symmetry

*Article*

# Secure Beamforming in 5G-Based Cognitive Radio Network

**Hyils Sharon Magdalene Antony * and Thulasimani Lakshmanan ***

Department of Electronics and Communication Engineering, PSG College of Technology, Peelamedu, Coimbatore 641004, India

* Correspondence: hsm.ece@psgtech.ac.in (H.S.M.A.); ltm.ece@psgtech.ac.in (T.L.); Tel.: +91-8754079046 (H.S.M.A.); +91-9443654012 (T.L.)

Received: 14 August 2019; Accepted: 18 September 2019; Published: 9 October 2019

**Abstract:** Cognitive radio network (CRN) and non-orthogonal multiple-access (NOMA) is a significant system in the 5G wireless communication system. However, the system is an exceptional way for the cognitive users to secure a communication from the interferences in multiple-input multiple-output (MIMO)-NOMA-based cognitive radio network. In this article, a new beamforming technique is proposed to secure an information exchange within the same cells and neighboring cells from all intervened users. The interference is caused by an imperfect spectrum sensing of the secondary users (SUs). The SUs are intended to access the primary channels. At the same time, the primary user also returns to the channel before the SUs access ends. This similar way of accessing the primary channel will cause interference between the users. Thus, we predicted that the impact of interferences would be greatly reduced by the proposed technique, and that the proposed technique would maximize the entire secrecy rate in the 5G-based cognitive radio network. The simulation result provides better evidence for the performance of the proposed technique.

**Keywords:** cognitive radio network; non-orthogonal multiple-access; multiple-input multiple-output; 5G engineering

## 1. Introduction

The future technique of 5G-based cognitive radio network (CRN) has high throughput and low latency with a wide range of connectivity. This target was achieved by the non-orthogonal multiple-access (NOMA) technique to reuse the resources in spatial [1] and temporal varieties. A NOMA uses the distinct channel gains within the same cell and assigns the same frequency to a number of users. A NOMA is combined with a multiple-input multiple-output (MIMO) system [2] to obtain a high diversity and a high spectral efficiency in a multi-cell substructure. A serious interference will be caused due to the high spectral efficiency in NOMA network. Thus, security is needed for the design of communication systems in the MIMO-NOMA framework [1,2]. The transmitting and receiving beamforming techniques were used in [3] to reduce the inter- and intra-cell interferences. The eavesdroppers may secretly listen to the channel by simply ignoring the receiving beamformer technique. The signal alignment and the receiving beamformer methods were used in [4,5] to control the interference and raise the total throughput. The greedy algorithm and a convex approximation method were used in [6] to solve the scheduling problem. A two-stage transmission [7] scheme was used in the cooperative NOMA system model. During the first stage, the source transmits the code symbol to the relay and the destination. At the last stage, the relay decodes and forwards a new code symbol to the destination with the corresponding power allocation factor. The artificial noise method was used in [8] to secure the transmission in the MIMO-NOMA system model. The convex optimization problem was solved in [9] for the better MIMO-NOMA network. In [10], an investigation was based on the joint subcarrier (SC) assignment and the power allocation problem in NOMA features in the presence of eavesdroppers. The cooperative jamming (CJ) technique and the smart sensor protocol algorithm (SSPA) were implemented in the security of the better communication link. Then, the overall energy efficiency was increased. The relay-based downlink NOMA network contains the physical layer security (PLS) and was considered in [11]. The receiver beamforming technique used in [3–5,8,9] does not provide a beneficial assurance for the system security in a multi-cell network.

In this article, the proposed beamforming technique was compared with the existing zero forcing technique, which was used in [12]. The simulation results provide better evidence for the enhancement of the proposed method.

## 2. Related Work and Contributions

### 2.1. Zero-Forcing Beamforming (ZFBF) Related Works

A downlink cascaded transmitting ZFBF technique [12] was proposed to secure the communications in a two-cell MIMO-NOMA-based CRN. This technique was combined with the proposed method for better security in the MIMO-NOMA network. It should be noted that this article uses an existing method in which the proposed technique has improved greatly.

