PAS OUF

4.11.2020

Contents lists available at ScienceDirect

Physical Communication

journal homepage: www.elsevier.com/locate/phycom

Full length article

NOMA and massive MIMO assisted physical layer security using artificial noise precoding

Pooja Singh [*], Aditya Trivedi

Department of Information and Communication Technology, ABV - Indian Institute of Information Technology and Management, Gwalior, India

ARTICLE INFO

Article history:
Received 26 May 2019
Received in revised form 11 November 2019
Accepted 16 December 2019
Available online 24 December 2019

Keywords:
PLS
Massive multiple-input-multiple-output (massive MIMO)
Artificial noise precoding
Non-orthogonal multiple access (NOMA)
Maximal Ratio Transmission (MRT)

ABSTRACT

In this paper, combined secrecy performance of two 5G technologies viz. massive multiple-input-multiple-output (massive MIMO) and non-orthogonal multiple access (NOMA) for a wireless communication network is investigated. Both, large scale path loss and small scale Rayleigh fading channel are taken into account. An amplify-and-forward (AF) relay is considered in the presence of an eavesdropper, both having multiple antennas. The achievable secrecy rate is obtained for the given system model using the suitable linear precoding method, the artificial noise precoding, and the secrecy performance is compared with the existing systems. Results show that the proposed approach outperforms existing systems for a particular range of signal-to-noise ratio (SNR). To improve the performance for all SNR values, artificial noise (AN) precoding is used. The frequently used linear precoding methods are also compared to get the suitable technique. Simulations are carried out for the verification of results.

1. Introduction

The emerging and developing nature of 5G wireless communication networks in every field of life creates a critical concern about its security. Maintaining the confidentiality, integrity, privacy, and secrecy of information and data are pivotal issues nowadays. 5G technologies like non-orthogonal multiple access (NOMA), massive multiple-input-multiple-output (massive MIMO), millimetre wave, etc. may be utilized to counter the security challenges against eavesdropper who always try to intercept the data. Presently, cryptographic methods are used to secure the communication. However, these methods are likely to fail when the eavesdroppers have quantum computers as it faces the hard mathematical problem [1]. Physical layer security (PLS) is a method to secure the 5G wireless communication networks. Its first concept is given by A.D. Wyner in 1975 [2]. A recent survey for PLS techniques for 5G wireless networks is given in [1], and the various approaches used in PLS are presented in [3]. PLS uses the impairments of the channel like fading and noise for the security [4]. It also does not rely on the computational complexity so even if eavesdropper uses the quantum computer security is maintained. PLS for NOMA and massive MIMO were investigated separately in the literature. The main motivation for this paper is integrating of these 5G technologies for boosting PLS.

NOMA increases spectral efficiency, reduces signalling cost and latency [5]. PLS for NOMA was first investigated in [6] for stochastic geometry networks. Later, its extension was presented in [7] where secrecy performance was improved for single as well as multi antenna stochastic geometry networks. A new approach for secrecy of NOMA systems considering optimal power allocation, optimal decoding order, and transmission rates was given in [8].

Massive MIMO increases the system throughput and capacity by multiplexing the large antenna gain. The beamforming is used for the effective utilization of massive inputs, which is done through precoding methods. PLS for massive MIMO was first investigated in [9]. A brief overview of passive and active eavesdropping for massive MIMO with their mitigation techniques is given in [10]. Massive MIMO itself is resilient to passive eavesdropping as the signal gain is increased for the intended user through beamforming. Eavesdropper's gain does not get affected by this beamforming. Hence, the secrecy capacity which is the difference of users and eavesdropper's capacity increases. The other type of attack is active eavesdropping whose security issues are still in research. Secure communication strategies for active attacks in massive MIMO systems were investigated in [11]. The effect of imperfect CSI on massive MIMO for a secure network is presented in [12].

The utilization of relay in the networks increases the range of communication. It makes the channel cascaded from source to destination. Secrecy performance of the cascaded channel is investigated in [13]. The precoding techniques used in massive

[*] Corresponding author.
E-mail addresses: mtdc.201707@gmail.com (P. Singh), atrivedi@iiitm.ac.in (A. Trivedi).

https://doi.org/10.1016/j.phycom.2019.100977
1874-4907/© 2019 Elsevier B.V. All rights reserved.

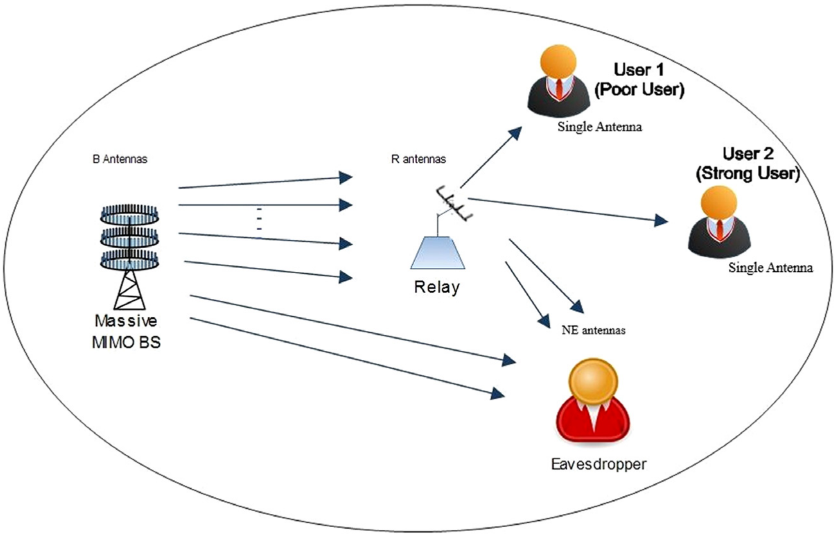

Fig. 1. Considered MIMO-NOMA-based network for PLS systems.

