n\frac{K\zeta_{Um}}{N_P-K}+\sigma^2_S} \Bigg). \tag{39}$$

Furthermore, $\mathcal{R}^{\text{eve}}_m$ is the information leakage rate to the eavesdropper for decoding the m-th SU's confidential information, and can be computed as: $\mathcal{R}^{\text{eve}}_m = \mathbb{E}\left[\log_2(1+\gamma_{E_m})\right]$, where γ_{E_m} is the SINR expression of the m-th SU signal intercepted at the eavesdropper, which is derived from (24) as:

$$\gamma_{E_m} = \frac{\left|\sqrt{P_S}\mathbf{h}^T_{S_m}\hat{\mathbf{w}}_{S_m}\right|^2}{P_P\left[\mathbf{H}^T_P\hat{\mathbf{W}}_P\hat{\mathbf{W}}^H_P\mathbf{H}^*_P\right]_{m,m}+P_n\left[\mathbf{H}^T_P\mathbf{W}_n\mathbf{W}^H_n\mathbf{H}^*_P\right]_{m,m}+\sigma^2_E}. \tag{40}$$

4. Asymptotic Secrecy Rate Analysis

In this section, the asymptotic secrecy rates are derived whenever the numbers of antennas at the PBS and SBS grow without limit while keeping a fixed ratio $\beta = N_P/N_S$. In this context, the pilot transmit power is assumed to be fixed, whereas the transmit powers at the PBS and SBS are scaled as follows: $P_P = E_P/N_P$, $P_n = E_n/N_P$, and $P_S = E_S/N_S$, where E_P, E_n, and E_S are constants [3]. Hence, by letting $N_P, N_S \to \infty$ in (35), the corresponding achievable secrecy rate for the case in which the eavesdropper intends to intercept the confidential signal transmitted to the k-th PU can be derived as (see Appendix A.3 for the derivation):

$$\mathcal{R}^{\text{sec}}_{P_k,\infty} = \left(\frac{T-\tau}{T}\right)\log_2\left(1+\frac{E_P\sum_{j=1}^{K}\sigma^2_{\hat{F}_j}}{E_{S_{max}}\sum_{j=1}^{M}\sigma^2_{\hat{G}_j}\left(\zeta^{-1}_{Gm}(\zeta_{V_k}+\frac{1}{\tau P_U})\right)^2+\sigma^2_P}\right). \tag{41}$$

The corresponding achievable secrecy rate for the case in which the eavesdropper is intercepting the confidential signal transmitted to the m-th SU can be derived, by letting $N_P, N_S \to \infty$ in (38), as (see Appendix A.3 for the derivation):

$$\mathcal{R}^{\text{sec}}_{S_m,\infty} = \left(\frac{T-\tau}{T}\right)\log_2\left(1+\frac{E_{S_{\max}}\sum\limits_{m=1}^{M}\sigma^2_{\hat{G}_m}}{E_P\sum_{j=1}^{K}\sigma^2_{\hat{F}_j}\left(\zeta^{-1}_{F_k}(\zeta_{U_m}+\frac{1}{\tau P_U})\right)^2+\sigma^2_S}\right). \tag{42}$$

Remark 2. *The achievable asymptotic secrecy rate expressions in (41) and (42) are independent of the BS-to-eavesdropper channels. Consequently, the corresponding information leakage rate at the eavesdropper vanishes in the limit of infinitely many BS antennas.*

In particular, the transmit powers of the payload data at both BSs and the transmit power of AN sequence at the PBS can be scaled inversely proportional to the number of BS antennas without incurring any performance penalty. Moreover, the asymptotic secrecy rates are independent of the fast fading components of the corresponding wireless channels.

5. Performance Analysis for Perfect CSI

For further investigations, the performance analysis of the considered system is provided in this section for the idealistic scenario of having perfect CSI, i.e., $\hat{\mathbf{F}} = \mathbf{F}$ and $\hat{\mathbf{G}} = \mathbf{G}$. Hence, the amounts of performance degradation due to inaccurate channel knowledge and pilot contamination are quantified and compared. To this end, the ZF detectors at the PBS and SBS can be constructed by assuming the availability of the genie-aided perfect CSI as follows:

$$\mathbf{W}_P = \frac{\mathbf{F}^*\left(\mathbf{F}^T\mathbf{F}^*\right)^{-1}}{\sqrt{\text{Tr}((\mathbf{F}^T\mathbf{F}^*)^{-1})}}, \tag{43}$$

$$\mathbf{W}_S = \frac{\mathbf{G}^*\left(\mathbf{G}^T\mathbf{G}^*\right)^{-1}}{\sqrt{\text{Tr}((\mathbf{G}^T\mathbf{G}^*)^{-1})}}. \tag{44}$$

5.1. Secondary Transmit Power Constraint for Perfect CSI Case

The secondary transmit power constraint for perfect CSI can be re-written as:

$$P_S = \min\left(P_{S_{\max}}, \frac{I_P\text{Tr}\left(\left(\frac{\mathbf{G}^T\mathbf{G}^*}{N_S}\right)^{-1}\right)}{N_S\text{Tr}\left(\left(\frac{\mathbf{V}^T\mathbf{G}^*}{N_S}\right)\left(\frac{\mathbf{G}^T\mathbf{G}^*}{N_S}\right)^{-1}\left(\frac{\mathbf{G}^T\mathbf{G}^*}{N_S}\right)^{-1}\left(\frac{\mathbf{G}^T\mathbf{V}^*}{N_S}\right)\right)}\right). \tag{45}$$

Next, the maximum transmit power at the SBS is scaled inversely proportional to the number of antennas as $P_{S_{\max}} = E_{S_{\max}}/N_S$. The secondary transmit power constraint can then be rewritten as:

$$P_S = \min\left(\frac{E_{S_{\max}}}{N_S}, \frac{\left(\frac{I_P}{N_S}\right)\text{Tr}\left(\left(\frac{\mathbf{G}\mathbf{G}^H}{N_S}\right)^{-1}\right)}{\text{Tr}\left(\left(\frac{\mathbf{V}\mathbf{G}^H}{N_S}\right)\left(\frac{\mathbf{G}\mathbf{G}^H}{N_S}\right)^{-1}\left(\frac{\mathbf{G}\mathbf{G}^H}{N_S}\right)^{-1}\left(\frac{\mathbf{G}\mathbf{V}^H}{N_S}\right)\right)}\right). \tag{46}$$