In [13], a beamforming (BF) scheme was proposed to use the interference as a green source for the enhancement of PLS in the satellite network. The ZFBF technique was used as a sub-method for the secure communication in the cognitive satellite terrestrial network (CSTN) with a sphere decoder algorithm (SDA).

The joint design of the beamforming vector and an artificial noise covariance matrix was investigated [14] for the multiple-input-single-output-multiple eavesdropper simultaneous wireless information and power transfer (MISOME-SWIPT) systems. In the MISOME-SWIPT system, the base station (BS) sends an information signal to the honest user equipment and transmits a jamming signal to the eavesdropper. A secret energy efficiency (SEE) maximization problem was proposed for the MISOME-SWIPT system with an imperfect channel state information (CSI). A ZFBF method was used in the MISOME-SWIPT system to perform the task, but did not show better improvement than SEE.

In [15], a uniform planar array (UPA) at the BS was applied for the robust security of 5G cellular networks coexisting with a satellite network. Then, a known imperfect angle of arrival (AoA)-based CSI was assumed of a multiple Eves. The constrained optimization problem was formulated to maximize the secrecy rate (SR) of the cellular user under the limitations of the transmit power at the BS. Two robust BF methods were proposed to solve the complex optimization problem for both an uncoordinated and a coordinated Eves. The authors then converted the non-convex problem into a convex one, and further proposed an iterative penalty function (IPF)-based algorithm to obtain the optimal beamforming weight vectors. ZFBF methods were also used as one of the methods to solve the same problem, but the performance was not higher than that of an IPF-based algorithm.

In [16], an optimal multiuser multiple-input single-output (MISO) beamforming for power splitting SWIPT CRN was studied. A multi-antenna secondary trasnsmitter (ST) sent a data stream to multiple single antenna single receivers (SRs) equipped with a power splitting (PS) structure for an information decoding and an energy harvesting. A non-convex problem occurred in this structure, which was solved by an optimal method. First, the problem with fixed PS ratios was solved using the software-defined ratio (SDR) technique and the optimal PS ratios were found using the particle swarm optimization (PSO) method. The overall EPS technique was used to solve the problem, which showed a better performance than all other methods. A ZFBF technique was also proposed to solve the problem. It showed a better performance than the optimal methods, but a slightly worse performance compared with the equal power splitting (EPS) method.

### 2.2. *Mimimum Mean Squared Error (MMSE) Related Works*

In [17], the authors surveyed the hybrid beamforming methods for the Massive MIMO communications in the context of a hybrid transceiver. This method also included an MMSE regularization for a hybrid precoding in the mmWave massive MIMO systems.

An MMSE MIMO-orthogonal frequency division multiplexing (OFDM) detector was proposed in [18] to balance an error performance and the spectral efficiency. It used maximum likelihood (ML), simple MMSE, and ordered successive interference cancellation (SIC) methods. This method was used in 5G CRN in massive MIMO to develop a secure transmission and to mitigate an interference and a peak-to-average power ratio.

In [19], the objective of an MMSE receiver was used to reduce the MSE of the estimated signal in contrast to the transmitted signal. The massive MIMO system performance was examined under the characteristics of a different linear receiver. A performance of an MMSE receiver in a realistic system was found in [20] under interference conditions.

In [21], an opportunistic transmission protocol (OTP) was examined according to the three types of beamforming techniques. One of the most perfect beamforming techniques is MMSE-SIC detection method. In this article, all the beamforming techniques and the OTPs were executed by the secondary user (SU) in a decentralized process.

Reference [22] proposed a transmit filter design using an MMSE approach to ensure a low complexity for a MIMO interference channel. The MMSE scheme combined the signal and the interference leakage of each transmitter.