MIMO play an important role in increasing its capacity. The precoding techniques adds up the signal from large number of antennas constructively for the benefit of the legitimate user. There are two types of precoding: linear and non-linear. A comprehensive survey on linear precoding techniques is given in [14], while non-linear techniques are briefly described in [15]. Linear precoding techniques like Zero Forcing (ZF), Minimum-mean square error (MMSE), Maximal Ratio Transmission (MRT) are less complex than the non-linear precoding techniques like dirty paper coding. For MRT, perfect channel state information (CSI) is required [16]. The performance analysis of precoding techniques for multiuser massive MIMO systems is given in [17]. The frequently used precoding techniques for security of massive MIMO are presented in [18]. The precoding is also done by creating artificial noise (AN). AN is produced to degrade the performance of eavesdropper. It does not affect the performance of the legitimate user. The use of AN for secure massive MIMO systems is given in [19] and [20] where AN precoding is used to guarantee the secrecy. The secrecy capacity can be optimized using AN to improve the performance of the system [21].

In this paper, the concepts of massive MIMO and NOMA are integrated for the PLS of 5G wireless communication networks. Also, the performance of orthogonal multiple access (OMA) and NOMA for massive MIMO systems are compared on the basis of secrecy rate. The main contributions of this paper are as follows:

- Integrating the concepts of NOMA and massive MIMO for PLS and hence, developing a novel technique for the security of 5G wireless communication networks. Secrecy performance for the proposed system model is investigated.
- The concept of AN precoding is used to improve the secrecy performance of the given system model. The design of this precoder is based on the property of massive MIMO system.
- A comparative analysis is made for three frequently used linear precoding techniques on the basis of computational complexity and power requirement for finding precoding matrix, and on the basis of average power radiated by per base station (BS) antenna. Simulations are carried out for the verification of results.

The rest of the paper is organized as follows: Section 2 defines the system, channel, and signal model. Section 3 investigates the secrecy performance for the proposed system model. Section 4 describes the different precoding techniques along with the comparison among them. Section 5 describes the artificial noise (AN) precoding. Simulation results are given in Section 6. Finally, concluding remarks are given in Section 7.

Notation. $\boldsymbol{M^H}$, Tr ($\mathbf{M}$), $\|M\|$ denotes the Hermitian-transpose, trace, Frobenius norm of the matrix M, respectively. $\mathbb{V}ar[.]$ and $\mathbb{E}[.]$ are the variance and expectation operators, respectively. The operator $\otimes$ is the Kronecker product and $M \sim \mathcal{CN}(.)$ denotes the circularly symmetric Gaussian distributed random variable.

2. System model

Fig. 1 shows the high level presentation of the proposed system model. Consider a NOMA system having a relay assisted massive MIMO BS (MMBS) having B antennas, an amplify and forward (AF) relay having R antennas (satisfying $B \gg R$), multiple user pairs having single antenna (Consider two single antenna users as a NOMA pair: one poor user (U1) and one strong user (U2) for simplicity) categorized on the basis of channel properties, in the presence of an eavesdropper having multiple antennas (N_E). Eavesdropper can intercept the messages from MMBS to relay and from relay to users. The AF relay amplifies the signal received and forward it to the users. All the channels suffer from large scale path loss and small scale independent Rayleigh fading. In the first time interval, the signal is broadcasted from MMBS to relay using precoding methods. In the second time interval, the relay transfers this received signal to users. The MMBS-to-relay channel matrix gain is represented by W. The relay-to-user channel matrix gain is represented by X. The MMBS-to-user channel is a cascaded channel. The MMBS-to-eavesdropper and relay-to-eavesdropper channel matrix gains are represented by Z and Y, respectively. All channels can be designed in a uniform manner as follows [22]:

$$K = D_K^{1/2}\tilde{K}, \tag{1}$$

where $\tilde{K} \sim \mathcal{CN}_{m\times n}(0_{m\times n}, I_m \otimes I_n)$ is the independent small scale Rayleigh fading. The matrix dimension (m, n) is equivalent to the order of channel matrices $W,\ X,\ Z,\ Y$, respectively. The $m \times m$ diagonal matrix D_K denotes the path-loss having $[D_K]_{j,j} = \zeta_{K,j}$ as the jth diagonal element. Since base station and relay antennas are parallel, the diagonal matrix is defined as: $D_W = \zeta_W I_R$. The path-loss is modelled as $\left(\dfrac{d_{m,n}}{d_0}\right)^{\nu}$; where ν is the path-loss exponent, $d_{m,n}$ refers to the distance between m and n nodes, d_0 is the reference distance.

2.1. Accession of CSI

In NOMA system, the basic requirement for successive interference cancellation (SIC) is to have perfect CSI. In massive MIMO system, the estimation of downlink channel is impractical at the users node because of very large number of BS antennas. Uplink channel $\hat{W}$ is estimated at BS and $\hat{X}$ is estimated at the relay by the method of pilot signalling. Downlink channel is estimated via channel reciprocity assuming the channel is reciprocal. Assuming the system has perfect CSI. The minimum mean square error (MMSE) estimators are given below [22]:

$$\hat{W} = D_W \left(D_W P_{p_1} + I_R\right)^{-1} \left(W\sqrt{P_{p_1}} + N_W\right)\sqrt{P_{p_1}}, \tag{2}$$

$$\hat{X} = D_X \left(D_X P_{p_2} + I_K\right)^{-1} \left(X\sqrt{P_{p_2}} + N_X\right)\sqrt{P_{p_2}}, \tag{3}$$

where $P_{p_1} = T_{R_1}P_{R_1}$ and $P_{p_2} = T_{U_2}P_{U_2}$. Here, T_{R_1} and T_{U_2} are delay of pilot transmission from relay and the users, respectively. P_{R_1} and P_{U_2} are the powers for pilot transmission from relay and users, respectively. N_W, N_X, X and W, are statistically independent, where N_W, N_X are the faded parameters for the estimated channels, respectively.