By first letting $N_S \to \infty$ in (46) and then using the identities (A15) and (A16) given in the appendix, an asymptotic expression for the transmit power constraint at the SBS can be derived as:

$$\lim_{N_S\to\infty} P_S N_S \to E_{S_{\max}}. \tag{47}$$

5.2. Achievable Rate Analysis for Perfect CSI Case

In this subsection, the achievable rate at the PUs, SUs, and eavesdropper are derived by replacing $\mathbf{W}_P^T$ and $\mathbf{W}_S^T$ with $\hat{\mathbf{W}}_P^T$ and $\hat{\mathbf{W}}_S^T$ in (20), (22), and (24), respectively. To this end, by using (20), the achievable rate at the k-th primary user node can be computed as $\mathcal{R}_{P_k} = \mathbb{E}\left[\log_2(1+\gamma_{P_k})\right]$, where γ_{P_k} is:

$$\gamma_{P_k} = \frac{P_P \Big/ \mathrm{Tr}\left((\mathbf{F}^T\mathbf{F}^*)^{-1}\right)}{P_n\left[\mathbf{F}^T\mathbf{W}_n\mathbf{W}_n^H\mathbf{F}^*\right]_{k,k} + P_S\left[\mathbf{V}^T\mathbf{W}_S\mathbf{W}_S^H\mathbf{V}^*\right]_{k,k} + \sigma_P^2}. \tag{48}$$

Similarly, by using (22), the achievable rate at the m-th secondary user node can be derived as $\mathcal{R}_{S_m} = \mathbb{E}\left[\log_2(1+\gamma_{S_m})\right]$, where γ_{S_m} is given by

$$\gamma_{S_m} = \frac{P_S \Big/ \mathrm{Tr}\left((\mathbf{G}^T\mathbf{G}^*)^{-1}\right)}{P_P\left[\mathbf{U}^T\mathbf{W}_P\mathbf{W}_P^H\mathbf{U}^*\right]_{m,m} + P_n\left[\mathbf{U}^T\mathbf{W}_n\mathbf{W}_n^H\mathbf{U}^*\right]_{m,m} + \sigma_S^2}. \tag{49}$$

Next, by using (24) and by assuming the eavesdropper is capable of fully mitigating the inter-substream interference, the information leakage rate to the eavesdropper for decoding the k-th PU's confidential information is computed as $\mathcal{R}_k^{\text{eve}} = \mathbb{E}\left[\log_2(1+\gamma_{E_k})\right]$, where γ_{E_k} is the SINR expression of the k-th PU signal intercepted at the eavesdropper, which is given by:

$$\gamma_{E_k} = \frac{P_P\left[\mathbf{H}_P^T\mathbf{W}_P\mathbf{W}_P^H\mathbf{H}_P^*\right]_{k,k}}{P_S\left[\mathbf{H}_S^T\mathbf{W}_S\mathbf{W}_S^H\mathbf{H}_S^*\right]_{k,k} + P_n\left[\mathbf{H}_P^T\mathbf{W}_n\mathbf{W}_n^H\mathbf{H}_P^*\right]_{k,k} + \sigma_E^2}. \tag{50}$$

Similarly, the rate of the m-th SU signal leaked into the eavesdropper is computed as $\mathcal{R}_m^{\text{eve}} = \mathbb{E}\left[\log_2(1+\gamma_{E_m})\right]$, where γ_{E_m} is a closed-form expression for the SINR of the m-th SU signal intercepted at the eavesdropper, which is derived from (24) as:

$$\gamma_{E_m} = \frac{P_S\left[\mathbf{H}_S^T\mathbf{W}_S\mathbf{W}_S^H\mathbf{H}_S^*\right]_{m,m}}{P_P\left[\mathbf{H}_P^T\mathbf{W}_P\mathbf{W}_P^H\mathbf{H}_P^*\right]_{m,m} + P_n\left[\mathbf{H}_P^T\mathbf{W}_n\mathbf{W}_n^H\mathbf{H}_P^*\right]_{m,m} + \sigma_E^2}. \tag{51}$$

5.3. Asymptotic Secrecy Rate Analysis for Perfect CSI Case

In this subsection, the asymptotic secrecy rate expressions are derived for both primary and secondary systems when the numbers of antennas at the PBS and SBS grow without limit, while keeping a fixed ratio $\beta = N_P = N_S$. In this context, the transmit powers at the PBS and SBS are scaled inversely proportional to the number of BS antennas as $P_P = E_P/N_P$, $P_n = E_n/N_P$, and $P_S = E_S/N_S$, where E_P, E_n, and E_S are constants. Whenever N_P and N_S grow without bound, the corresponding achievable secrecy rate for the case in which the eavesdropper intends to intercept the confidential signal transmitted to the k-th primary user is derived as (see Appendix B for the derivation):

$$\mathcal{R}_{P_k,\infty}^{\text{sec}} = \lim_{N_P,N_S\to\infty} \mathcal{R}_{P_k}^{\text{sec}} = \log\left(1 + \frac{E_P}{\sigma_P^2\mathrm{Tr}\left(\mathbf{D}_F^{-1}\right)}\right). \tag{52}$$

Similarly, the corresponding asymptotic secrecy rate for the case in which the eavesdropper intends to intercept the confidential signal transmitted to the m-th SU is given by:

$$\mathcal{R}_{S_m,\infty}^{\text{sec}} = \lim_{N_P,N_S\to\infty} \mathcal{R}_{S_m}^{\text{sec}} = \log\left(1 + \frac{E_{S_{\max}}}{\sigma_S^2\mathrm{Tr}\left(\mathbf{D}_G^{-1}\right)}\right). \tag{53}$$

Remark 3. *The achievable asymptotic secrecy rate expressions in (52) and (53) are independent of the BS-to-eavesdropper channels. Consequently, the corresponding rate at the eavesdropper vanishes in the limit of infinitely many BS antennas.*

6. Numerical Results

In Figure 2, the achievable secrecy sum rates at the PUs and SUs are plotted. Furthermore, the information leakage rates to the eavesdropper from the primary and secondary transmissions are plotted against N_P while keeping N_E fixed. The exact (simulation) curves are generated by using (29), (33), (37), and (40) through Monte-Carlo simulations. Moreover, the asymptotic secrecy rate is plotted by using (41) and (42). Figure 2 reveals that the corresponding information leakage rates to the eavesdropper asymptotically vanish when $N_P \to \infty$ and $N_S \to \infty$. Hence, the secrecy rate asymptotically approaches the achievable rate at the user nodes. Therefore, the intra-cell pilot contamination effects in cognitive massive MIMO systems do not hinder the use of random pseudo-inverse based AN shaping matrices.