By using orthogonal property of MMSE,

$$X = \hat{X} + \mathcal{E}_X, \tag{4}$$

where $\mathcal{E}_X$ is an error matrix from estimation which is statistically independent from $\hat{X}$, and both are distributed as $\mathcal{CN}(0,\ D_X - \hat{D}_X)$ and $\mathcal{CN}(0, \hat{D}_X)$, respectively. The jth entry of the diagonal matrix $\hat{D}_X$ is given by

$$\hat{\zeta}_{X_j} = \frac{P_{p_2}{\zeta_{X_j}}^2}{P_{p_2}\zeta_{X_j} + 1}. \tag{5}$$

2.2. Signal model

In the first time interval, the MMBS broadcasts the signal vector as

$$y_t = P_{th} * x_t * \hat{H}, \tag{6}$$

where

$$x_t = \alpha_{11}S_1 + \alpha_{22}S_2, \tag{7}$$

where α_{11} and α_{22} are the power allocation factors for the two users, satisfying ${\alpha_{11}}^2 + {\alpha_{22}}^2 = 1$. More power is allocated to the user, whose channel conditions are poor, to compensate channel conditions. P_{th} is the transmit power allocated for the user symbols. $\hat{H}$ is the precoder. The precoding techniques used at the MMBS helps to effectively use the concept of massive MIMO.

table The signal received at the relay through MMBS is given by

$$y_r = W * y_t + N_B, \tag{8}$$

where W is the channel matrix gain from MMBS to relay of order $R \times B$. y_t is the signal transmitted vector from MMBS to relay. N_B is the additive white Gaussian noise (AWGN) vector satisfying $E[N_B {N_B}^H] = {\sigma_B}^2 I_{NB}$. This is due to the orthonormal property for the Hermitian matrix.

The transmitted signal from MMBS also supposed to be leaked to eavesdropper. The received signal at eavesdropper through MMBS is defined by

$$y_e = Z * y_t + N_E, \tag{9}$$

where Z is the channel matrix gain from MMBS to eavesdropper of order $E \times B$. y_t is the signal transmitted vector from MMBS to relay. N_E is the AWGN vector satisfying $E[N_E {N_E}^H] = {\sigma_E}^2 I_{NE}$.

In the second time interval, the relay transfers the received information to users. The AF relay amplifies and forwards the received signal towards the destination without decoding it. The signal received at the user i is,

$$y_{r,i} = \beta * y_t * W * X_i + \beta * N_B * X_i + N_{U,i}, \tag{10}$$

where X_i is the channel matrix gain from the relay to user i of order $R \times 1$. $N_{U,i}$ is the AWGN vector at user nodes satisfying $E[N_{U,i}{N^H}_{U,i}] = {\sigma_U}^2 I_{N_{U,i}}$, and β is the relay amplification factor given by

$$\beta^2 = P_r \Bigg/ \left(P_t\ \mathbb{E}\left[\mathrm{Tr}\left(W\hat{H}\left(W\hat{H}\right)^H\right)\right] + R\sigma_B^2\right), \tag{11}$$

where P_r is the relay transmit power. P_t is the MMBS transmit power.

The wireless transmitted signals are broadcasting in nature, so eavesdropper also get the replica of the information from the relay and the replica signal received at the eavesdropper from relay is defined by

$$y_{r,e} = \beta * x_t * W * Y_i + \beta * N_B * Y_i + N_{E,i}. \tag{12}$$

where Y_i is the channel matrix gain from the relay to the eavesdropper. $N_{E,i}$ is the AWGN vector satisfying the orthonormal property.

2.2.1. Users capacity

In the NOMA technology, SIC is applied at the receiver (strong user) to decode the signal s_i of user i. Since the power at the strong user in downlink is greater than the power at transmitter in uplink, so SIC is performed which considers uplink powers as noise [23]. The transmission channel capacity from the AF relay to user i can be defined by [22]

$$C_{r,i} = \frac{\min(T_{C1} - T_{R1}, T_{C2} - T_{U2})}{T_{C1} + T_{C2}}\ log_2(1 + \gamma_{r,i}), \tag{13}$$

where $\gamma_{r,1}$ $(i = 1)$ represents the instantaneous signal-to-interference-plus-noise ratio (SINR) at user 1. $\gamma_{r,2}$ $(i = 2)$ denotes the received signal-to-noise ratio (SNR) at user 2. T_{C1} and T_{C2} are the coherence time interval in first and second time intervals, respectively. $\gamma_{r,1}$ and $\gamma_{r,2}$ are given in (14), (15), respectively.

$$\gamma_{r,1} = \frac{\beta^2\alpha_{11}^2 P_t \mathbb{E}\left[\left|x_1 W\hat{h}_1\right|^2\right]}{\beta^2\alpha_{22}^2 P_t \mathbb{E}\left[\left\|x_1 W\hat{h}_{i\neq 1}\right\|^2\right] + \beta^2 P_t \mathbb{V}\mathrm{ar}\ \left[x_1 W\hat{h}_1\right] + \beta^2\sigma_B^2 R + \sigma_U^2}, \tag{14}$$

$$\gamma_{r,2} = \frac{\beta^2\alpha_{22}^2 P_t \mathbb{E}\left[\left|x_2 W\hat{h}_2\right|^2\right]}{\beta^2 P_t \mathbb{V}\mathrm{ar}\ \left[x_2 W\hat{h}_2\right] + \beta^2\sigma_B^2 R + \sigma_U^2}. \tag{15}$$

2.2.2. Eavesdropper capacity

As MMBS and relay transmits in different time intervals, eavesdropper will have two chances to intercept the information. In the first time interval, the information rate leakage from MMBS to eavesdropper is given by the Shannon's capacity definition

$$C_{E_{i,1}} = 0.5 * log_2\ (1 + \gamma_{E_{i,1}}), \tag{16}$$

where $\gamma_{E_{i,1}}$ is the received SNR at eavesdropper from MMBS as given in (17).

$$\gamma_{E_{i,1}} = \frac{P_t \mathbb{E}\left[\left|z_i\hat{h}_i\right|^2\right]}{P_t \mathbb{E}\left[\left|z_i\hat{h}_{\neq i}\right|^2\right] + {\sigma_E}^2 I_{NE}}, \tag{17}$$

In the second time interval, the information rate leakage from relay to users is given by

$$C_{E_{i,2}} = 0.5 * log_2\ (1 + \gamma_{E_{i,2}}), \tag{18}$$

Table 1
Number of complex multiplications for precoding techniques.