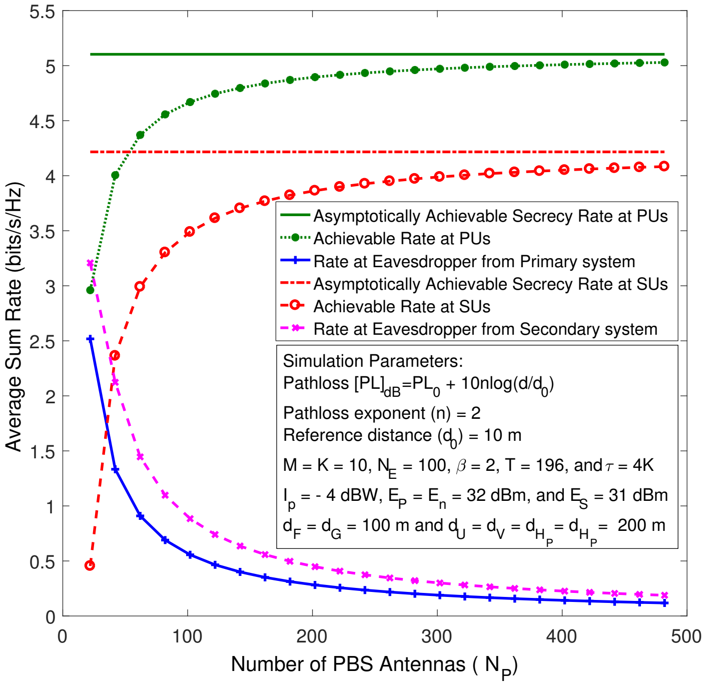

Figure 2. The achievable secrecy rates versus the number of PBS antennas for imperfect channel state information (CSI) case.

To investigate the impact of the primary interference temperatures on the secondary system transmissions for the imperfect and perfect CSI cases, the transmit power constraint of the SUs is plotted, in Figure 3, against the number of PBS antennas for two different primary interference temperatures. The asymptotic transmit power constraints are plotted by using the asymptotic analysis in (14) and (47), while the exact curves are plotted by using Monte-Carlo simulations. Figure 3 clearly reveals that the transmit power of the secondary system approaches its allowable peak value when the number of PBS antennas grows large. However, the rate of asymptotic convergence depends on the CSI assumption and the primary interference temperature. Specifically, the curves corresponding to imperfect CSI exhibit the lowest rate of asymptotic convergence compared to the perfect CSI case. Moreover, the asymptotic rate of convergence decreases whenever the primary interference temperature decreases.

In Figure 4, the transmit power constraint at the secondary system is plotted versus the number of PBS antennas by varying the number of user nodes for the cases of imperfect and perfect CSI. Figure 4 shows that the secondary system transmit power asymptotically approaches its peak level as the number of PBS antennas grows without bound, irrespective of the number of user nodes. Nevertheless, the rate of asymptotic convergence decreases when the numbers of user nodes increase. Therefore, the secondary system can asymptotically be operated at its peak transmit power, regardless of the number of user nodes and primary interference temperature, whenever the PBS is equipped with a very large antenna array.

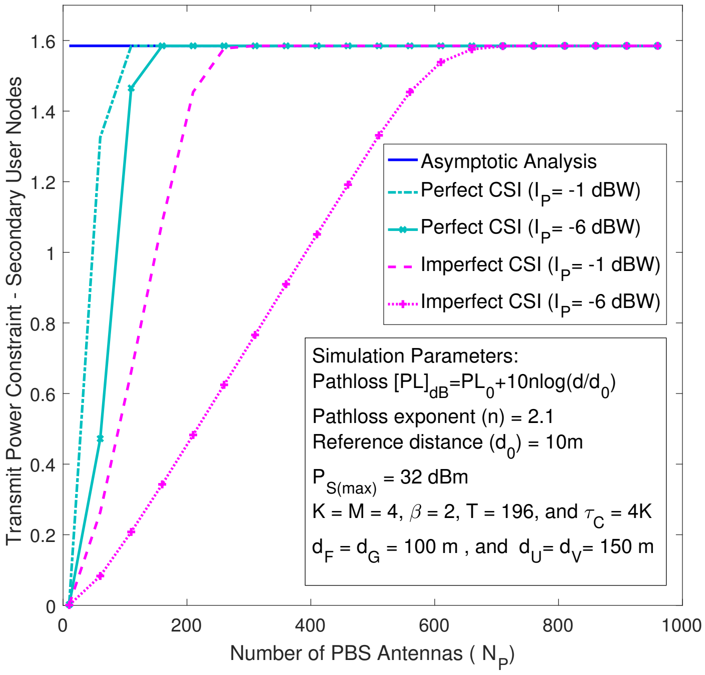

Figure 3. The transmit power constraint of the secondary system versus the number of PBS antennas by varying I_P.

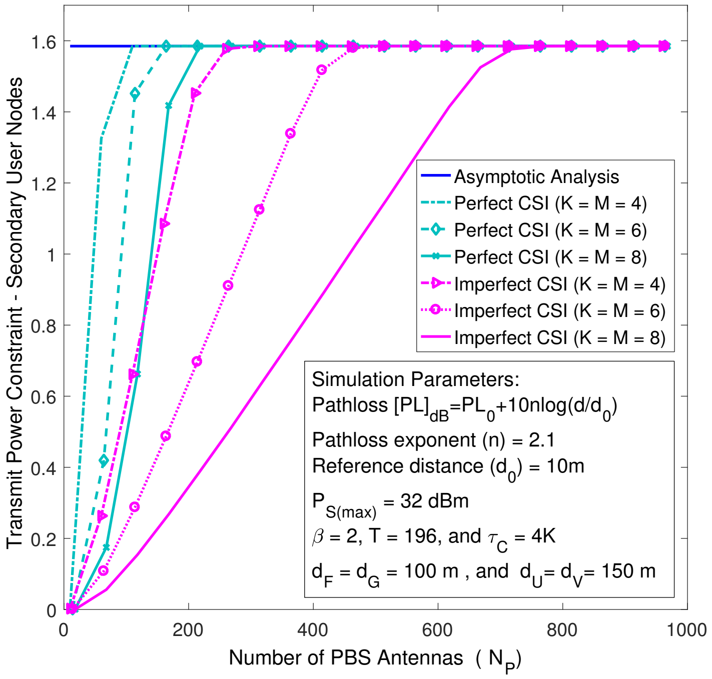

Figure 4. The transmit power constraint of the secondary system versus the number of PBS antennas by varying M.

Figure 5 depicts the achievable secrecy rate of the primary and secondary systems against the number of PBS antennas for the perfect CSI case. The asymptotic secrecy rate curves are plotted by using (52) and (53), whereas the exact sum rate curves are plotted by using Monte-Carlo simulations. As shown in Figure 5, for a fixed number of antennas at the eavesdropper ($N_E = 100$), the achievable secrecy rates at the primary and secondary systems go up gradually with the growing of N_P and N_S until they approach their corresponding asymptotic curves, which basically means the capability of the eavesdropper decreases and eventually vanishes whenever the number of antennas grows large.

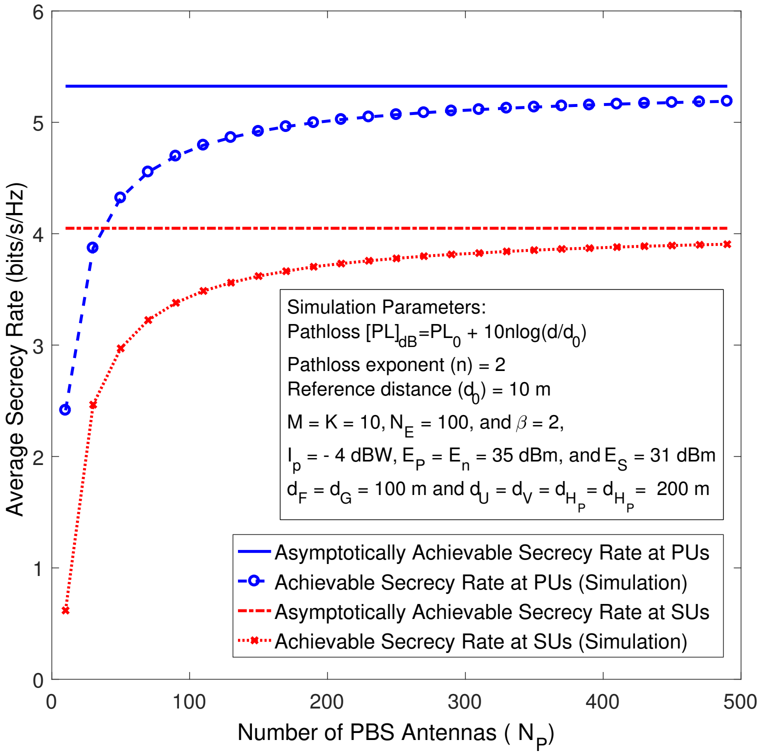

Figure 5. The achievable secrecy rates versus the number of PBS antennas for perfect CSI case.

7. Conclusions

In this paper, a secure communication model for cognitive multi-user massive MIMO networks with underlay spectrum sharing has been proposed and analyzed. The extra degrees-of-freedom provided by the massive MIMO have been exploited to transmit AN sequences to incapacitate the eavesdropper's ability to decode the confidential data. The asymptotic achievable secrecy rates of this system model have been derived in closed form for imperfect and perfect CSI cases. Thereby, the detrimental effects of AN leakage into the desired signals and performance degradation due to pilot contamination have been investigated. Random AN shaping matrices can be employed in this model, and avoid the complication of designing a null-space based precoder, without any asymptotic performance penalty. The transmit power allocated for the AN sequence can be scaled down inversely proportional to the number of PBS antennas, and hence, a significant energy efficiency gain can be attained. The secondary transmit power constraint becomes independent of the primary interference temperature, and consequently, the secondary system can be operated independent of the primary system in the limit of infinitely many BS antennas. The asymptotic information leakage into the eavesdropper vanishes whenever the numbers of PBS and SBS antennas grow without bound, and hence, the asymptotic secrecy rates become independent of the BS-to-eavesdropper channels. Therefore, our work brings some valuable designing insights on physical layer security analysis in cognitive massive MIMO networks, and proposes an elegant mechanism for strengthening the security of communications against the potential attacks in the cognitive radio networks.

Author Contributions: All authors contributed equally to this work.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Derivations for the Performance Metrics for Imperfect CSI Case

In this appendix, derivations for the secrecy performance metrics are outlined. The achievable rates at the primary and secondary systems, and the transmit power constraint are derived arbitrarily for many antennas at the PBS and SBS. The asymptotic secrecy rates corresponding to the primary and secondary systems are derived when the numbers of antennas at the BS grow large.

Appendix A.1. Transmit Power Constraint at the Secondary System

The transmit power constraint in (9) can be re-written as:

$$P_S = \min\left(P_{S_{\max}}, I_P/\Delta\right), \tag{A1}$$

where $\Delta = \mathbb{E}\left[\mathrm{Tr}\left(\mathbf{V}^T\hat{\mathbf{W}}_S\hat{\mathbf{W}}_S^H\mathbf{V}^*\right)\right]$. To begin with, $\hat{\mathbf{G}}$ and $\mathbf{V}^T$ are dependent; the channel $\mathbf{V}^T$, by using (6), can be re-written as:

$$\mathbf{V}^T = \tilde{\mathbf{D}}_G^{-1}\hat{\mathbf{G}}^T - \mathbf{G}^T - \frac{\mathbf{Z}_G^T}{\sqrt{\tau P_U}}, \tag{A2}$$

where,

$$\tilde{\mathbf{D}}_G = \mathbf{D}_G^T\left(\mathbf{D}_G^T + \mathbf{D}_V^T + \frac{\mathbf{I}_M}{\tau P_U}\right)^{-1}. \tag{A3}$$

Then, by using (A2), Δ can be derived as follows:

$$\begin{aligned}
\Delta &= \mathbb{E}\left[\mathrm{Tr}\left(\left(\tilde{\mathbf{D}}_G^{-1}\hat{\mathbf{G}}^T - \mathbf{G}^T - \frac{\mathbf{Z}_G^T}{\sqrt{\tau P_U}}\right)\hat{\mathbf{W}}_S\hat{\mathbf{W}}_S^H\left(\hat{\mathbf{G}}^*\tilde{\mathbf{D}}_G^{-1} - \mathbf{G}^* - \frac{\mathbf{Z}_G^*}{\sqrt{\tau P_U}}\right)\right)\right] \\
&= \mathrm{Tr}\left(\mathbb{E}\left[\left(\tilde{\mathbf{D}}_G^{-1}\hat{\mathbf{G}}^T\hat{\mathbf{W}}_S - \left(\hat{\mathbf{G}}^T + \boldsymbol{\mathcal{E}}_G^T\right)\hat{\mathbf{W}}_S - \frac{\mathbf{Z}_G^T}{\sqrt{\tau P_U}}\hat{\mathbf{W}}_S\right)\right.\right. \\
&\qquad \left.\left.\left(\hat{\mathbf{W}}_S^H\hat{\mathbf{G}}^*\tilde{\mathbf{D}}_G^{-1} - \hat{\mathbf{W}}_S^H\left(\hat{\mathbf{G}}^* + \boldsymbol{\mathcal{E}}_G^*\right) - \hat{\mathbf{W}}_S^H\frac{\mathbf{Z}_G^*}{\sqrt{\tau P_U}}\right)\right]\right) \\
&= \mathrm{Tr}\left(\mathbb{E}\left[\alpha_S^2\tilde{\mathbf{D}}_G^{-2} - 2\alpha_S^2\tilde{\mathbf{D}}_G^{-1} - \tilde{\mathbf{D}}_G^{-1}\hat{\mathbf{G}}^T\hat{\mathbf{W}}_S\hat{\mathbf{W}}_S^H\frac{\mathbf{Z}_G^*}{\sqrt{\tau P_U}} + \alpha_S^2\mathbf{I}_M\right.\right. \\
&\qquad + \boldsymbol{\mathcal{E}}_G^T\hat{\mathbf{W}}_S\hat{\mathbf{W}}_S^H\boldsymbol{\mathcal{E}}_G^* + \hat{\mathbf{G}}^T\hat{\mathbf{W}}_S\hat{\mathbf{W}}_S^H\frac{\mathbf{Z}_G^*}{\sqrt{\tau P_U}} - \frac{\mathbf{Z}_G^T}{\sqrt{\tau P_U}}\hat{\mathbf{W}}_S\mathbf{W}_S^H\hat{\mathbf{G}}^*\tilde{\mathbf{D}}_G^{-1} \\
&\qquad \left.\left. + \frac{\mathbf{Z}_G^T}{\sqrt{\tau P_U}}\hat{\mathbf{W}}_S\mathbf{W}_S^H\hat{\mathbf{G}}^*\tilde{\mathbf{D}}_G^{-1} + \frac{\mathbf{Z}_G^T}{\sqrt{\tau P_U}}\hat{\mathbf{W}}_S\hat{\mathbf{W}}_S^H\frac{\mathbf{Z}_G^*}{\sqrt{\tau P_U}}\right]\right).
\end{aligned} \tag{A4}$$