Techniques	Number of complex multiplications
MMSE	$\tau(BR+RK)+\frac{3}{2}(B^2R+R^2K)+\frac{1}{2}(BR+RK)+\frac{1}{3}((B^3-B)+(R^3-R))$
ZF	$\tau(BR+RK)+\frac{3}{2}(R^2B+K^2R)+\frac{1}{2}(RB+KR)+\frac{1}{3}((R^3-R)+(K^3-K))$
MRT	$\tau\,\frac{3}{2}(R^2B+K^2R)$

where $\gamma_{E_{i,2}}$ is the received SNR at eavesdropper from relay as given in (19).

$$\gamma_{E_{i,2}}=\frac{\beta^2\alpha^2{}_{ii}P_t\mathbb{E}\left[\left|y_iW\hat{h}_i\right|^2\right]}{\beta^2P_t\mathbb{E}\left[\left\|y_iW\hat{h}_{\neq i}\right\|^2\right]+\beta^2\sigma^2{}_BYY^H+\sigma^2{}_EI_{NE}}, \tag{19}$$

Therefore, the average information rate leaked to the eavesdropper is the average leakage in the two time slots given by

$$C_{E,i}=\frac{1}{2}(C_{E_{i,1}}+C_{E_{i,2}}). \tag{20}$$

3. Secrecy performance

The secrecy rate or the achievable rate of the system for user i is the difference between the user capacity and the eavesdropper capacity given by [24]

$$C_i=\left\lceil C_{r,i}-C_{E,i}\right\rceil^+ \tag{21}$$

where $\lceil x\rceil^+=\max(x,0)$. If the value of C_i becomes positive then the system is secure.

3.1. Secrecy Outage Probability (SOP)

If R_i is the target rate of user i, then outage occurs whenever C_i falls below their target rates. SOP is given by [24]

$$\begin{aligned}\mathrm{SOP}&=Pr\ (C_1<R_1 \text{ or } C_2<R_2)\\&=1-Pr\ (C_1>C_{R_1} \text{ or } C_2>C_{R_2}),\end{aligned} \tag{22}$$

where $C_{R_i}=2^{2R_i}$. SOP should be as small as possible.

3.2. Strictly Positive Secrecy Capacity (SPSC)

The probability of existence of secrecy capacity is measured in terms of SPSC given by [24]

$$\mathrm{SPSC}=Pr\ (C_1>0\ \text{ or } C_2>0), \tag{23}$$

It should be as high as possible.

4. Precoding techniques

Precoding increases the efficiency of the transmitter antennas by adding up the signals from individual antenna constructively, hence, it increases the signal gain for the legitimate users. It also reduces the fading effect of channel. The three types of precoding techniques considered are [18]:

4.1. MMSE

It is the minimum mean square error method keeping constraint on the average transmit power by each transmitted antenna at the BS. The precoding matrix for MMSE is given by:

$$\hat{H}_{MMSE}=\eta_1(\hat{X}\hat{W})^H\left(\hat{X}\hat{W}\left(\hat{X}\hat{W}\right)^H+\frac{K}{P_t}I_K\right)^{-1}, \tag{24}$$

where $\eta_1=(\mathbb{E}[\mathrm{Tr}(\hat{X}\hat{W})^H\left(\hat{X}\hat{W}\left(\hat{X}\hat{W}\right)^H+\frac{K}{P_t}I_K\right)^{-1}])^{-1/2}$ is the power normalization factor.

Table 2
Power requirement for finding $\hat{H}$.

Techniques	Transmit power per base station antenna (In Watts)
MMSE	Convergence factor $*\,(\frac{Bandwidth}{\text{Coherence Blocks}}\left(\frac{K^3+R^3}{3L_{CE}}+\frac{3RK^2+RK+3BR^2+BR}{L_{CE}}\right))$
ZF	$\frac{Bandwidth}{\text{Coherence Blocks}}\left(\frac{K^3+R^3}{3L_{CE}}+\frac{3RK^2+RK+3BR^2+BR}{L_{CE}}\right)$
MRT	$\frac{Bandwidth}{\text{Coherence Blocks}}\ \frac{3BR+3RK}{L_{CE}}$

4.2. ZF

It nullifies the multi-user interference signals from the transmitter consisting of multiple antennas at the expense of losing signal gain. It requires perfect CSI, else, some residual multiuser interference inversely affects the system. The precoding matrix for ZF is given by:

$$\hat{H}_{ZF}=\eta_2(\hat{X}\hat{W})^H\left(\hat{X}\hat{W}\left(\hat{X}\hat{W}\right)^H\right)^{-1}, \tag{25}$$

where $\eta_2=\left(\mathbb{E}\left[\mathrm{Tr}\left(\hat{X}\hat{W}(\hat{X}\hat{W})^H\right)^{-1}\right]\right)^{-1/2}$ is the power normalization factor.

4.3. MRT

It increases the signal gain for the legitimate receiver. It is perfect for noise limited systems, where multi-user interference is negligible. The precoding matrix for MRT is given by:

$$\hat{H}_{MRT}=\eta_3(\hat{X}\hat{W})^H, \tag{26}$$

where $\eta_3=\left(\mathbb{E}\left[\mathrm{Tr}\left((\hat{X}\hat{W})^H\left((\hat{X}\hat{W})^H\right)^H\right)\right]\right)^{-1/2}$ is the power normalization factor.