Here, from (10), $\hat{\mathbf{W}}_S\hat{\mathbf{W}}_S^H = \alpha_S^2\hat{\mathbf{G}}^*\left(\hat{\mathbf{G}}^T\hat{\mathbf{G}}^*\right)^{-1}\left(\hat{\mathbf{G}}^T\hat{\mathbf{G}}^*\right)^{-1}\hat{\mathbf{G}}^T$, since $N_S \gg M$, the law of large numbers can be used to do this approximation, $\hat{\mathbf{G}}^T\hat{\mathbf{G}}^* \approx N_S\hat{\mathbf{D}}_G$, and consequently, $\hat{\mathbf{W}}_S\hat{\mathbf{W}}_S^H \approx \frac{\alpha_S^2}{N_S^2}\hat{\mathbf{G}}^*\hat{\mathbf{D}}_G^{-2}\hat{\mathbf{G}}^T$. Moreover, the term $\mathbf{Z}_G^T\hat{\mathbf{G}}^*$, by using (6) can be simplified as $\tilde{\mathbf{D}}_G\mathbf{Z}_G^T\mathbf{Z}_G^*/\sqrt{\tau P_U}$. Thus,

$$\Delta \approx \alpha_S^2\mathrm{Tr}\left(\left(\tilde{\mathbf{D}}_G^{-1} - \mathbf{I}_M\right)^2\right) + \frac{N_S - M}{N_S}\left(\mathrm{Tr}\left(\mathbf{D}_G - \hat{\mathbf{D}}_G\right) + \frac{2}{\tau P_U}\mathrm{Tr}\left(\tilde{\mathbf{D}}_G\right) - \frac{1}{\tau P_U}\right). \tag{A5}$$

By substituting (A5) into (9), the transmit power constraint for finitely many SBS antennas can be derived as shown in (12).

Appendix A.2. $\mathcal{R}_{P_k}$ for Finite Antenna Numbers

The achievable rate at the k-th PU is derived when both BSs are equipped with finite antenna numbers. From (29) the desired power can be derived as $(\mathbf{F}^T\hat{\mathbf{W}}_P)$ by invoking (16) and (4) as follows:

$$\begin{aligned}\mathbf{F}^T\hat{\mathbf{W}}_P &= (\hat{\mathbf{F}}^T + \boldsymbol{\mathcal{E}}_F^T)\hat{\mathbf{W}}_P \\ &= \alpha_P \mathbf{I}_K + \boldsymbol{\mathcal{E}}_F^T\hat{\mathbf{W}}_P. \end{aligned} \tag{A6}$$

Then, the desired power for the k-th PU can be re-written as:

$$\mathbf{f}_k^T\hat{\mathbf{w}}_{P_k} = \alpha_P + \mathcal{E}_{F_k}^T\hat{\mathbf{w}}_{P_k} \tag{A7}$$

where $\mathcal{E}_{F_k}^T$ is the k-th column of $\boldsymbol{\mathcal{E}}_F^T$, since $\hat{\mathbf{w}}_{P_k}$ and $\mathcal{E}_{F_k}^T$ are uncorrelated, and $\mathcal{E}_{F_k}^T$ is a zero-mean random variable, $\mathbb{E}[\mathcal{E}_{F_k}^T\hat{\mathbf{w}}_{P_k}] = 0$. Thus,

$$\mathbb{E}\left[\mathbf{f}_k^T\hat{\mathbf{w}}_{P_k}\right] = \alpha_P. \tag{A8}$$

Next, the first term of the effective noise in (29), $\mathbb{V}\mathrm{ar}(\mathbf{f}_k^T\hat{\mathbf{w}}_{P_k})$, can be derived by using (A7) and (A8) as:

$$\begin{aligned}\mathbb{V}\mathrm{ar}(\mathbf{f}_k^T\hat{\mathbf{w}}_{P_k}) &= \mathbb{E}\left[\left|\mathcal{E}_{F_k}^T\hat{\mathbf{w}}_{P_k}\right|^2\right] \\ &= (\zeta_{F_k} - \sigma_{\hat{F}_k}^2)\mathbb{E}\left[\left\|\hat{\mathbf{w}}_{P_k}\right\|^2\right] \\ &= \alpha_P^2(\zeta_{F_k} - \sigma_{\hat{F}_k}^2)\mathbb{E}\left[\left[\left(\hat{\mathbf{F}}^*\hat{\mathbf{F}}^T\right)^{-1}\right]_{k,k}\right] \\ &= \frac{\alpha_P^2\left(\zeta_{F_k} - \sigma_{\hat{F}_k}^2\right)}{\sigma_{\hat{F}_k}^2 K}\mathbb{E}\left[\mathrm{Tr}(\mathbf{X}^{-1})\right] \\ &= \frac{\alpha_P^2\left(\zeta_{F_k} - \sigma_{\hat{F}_k}^2\right)}{\sigma_{\hat{F}_k}^2 (N_P - K)}. \end{aligned} \tag{A9}$$

where $\mathbf{X}$ is a $K \times K$ central Wishart matrix with N_P degrees of freedom and covariance matrix $\mathbf{I}_K$, where $\mathrm{Tr}(\mathbf{X}^{-1}) = K/(N_P - K)$ [19].

The derivations for the remaining terms of the effective noise in (30) are given in the following:

- Deriving I_{P_k}: From (A6), $\mathbf{f}_k^T\hat{\mathbf{w}}_{P_j} = \mathcal{E}_{F_k}^T\hat{\mathbf{w}}_{P_j}^T$ for $j \neq k$. Since $\mathcal{E}_{F_k}^T$ and $\hat{\mathbf{w}}_{P_j}$ are uncorrelated, then,

$$\begin{aligned}\mathbb{E}\left[\left|\mathbf{f}_k^T\hat{\mathbf{w}}_{P_j}\right|^2\right] &= \left(\zeta_{F_k} - \sigma_{\hat{F}_k}^2\right)\mathbb{E}\left[\left\|\hat{\mathbf{w}}_{P_j}\right\|^2\right] \\ &= \frac{\alpha_P^2\left(\zeta_{F_k} - \sigma_{\hat{F}_k}^2\right)}{\sigma_{\hat{F}_j}^2 (N_P - K)}. \end{aligned} \tag{A10}$$

  Hence,

$$I_{P_k} = P_P \sum_{j=1, j\neq k}^{K} \frac{\alpha_P^2\left(\zeta_{F_k} - \sigma_{\hat{F}_k}^2\right)}{\sigma_{\hat{F}_j}^2 (N_P - K)}. \tag{A11}$$

- Deriving I_{S_k}: From (30b), I_{S_k} can be re-written as:

$$P_S\mathbb{E}\left[\left\|\mathbf{v}_k^T\hat{\mathbf{W}}_S\right\|^2\right] = P_S\mathbb{E}\left[\mathbf{v}_k^T\hat{\mathbf{W}}_S\hat{\mathbf{W}}_S^H\mathbf{v}_k^*\right]. \tag{A12}$$

By following the same derivation steps that used to drive Z in (A5), I_{S_k} can be approximated as:

$$\begin{aligned} I_{S_k} \approx\ & P_S(N_S-M)\Bigg(\sum_{j=1}^{M}\sigma^2_{\hat{G}_j}\left(\zeta^{-1}_{G_m}(\zeta_{V_k}+1/\tau P_U)\right)^2 \\ & + \frac{1}{N_S}\left(\frac{2\zeta_{G_m}/\tau P_U}{\zeta_{G_m}+\zeta_{V_k}+1/\tau P_U} - \frac{1}{\tau P_U} + \zeta_{G_m} - \sigma^2_{\hat{G}_m}\right)\Bigg). \end{aligned} \tag{A13}$$

- Deriving AN_k: Similarly, AN_k can be derived as:

$$P_n\mathbb{E}\left[\left\|\mathbf{f}_k^T\mathbf{W}_n\right\|^2\right] = \frac{P_nK\zeta_{F_k}}{N_P-K}. \tag{A14}$$

Next, by substituting (A8), (A9), (A11), (A13), and (A14) into (29), a lower bound approximation for the achievable rate at the k-th PU can be derived as shown in (36).

Appendix A.3. Asymptotic Achievable Rate at the Eavesdropper

To evaluate the asymptotic achievable rate at the eavesdropper when the PBS and SBS are deploying massive antenna arrays, the following identities are recalled from [20].

For a random matrix $\mathbf{A} \in \mathbb{C}^{M\times N}$ having elements of zero mean and unit variance, as $N \to \infty$ the column vectors of $\mathbf{A}$ become orthogonal, and hence, the following identity holds:

$$\lim_{N\to\infty} \mathbf{A}\mathbf{A}^H/N = \mathbf{I}_M. \tag{A15}$$

Also, whenever a random matrix $\mathbf{B} \in \mathbb{C}^{M\times N}$ is independently distributed with $\mathbf{A}$, the following identity holds:

$$\lim_{N\to\infty} \mathbf{A}\mathbf{B}^H/N = \mathbf{0}. \tag{A16}$$

By first letting $P_P = E_P/N_P$ and $P_n = E_n/N_P$, and then by substituting (10), (16), and (18) into (37), the SINR of the k-th PU signal intercepted at the eavesdropper can be re-written as:

$$\gamma_{E_k} = \frac{\frac{E_P\alpha_P^2}{N_P}\left[\left(\frac{\mathbf{H}_P^T\hat{\mathbf{F}}^*}{N_P}\right)\left(\frac{\hat{\mathbf{F}}^T\hat{\mathbf{F}}^*}{N_P}\right)^{-2}\left(\frac{\hat{\mathbf{F}}^T\mathbf{H}_P^*}{N_P}\right)\right]_{k,k}}{\frac{E_S\alpha_S^2}{N_S}\left[\left(\frac{\mathbf{H}_S^T\hat{\mathbf{G}}^*}{N_S}\right)\left(\frac{\hat{\mathbf{G}}^T\hat{\mathbf{G}}^*}{N_S}\right)^{-2}\left(\frac{\hat{\mathbf{G}}^T\mathbf{H}_S^*}{N_S}\right)\right]_{k,k} + \frac{E_n\alpha_n^2}{N_P}\left[\left(\frac{\mathbf{H}_P^T\mathbf{R}_n^*}{N_P}\right)\left(\frac{\mathbf{R}_n^T\mathbf{R}_n^*}{N_P}\right)^{-2}\left(\frac{\mathbf{R}_n^T\mathbf{H}_P^*}{N_P}\right)\right]_{k,k} + \sigma_E^2}. \tag{A17}$$

Next, by letting $N_P \to \infty$ and $N_S \to \infty$ in (A17) and then by invoking (A15) and (A16), it can be shown that:

$$\lim_{N_P,N_S\to\infty} \gamma_{E_k} = 0. \tag{A18}$$

Similarly, by using (40), the SINR at the eavesdropper, who is interested in intercepting the signal of the m-th SU, can be re-written as:

$$\gamma_{E_m} = \frac{\frac{E_S\alpha_S^2}{N_S}\left[\left(\frac{\mathbf{H}_S^T\hat{\mathbf{G}}^*}{N_S}\right)\left(\frac{\hat{\mathbf{G}}^T\hat{\mathbf{G}}^*}{N_S}\right)^{-2}\left(\frac{\hat{\mathbf{G}}^T\mathbf{H}_S^*}{N_S}\right)\right]_{m,m}}{\frac{E_P\alpha_P^2}{N_P}\left[\left(\frac{\mathbf{H}_P^T\hat{\mathbf{F}}^*}{N_P}\right)\left(\frac{\hat{\mathbf{F}}^T\hat{\mathbf{F}}^*}{N_P}\right)^{-2}\left(\frac{\hat{\mathbf{F}}^T\mathbf{H}_P^*}{N_P}\right)\right]_{m,m} + \frac{E_n\alpha_n^2}{N_P}\left[\left(\frac{\mathbf{H}_P^T\mathbf{R}_n^*}{N_P}\right)\left(\frac{\mathbf{R}_n^T\mathbf{R}_n^*}{N_P}\right)^{-2}\left(\frac{\mathbf{R}_n^T\mathbf{H}_P^*}{N_P}\right)\right]_{m,m} + \sigma_E^2}. \tag{A19}$$