4.4. Comparison of linear precoding techniques

The three frequently used linear precoding techniques are compared on three different aspects: (1) On the basis of computational complexity, (2) On the basis of required power for evaluating precoding matrix, and (3) On the basis of average power radiated each MMBS antenna.

(1) *On the basis of computational complexity*: The number of complex multiplications required for evaluating $\hat{h}$ is given in Table 1.

(2) *On the basis of power requirement for finding* $\hat{H}$: The linear processing is used to find out precoding vectors [25], then the power required for computing $\hat{H}$ is given by Table 2.

(3) *On the basis of average power radiated per MMBS antenna*: The massive MIMO works for optimal number of users effectively. The comparison among linear precoding techniques is carried out on the basis of average radiated power per MMBS antenna [25] as shown in the simulation results.

5. Artificial Noise (AN) precoding

AN is generated intentionally to use it constructively. In this research work, selfish null space based AN precoder [19] is used to eliminate the drawback (for some SNR range, performance is not good) of the proposed work. This is a linear type of AN precoding. In this AN precoding, the AN shaping matrix is adopted to exist in the null space of the estimated channel. The selfish null space based AN precoder is defined as

$$NL = T/\sqrt{\mathbb{E}[Tr(TT^H)]} \tag{27}$$

where T can be determined as

$$T = I_B - (\hat{X}\hat{W})^H \left(\hat{X}\hat{W}(\hat{X}\hat{W})^H\right)^{-1}\hat{X}\hat{W}. \tag{28}$$

At the base station, this AN precoder is designed such that the AN signals exists in the null space of the channel between MMBS and user through relay, i.e, XW as $(NL)(XW)^H = 0$. As perfect CSI of user channel is available at the MMBS, AN does not affect the user's performance as it nulls out the AN. However, the eavesdropper channel is independent of users channel. Hence, AN does not lie completely in its null space. Therefore, it affects the channel gain for the eavesdropper.

5.1. Analysis with AN precoding

By utilizing the concept of AN precoding, the signal transmitted from MMBS in the first interval is given by

$$y_{t_{AN}} = P_{th} * x_t * \hat{H} + P_{AN} NL g_{AN}, \tag{29}$$

where P_{AN} is the power assigned to AN signal at MMBS, g_{AN} is the AN vector represented as $\mathcal{CN}(0, \sigma_g^2 I_R)$, NL is the precoding AN matrix (order of $B \times R$). At the relay, the signal received from MMBS is defined by

$$y_{r_{AN}} = W * y_{t_{AN}} + N_B, \tag{30}$$

The signal from MMBS is leaked towards eavesdropper as

$$y_{e_{AN}} = Z * y_{t_{AN}} + N_E \tag{31}$$

In the second time interval, after relay amplification, the signal transfers towards user i is defined by

$$y_{r,i_{AN}} = \beta * y_{t_{AN}} * W * X_i + \beta * N_B * X_i + N_{U,i}, \tag{32}$$

Also, the information leaked towards eavesdropper through the relay is given by

$$y_{r,e_{AN}} = \beta * y_{t_{AN}} * W * Y_i + \beta * N_B * Y_i + N_{E,i}, \tag{33}$$

Following these signal transmissions, the definition for users capacity (13), and eavesdropper capacity (16), (18), (20), remains same. But, the SINR and SNR in (14), (15), (17), (19), are modified as (34), (35), (36), (37), respectively (see Box I).
The secrecy performance is analysed based on these modifications. The definitions for the performance metrics remain same for the analysis.

6. Results and discussions

6.1. Comparison of precoding techniques

The comparison of three frequently used linear precoding techniques will be done in three aspects: (1) On the basis of computational complexity. (2) On the basis of power required for computing precoding matrix. (3) On the basis of average power radiated per BS antenna.

Consider matrix A (order of $N_1 \times N_2$) and matrix B (order of $N_2 \times N_3$). The matrix product AB requires $N_1N_2N_3$ complex multiplications. The matrix product AA^H requires $(\frac{{N_1}^2+N_1}{2}N_2)$ complex multiplications. The A^H requires $(\frac{{N_1}^2+N_1}{2})$ complex multiplications. Number of complex multiplications common to all techniques required for receiver processing is given by $\tau *$ transmitter antennas $*$ receiver antennas.

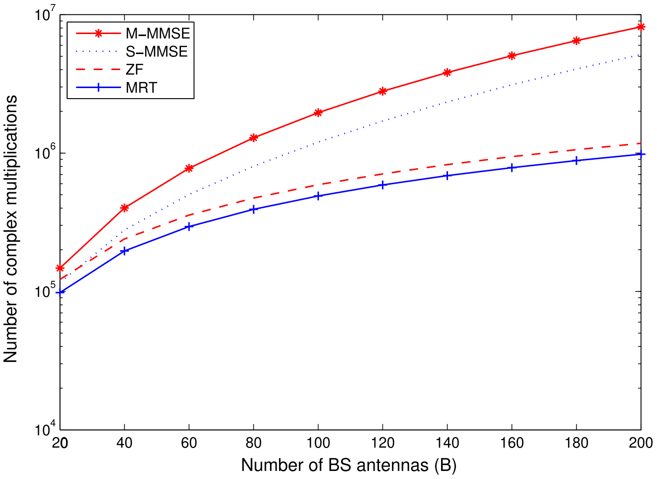

Fig. 2. Number of complex multiplications Vs number of MMBS antennas.

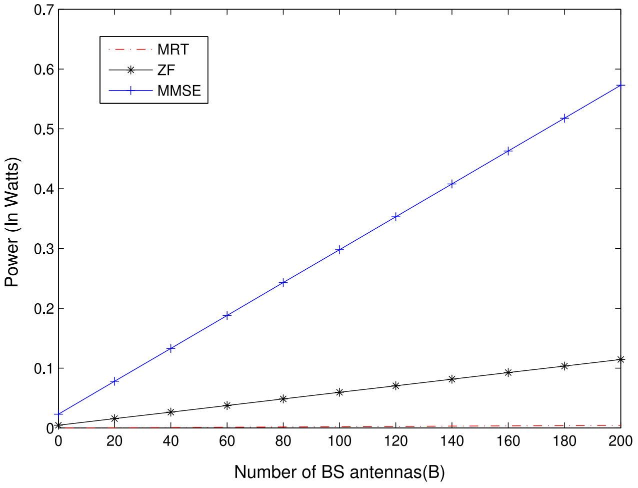

Fig. 3. Power required for computing $\hat{H}$.