Then, by invoking (A15) and (A16), and when N_S and N_P go to infinity in (A19), it can be shown that:

$$\lim_{N_P,N_S\to\infty} \gamma_{E_m} = 0. \tag{A20}$$

Appendix B. Derivations the Asymptotic Performance Metrics for Perfect CSI

In this appendix, the derivations of the asymptotic rates of primary and secondary systems with perfect CSI are outlined. To begin with, by letting $P_P = E_P/N_P$, $P_n = E_n/N_P$, and $P_S = E_S/N_S$ and then by substituting (43), (44) and (18) into (48), the end-to-end SINR at the k-th PU can be re-written as:

$$\gamma_{P_k} = \frac{E_P \Big/ \mathrm{Tr}\left(\left(\frac{\mathbf{F}^T\mathbf{F}^*}{N_P}\right)^{-1}\right)}{\frac{E_n\sigma_n^2}{\mathrm{Tr}\left(\left(\frac{\mathbf{R}_n^T\mathbf{R}_n^*}{N_P}\right)^{-1}\right)}\left[\left(\frac{\mathbf{F}^T\mathbf{R}_n^*}{N_P}\right)\left(\frac{\mathbf{R}_n^T\mathbf{R}_n^*}{N_P}\right)^{-2}\left(\frac{\mathbf{R}_n^T\mathbf{F}^*}{N_P}\right)\right]_{k,k} + \frac{P_S N_S}{\mathrm{Tr}\left(\left(\frac{\mathbf{G}^T\mathbf{G}^*}{N_S}\right)^{-1}\right)}\left[\left(\frac{\mathbf{V}^T\mathbf{G}^*}{N_S}\right)\left(\frac{\mathbf{G}^T\mathbf{G}^*}{N_S}\right)^{-2}\left(\frac{\mathbf{G}^T\mathbf{V}^*}{N_S}\right)\right]_{k,k} + \sigma_P^2}. \tag{A21}$$

Next, by letting $N_S \to \infty$ and $N_P \to \infty$ in (A21) and then by using (47), (A15) and (A16), the asymptotic SINR for the k-th PU can be written as:

$$\gamma_{P_k}^{\infty} = \frac{E_P}{\sigma_P^2 \mathrm{Tr}\left(\mathbf{D}_F^{-1}\right)}. \tag{A22}$$

Moreover, by using steps similar to those used for deriving (A21), the end-to-end SINR at the m-th SU can be re-written as:

$$\gamma_{S_m} = \frac{P_S N_S \Big/ \mathrm{Tr}\left(\left(\frac{\mathbf{G}^T\mathbf{G}^*}{N_S}\right)^{-1}\right)}{\frac{E_n\sigma_n^2}{\mathrm{Tr}\left(\left(\frac{\mathbf{R}_n^T\mathbf{R}_n^*}{N_P}\right)^{-1}\right)}\left[\left(\frac{\mathbf{U}^T\mathbf{R}_n^*}{N_P}\right)\left(\frac{\mathbf{R}_n^T\mathbf{R}_n^*}{N_P}\right)^{-2}\left(\frac{\mathbf{R}_n^T\mathbf{U}^*}{N_P}\right)\right]_{m,m} + \frac{E_P}{\mathrm{Tr}\left(\left(\frac{\mathbf{F}^T\mathbf{F}^*}{N_P}\right)^{-1}\right)}\left[\left(\frac{\mathbf{U}^T\mathbf{F}^*}{N_P}\right)\left(\frac{\mathbf{F}^T\mathbf{F}^*}{N_P}\right)^{-2}\left(\frac{\mathbf{F}^T\mathbf{U}^*}{N_P}\right)\right]_{m,m} + \sigma_S^2}. \tag{A23}$$

Again, by letting $N_S \to \infty$ and $N_P \to \infty$ in (A23) and then by using (47), (A15) and (A16), the asymptotic SINR for the m-th SU can be written as:

$$\gamma_{S_m}^{\infty} = \frac{E_{S_{\max}}}{\sigma_S^2 \mathrm{Tr}\left(\mathbf{D}_G^{-1}\right)}. \tag{A24}$$

Furthermore, the end-to-end SINR at the eavesdropper, who is interested in intercepting the signal of the k-th PU, can be obtained by substituting (44), (43) and (18) into (37) as follows:

$$\gamma_{E_k} = \frac{E_P\left[\left(\frac{\mathbf{H}_P^T\mathbf{F}^*}{N_P}\right)\left(\frac{\mathbf{F}^T\mathbf{F}^*}{N_P}\right)^{-2}\left(\frac{\mathbf{F}^T\mathbf{H}_P^*}{N_P}\right)\right]_{k,k} \Big/ \mathrm{Tr}\left(\left(\frac{\mathbf{F}^T\mathbf{F}^*}{N_P}\right)^{-1}\right)}{\frac{P_S N_S}{\mathrm{Tr}\left(\left(\frac{\mathbf{G}\mathbf{G}^H}{N_S}\right)^{-1}\right)}\left[\left(\frac{\mathbf{H}_S\mathbf{G}^H}{N_S}\right)\left(\frac{\mathbf{F}\mathbf{G}^H}{N_S}\right)^{-2}\left(\frac{\mathbf{G}\mathbf{H}_S^H}{N_S}\right)\right]_{k,k} + \frac{E_n\sigma_n^2}{\mathrm{Tr}\left(\left(\frac{\mathbf{R}_n^T\mathbf{R}_n^*}{N_P}\right)^{-1}\right)}\left[\left(\frac{\mathbf{H}_P^T\mathbf{R}_n^*}{N_P}\right)\left(\frac{\mathbf{R}_n^T\mathbf{R}_n^*}{N_P}\right)^{-2}\left(\frac{\mathbf{R}_n^T\mathbf{H}_P^*}{N_P}\right)\right]_{k,k} + \sigma_E^2}. \tag{A25}$$

Next, by letting $N_S \to \infty$ and $N_P \to \infty$ in (A25) and then by using (47), (A15) and (A16), the asymptotic SINR at the eavesdropper, who is interested in intercepting the signal of the k-th PU, can be derived as:

$$\lim_{N_P,N_S\to\infty} \gamma_{E_k} = \gamma_{E_k}^{\infty} \to 0. \tag{A26}$$

Similarly, by substituting (44), (43) and (18) into (40), the end-to-end SINR at the eavesdropper, who is interested in intercepting the signal of the m-th SU, can be re-written as:

$$\gamma_{E_m} = \frac{P_S N_S \left[\left(\frac{\mathbf{H}_S^T \mathbf{G}^*}{N_S} \right) \left(\frac{\mathbf{G}^T \mathbf{G}^*}{N_S} \right)^{-2} \left(\frac{\mathbf{G}^T \mathbf{H}_S^*}{N_S} \right) \right]_{m,m} \Big/ \mathrm{Tr}\left(\left(\frac{\mathbf{G}^T \mathbf{G}^*}{N_S} \right)^{-1} \right)}{\frac{E_P}{\mathrm{Tr}\left(\left(\frac{\mathbf{F}^T\mathbf{F}^*}{N_P}\right)^{-1}\right)} \left[\left(\frac{\mathbf{H}_P^T \mathbf{F}^*}{N_P} \right) \left(\frac{\mathbf{F}^T \mathbf{F}^*}{N_P} \right)^{-2} \left(\frac{\mathbf{F}^T \mathbf{H}_P^*}{N_P} \right) \right]_{m,m} + \frac{E_n \sigma_n^2}{\mathrm{Tr}\left(\left(\frac{\mathbf{R}_n^T\mathbf{R}_n^H}{N_P}\right)^{-1}\right)} \left[\left(\frac{\mathbf{H}_P^T \mathbf{R}_n^*}{N_P} \right) \left(\frac{\mathbf{R}_n^T \mathbf{R}_n^*}{N_P} \right)^{-2} \left(\frac{\mathbf{R}_n^T \mathbf{H}_P^*}{N_P} \right) \right]_{m,m} + \sigma_E^2}. \quad \text{(A27)}$$

Again, by letting $N_S \to \infty$ and $N_P \to \infty$ in (A27) and then by using (47), (A15) and (A16), the asymptotic SINR at the eavesdropper, who is interested in intercepting the signal of the m-th SU, can be derived as:

$$\lim_{N_P, N_S \to \infty} \gamma_{E_m} = \gamma_{E_m}^{\infty} \to 0. \quad \text{(A28)}$$

Next, by using (35), an achievable asymptotic secrecy rate at the k-th PU can be written as:

$$\mathcal{R}_{P_k,\infty}^{\text{sec}} = \left[\log\left(1 + \gamma_{P_k}^{\infty}\right) - \log\left(1 + \gamma_{E_k}^{\infty}\right) \right]^+. \quad \text{(A29)}$$

By substituting (A22) and (A26) into (A29), the desired asymptotic secrecy rate can be derived as given in (52).

Similarly, by using (35), the asymptotic secrecy rate at the m-th SU can be written as:

$$\mathcal{R}_{S_m,\infty}^{\text{sec}} = \left[\log\left(1 + \gamma_{S_m}^{\infty}\right) - \log\left(1 + \gamma_{E_m}^{\infty}\right) \right]^+. \quad \text{(A30)}$$

By substituting (A24) and (A28) into (A30), the desired asymptotic secrecy rate can be derived as given in (53).

References

1. Boccardi, F.; Heath, R.; Lozano, A.; Marzetta, T.; Popovski, P. Five disruptive technology directions for 5G. *IEEE Commun. Mag.* **2014**, *52*, 74–80.
2. Marzetta, T.L. Noncooperative Cellular Wireless with Unlimited Numbers of Base Station Antennas. *IEEE Trans. Wirel. Commun.* **2010**, *9*, 3590–3600.
3. Ngo, H.Q.; Larsson, E.G.; Marzetta, T.L. Energy and Spectral Efficiency of Very Large Multiuser MIMO Systems. *IEEE Trans. Commun.* **2013**, *61*, 1436–1449.
4. Yang, N.; Wang, L.; Geraci, G.; Elkashlan, M.; Yuan, J.; di Renzo, M. Safeguarding 5G wireless communication networks using physical layer security. *IEEE Commun. Mag.* **2015**, *53*, 20–27.
5. Liang, Y.; Poor, H.V.; Shamai, S. Information Theoretic Security. *Found. Trends Commun. Inf. Theor.* **2009**, *5*, 355–580.
6. Bloch, M.; Barros, J. *Physical-Layer Security: From Information Theory to Security Engineering*; Cambridge University Press: Cambridge, UK, 2001.
7. Kapetanovic, D.; Zheng, G.; Russek, F. Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks. *IEEE Commun. Mag.* **2015**, *53*, 21–27.
8. Schaefer, R.F.; Boche, H.; Khisti, A.; Poor, H.V. *Information Theoretic Security and Privacy of Information Systems*; Cambridge University Press: Cambridge, UK, 2017.
9. Poor, H.V.; Schaefer, R.F. Wireless physical layer security. *Proc. Natl. Acad. Sci. USA* **2016**, *114*, 19–26.
10. Goldsmith, A.; Jafar, S.A.; Maric, I.; Srinivasa, S. Breaking Spectrum Gridlock with Cognitive Radios: An Information Theoretic Perspective. *Proc. IEEE* **2009**, *97*, 894–914.
11. Liang, Y.; Somekh-Baruch, A.; Poor, H.V.; Shamai, S.; Verdú, S. Capacity of cognitive interference channels with and without secrecy. *IEEE Trans. Inf. Theor.* **2009**, *55*, 604–619.
12. Gabry, F.; Zappone, A.; Thobaben, R.; Jorswieck, E.A.; Skoglund, M. Energy Efficiency Analysis of Cooperative Jamming in Cognitive Radio Networks with Secrecy Constraints. *IEEE Wirel. Commun. Lett.* **2015**, *4*, 437–440.

13. Zhu, J.; Schober, R.; Bhargava, V. Secure Transmission in Multicell Massive MIMO Systems. *IEEE Trans. Wirel. Commun.* **2014**, *13*, 4766–4781.
14. Zhu, J.; Schober, R.; Bhargava, V.K. Linear Precoding of Data and Artificial Noise in Secure Massive MIMO Systems. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 2245–2261.
15. Guo, K.; Guo, Y.; Ascheid, G. Security-Constrained Power Allocation in MU-Massive-MIMO with Distributed Antennas. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 8139–8153.
16. Wang, L.; Wong, K.K.; Elkashlan, M.; Nallanathan, A.; Lambotharan, S. Secrecy and Energy Efficiency in Massive MIMO Aided Heterogeneous C-RAN: A New Look at Interference. *IEEE J. Sel. Top. Signal Process.* **2016**, *10*, 1375–1389.
17. Yang, H.; Marzetta, T.L. Performance of Conjugate and Zero-Forcing Beamforming in Large-Scale Antenna Systems. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 172–179.
18. Hassibi, B.; Hochwald, B.M. How much training is needed in multiple-antenna wireless links? *IEEE Trans. Inf. Theor.* **2003**, *49*, 951–963.
19. Tulino, A.M.; Verdú, S. Random matrix theory and wireless communications. *Found. Trends Commun. Inf. Theor.* **2004**, *1*, 1–128.
20. Cramer, H. *Random Variables and Probability Distributions*; Cambridge University Press: Cambridge, UK, 1970.