The comparison of the precoding techniques on the basis of computational complexity is given in Fig. 2. It shows that as the number of MMBS antennas increases, number of complex multiplications also increases for all techniques. S-MMSE and M-MMSE represents the single and multiple cell for the MMSE technique, respectively. It can be observed that MRT requires the least complex multiplications among all other mentioned techniques.

In [26], the power requirement for computing linear precoding matrix is defined. Simulation results for this consideration in given in Fig. 3. Results show that the power requirement for computing MRT matrix is the lowest.

Taking the same simulation parameters as given in [26], the comparison of precoding techniques on the basis of radiated power per MMBS antenna is given in Fig. 4. It may be observed that, MRT gives the best performance in this aspect.

From above analysis, it may seen that the MRT outperforms other linear precoding techniques in all the three given performance measures. So the MRT will be used for the analysis of secrecy performance of the given system model.

$$\gamma_{r,1_{AN}} = \frac{\beta^2\alpha_{11}^2 P_t \mathbb{E}\left[\left|x_1 W\hat{h}_1\right|^2\right]}{\beta^2\alpha_{22}^2 P_t\mathbb{E}\left[\left\|x_1 W\hat{h}_{i\neq 1}\right\|^2\right] + \beta^2{\sigma_g}^2 P_{AN}\mathbb{E}\left[||x_1 WNL||^2\right] + \beta^2 P_t \mathbb{V}\mathrm{ar}\left[x_1 W\hat{h}_1\right] + \beta^2\sigma_B^2 R + \sigma_U^2}, \tag{34}$$

$$\gamma_{r,2_{AN}} = \frac{\beta^2\alpha_{22}^2 P_t \mathbb{E}\left[\left|x_2 W\hat{h}_2\right|^2\right]}{\beta^2{\sigma_g}^2 P_{AN}\mathbb{E}\left[||x_2 WNL||^2\right] + \beta^2 P_t \mathbb{V}\mathrm{ar}\left[x_2 W\hat{h}_2\right] + \beta^2\sigma_B^2 R + \sigma_U^2}, \tag{35}$$

$$\gamma_{E_{i,1}} = \frac{P_t \mathbb{E}\left[\left|z_i\hat{h}_i\right|^2\right]}{P_t\mathbb{E}\left[\left|z_i\hat{h}_{\neq i}\right|^2\right] + \sigma_g^2 P_{AN}\mathbb{E}\left[||z_i NL||^2\right] + {\sigma_E}^2 I_{NE}}, \tag{36}$$

$$\gamma_{E_{i,2}} = \frac{\beta^2{\alpha^2}_{ii} P_t \mathbb{E}\left[\left|y_i W\hat{h}_i\right|^2\right]}{\beta^2 P_t\mathbb{E}\left[\left\|y_i W\hat{h}_{\neq i}\right\|^2\right] + \beta^2\sigma_g^2 P_{AN}\mathbb{E}\left[||y_i WNL||^2\right] + \beta^2{\sigma^2}_B YY^H + {\sigma^2}_E I_{NE}}. \tag{37}$$

Box I.

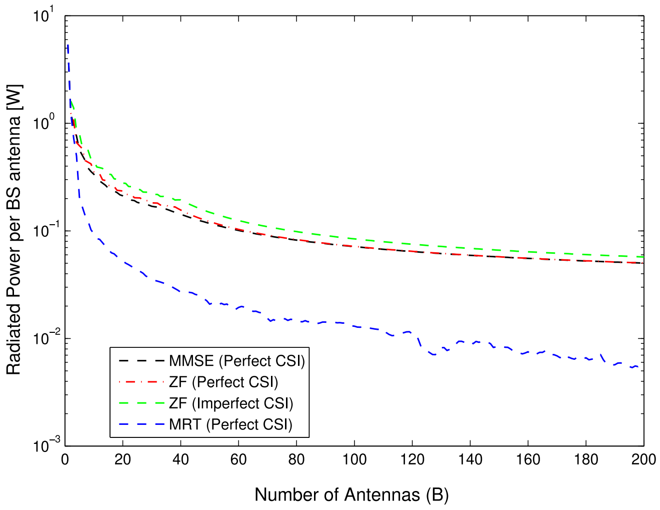

Fig. 4. Power radiated by per MMBS antenna.

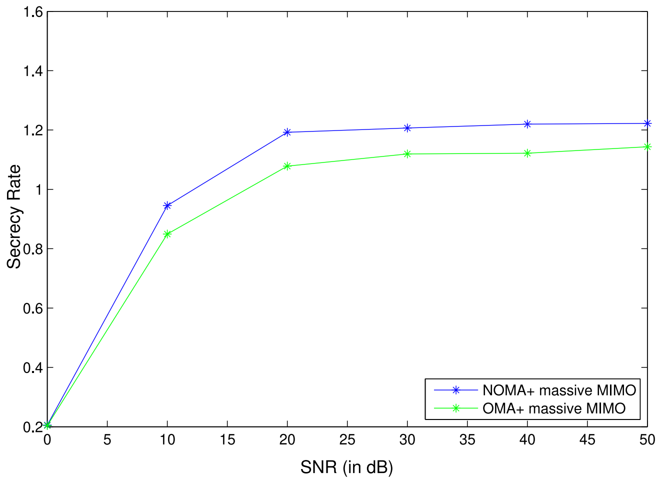

Fig. 5. Secrecy capacity of NOMA Vs OMA for massive MIMO systems.

6.2. Secrecy performance

Simulation parameters considered for the analysis of secrecy performance of the proposed system model is given in Table 3.

Fig. 5 shows simulation results for the secrecy rate of the massive MIMO system for NOMA as well as orthogonal multiple access (OMA). Results show that the secrecy rate for the proposed system model using NOMA is positive, hence, the system is secure. The results are better for NOMA than that of OMA. The integration of NOMA and massive MIMO for the PLS results in a novel technique for the 5G wireless communication networks.

Fig. 6 shows the variation of outage probability in accordance with the increasing SNR. Results shows that proposed technology is good for high SNR values (greater than 22 dB) as the outage probability is less as compared to existing technology [24]. It means the secrecy performance of the system is improved using two 5G technologies. For low SNR, secrecy performance is low which is a drawback of the proposed system model. By using the concept of AN precoding, this drawback is eliminated. The results of using AN with NOMA integrated with massive MIMO outperforms the existing technique for all range of SNR.

Table 3
Parameters considered for results.

Parameter	Value
T_{c1}, T_{c2}	196 samples
T_{R1} = B	200 antennas
T_{U2} = R	25
K	2
α_{11}, α_{22}	${\alpha_{11}}^2 + {\alpha_{22}}^2 = 1$
α_{11}	0.86
Bandwidth	20 MHz
Computation efficiency (L_{CE})	12.8 Gflops/Watts
Coherence block	1800
Convergence factor	100
$P_r = P_t = P_{R1} = P_{U2}$	10 dBW
Path loss exponent	2.4
Reference distance	100 m
Eavesdropper distance from relay	200 m
Eavesdropper distance from MMBS	200 m
Noise power (all)	0 dBW

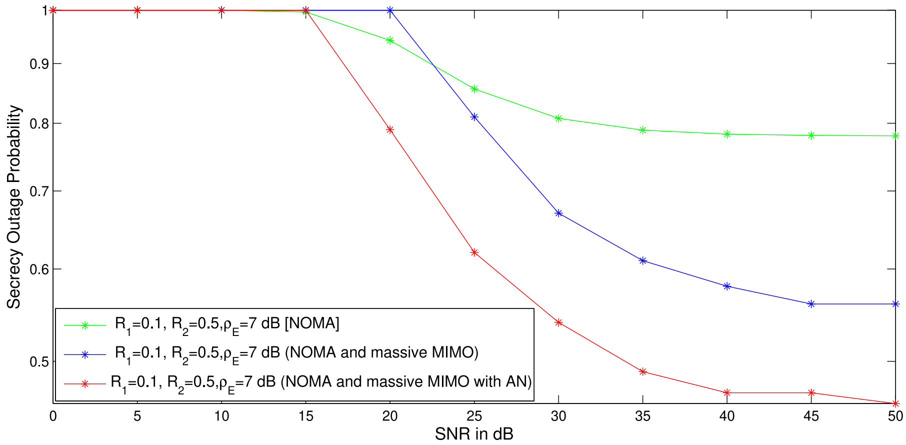

Fig. 6. Secrecy Outage probability Vs SNR.

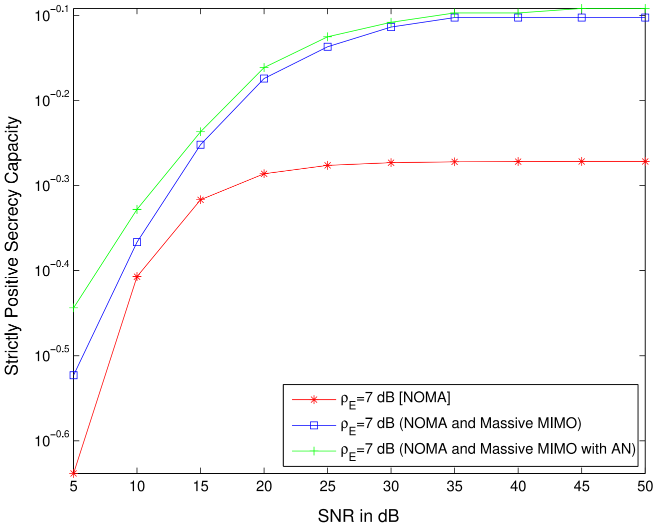

Fig. 7. Strictly positive secrecy capacity Vs SNR.

Fig. 7 shows that the strictly positive secrecy rate versus SNR. The results shows that the secrecy capacity is more for the proposed method than the existing method [24]. With the application of AN precoding, performance further increases.

7. Conclusion

A novel approach for PLS utilizing two 5G technologies viz. NOMA and massive MIMO is investigated. The comparison among the three frequently used linear precoding techniques is carried out, and the most suitable technique, i.e, MRT is used for further investigation. The secrecy performance for the proposed system model is investigated, and the results shows that the outage probability is good for a range of SNR as compared to the existing techniques. After utilizing the concept of AN precoding, the performance is improved practically for all SNR values when compared to the existing technique. Results also show that the achievable rate for NOMA is greater than the OMA.

In this paper, perfect CSI is considered at all the nodes. But in practical scenario, it is not possible to attain perfect CSI. Also, at very low SNR, the performance of this proposed approach cannot be distinguished with the existing techniques. In future, the effect of imperfect CSI may be investigated.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, X. Gao, A survey of physical layer security techniques for 5G wireless networks and challenges ahead, IEEE J. Sel. Areas Commun. 36 (4) (2018) 679–695.

[2] A.D. Wyner, The wire-tap channel, Bell Syst. Tech. J. 54 (8) (1975) 1355–1387.

[3] P. Singh, P. Pawar, A. Trivedi, Physical layer security approaches in 5G wireless communication networks, in: 2018 First International Conference on Secure Cyber Computing and Communication, ICSCCC, NIT Jalandhar, 2018 December, 2018, pp. 477–482.

[4] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, M. Di Renzo, Safeguarding 5G wireless communication networks using physical layer security, IEEE Commun. Mag. 53 (4) (2015) 20–27.

[5] L. Dai, B. Wang, Y. Yuan, S. Han, I. Chih-Lin, Z. Wang, Non-orthogonal multiple access for 5G: solutions, challenges, opportunities, and future research trends, IEEE Commun. Mag. 53 (9) (2015) 74–81.

[6] Z. Qin, Y. Liu, Z. Ding, Y. Gao, M. Elkashlan, Physical layer security for 5G non-orthogonal multiple access in large-scale networks, in: 2016 IEEE International Conference on Communications, ICC, Malaysia, 2016 May 22, IEEE, 2016, pp. 1–6.

[7] Y. Liu, Z. Qin, M. Elkashlan, Y. Gao, L. Hanzo, Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks, IEEE Trans. Wireless Commun. 16 (3) (2017) 1656–1672.

[8] B. He, A. Liu, N. Yang, V.K. Lau, On the design of secure non-orthogonal multiple access systems, IEEE J. Sel. Areas Commun. 35 (10) (2017) 2196–2206.

[9] J. Zhu, R. Schober, V.K. Bhargava, Secure transmission in multi-cell massive MIMO systems, in: 2013 IEEE Globecom Workshops, GC Wkshps, Atlanta USA, 9–13 December 2013, 2013, pp. 1286–1291.

[10] D. Kapetanovic, G. Zheng, F. Rusek, Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks, IEEE Commun. Mag. 53 (6) (2015) 21–27.

[11] Y. Wu, R. Schober, D.W.K. Ng, C. Xiao, G. Caire, Secure massive MIMO transmission with an active eavesdropper, IEEE Trans. Inform. Theory 62 (7) (2016) 3880–3900.

[12] T. Yang, R. Zhang, X. Cheng, L. Yang, Secure massive MIMO under imperfect CSI: Performance analysis and channel prediction, IEEE Trans. Inf. Forens. Secur. 14 (6) (2019) 1610–1623.

[13] S.O. Ata, Secrecy performance analysis over cascaded fading channels, IET Commun. 13 (2) (2019) 259–264.

[14] N. Fatema, G. Hua, Y. Xiang, D. Peng, I. Natgunanathan, Massive MIMO linear precoding: A survey, IEEE Syst. J. 12 (4) (2018) 3920–3931.

[15] F. Hasegawa, H. Nishimoto, N. Song, M. Enescu, A. Taira, A. Okazaki, A. Okamura, Non-linear precoding for 5G NR, in: 2018 IEEE Conference on Standards for Communications and Networking, CSCN, Paris France, 29–31 October 2018, 2018, pp. 1–7.

[16] T.K.Y. Lo, Maximum ratio transmission, IEEE Trans. Commun. 47 (10) (1999) 1458–1461.

[17] V.A. Beulah, S. Markkandan, Performance analysis of precoding techniques for massive MU-MIMO systems, in: 2015 International Conference on Innovations in Information, Embedded and Communication Systems, ICIIECS, Coimbatore, India, 19–20 March, 2015, 2015, pp. 1–5.

[18] M.H. Kabir, S.Z. Rashid, A. Gafur, M.N. Islam, M.J. Hoque, Maximum energy efficiency of three precoding methods for massive MIMO technique in wireless communication system, in: 2019 International Conference on Electrical, Computer and Communication Engineering, ECCE, Bangladesh, 7–9 February 2019, 2019, pp. 1–5.

[19] J. Zhu, R. Schober, V.K. Bhargava, Linear precoding of data and artificial noise in secure massive MIMO systems, IEEE Trans. Wireless Commun. 15 (3) (2016) 2245–2261.

[20] S. Goel, R. Negi, Guaranteeing secrecy using artificial noise, IEEE Trans. Wireless Commun. 7 (6) (2008) 2180–2189.

[21] Y. Gu, Z. Wu, Z. Yin, X. Zhang, The secrecy Capacity optimization artificial noise: A new type of artificial noise for secure communication in MIMO system, IEEE Access 7 (2019) 58353–58360.

[22] S. Timilsina, G. Amarasuriya, Secure communication in relay-assisted massive MIMO downlink, in: GLOBECOM 2017 - 2017 IEEE Global Communications Conference, Singapore, 4–8 December 2017, 2017, pp. 1–7.

[23] Y. Sun, D.W.K. Ng, Z. Ding, R. Schober, Optimal joint power and subcarrier allocation for full-duplex multicarrier non-orthogonal multiple access systems, IEEE Trans. Commun. 65 (3) (2017) 1077–1091.

[24] J. Chen, L. Yang, M. Alouini, Physical layer security for cooperative NOMA systems, IEEE Trans. Veh. Technol. 67 (5) (2018) 4645–4649.

[25] E. Björnson, L. Sanguinetti, J. Hoydis, M. Debbah, Optimal design of energy-efficient multi-user MIMO systems: Is massive MIMO the answer? IEEE Trans. Wireless Commun. 14 (6) (2015) 3059–3075.

[26] E. Björnson, J. Hoydis, L. Sanguinetti, Massive MIMO networks: Spectral, energy, and hardware efficiency, Found. Trends Signal Process. 11 (3–4) (2017) 154–655, [Online]. Available: http://dx.doi.org/10.1561/2000000093.

Pooja Singh is a post graduate student at ABV-IIITM, Gwalior working in the area of Digital Communication. Her research interests include physical layer security, 5G technology, artificial noise precoding, etc.
Email id- mtdc_201707@iiitm.ac.in.

Aditya Trivedi is a professor in the ICT department of ABV-IIITM, Gwalior, India. He obtained his Ph.D. from IIT Roorkee in the area of Wireless Communication Engineering. His teaching and research interest include Digital Communication, Signal Processing, Physical layer security, Advance communication techniques like mm wave, massive MIMO, and D2D. He is a fellow of the Institution of Electronics and Telecommunication Engineers (IETE) and a member of Institution of Electrical and Electronics Engineers (IEEE), USA.
Email id- atrivedi@iiitm.ac.in.