Both a ZFBF scheme and the MMSE methods were used in [23]. In this article, a multi-user detection (MUD) method is examined in multicarrier-direct-sequence code-division multiple-access (MC DS-CDMA), which inspired a low complexity and a high flexibility. A scope of a low-complexity MUDs was derived based on the ZF, MMSE, and interference cancellation (IC) principles. The proposed MUD was implemented using a modular structure and most of the modules were independent of each other.

The proposed contribution contains the integration of a zero forcing and the MMSE technique, which are implemented in the desired signal vector. The proposed technique is also known as the regularized zero forcing method [24]. However, the proposed method power transmission is limited by the iterative solutions of the normalized mean square error method. This provides an enhanced solution in the secrecy rate when compared to the existing zero forcing technique. In the proposed method, the bit error rate (BER) and the secrecy outage probability (SOP) are greatly reduced. The throughput and the channel capacity are increased.

## 3. System Model

### 3.1. *Secure Beamforming in 5G-Based CRN*

Beamforming [24] is a fast and an accurate process that is properly focused on the target user equipment (UE). The process of beamforming is demonstrated Figure 1. The process, in which a UE has a rapid movement, is not an easy task. It is able to adapt the radiation model of an antenna to a certain structure. It steers a power in a specific direction toward a user. This is the actual process of beamforming, which is shown in Figure 2.

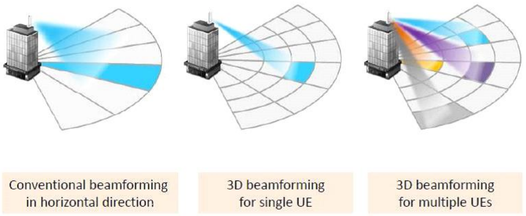

**Figure 1.** Beamforming of user qeipment (UE).

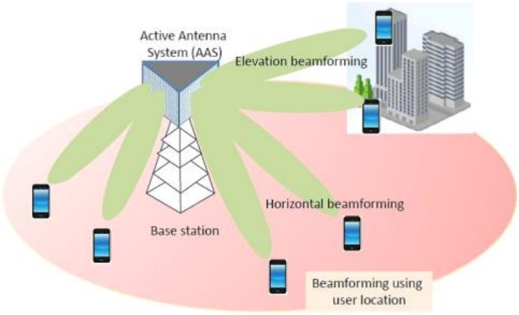

**Figure 2.** Beamforming toward a user.

Massive MIMO was examined as a part of beamforming. The CSI is a collection of spatial transfer functions between each antenna and a user terminal. The spatial information is found in the matrix (G), as shown in Figure 3.

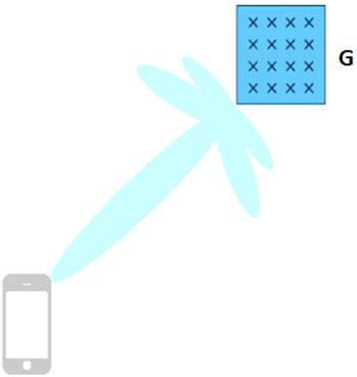

**Figure 3.** Traditional beamforming.

The research focuses on securing the CSI by aligning the signal matrix after applying the proposed method to reduce an interference in the channel matrix.

### 3.2. Proposed Beamformer

A cellular MIMO-NOMA-based CRN has two cells. Its BS with L clusters is shown in Figure 4 [12]. Each cluster has two users: One is the primary user (PU) and the other is a secondary user (SU). The BS and the two users of each cluster contains M and N antennas, respectively. Then, $c \in \{A,B\}$ indicates a cell and $l \in L \overset{\text{def}}{=} \{1, 2, \ldots, L\}$ represents the cluster, and $u \in \{pu, su\}$ denotes each user, respectively. The radius of a cell is $r_o$, in which the BS is situated at the center of an each cell. In this model, a cell is divided into two discs, namely $D_1$ and $D_{2.}$ They are the inner and outer discs in a cell. The D1 contains the radius of $r_i$ and $D_2$ contains the radius $r_o$, which lies within the circle of radius $r_i$. This model is easily extended for multi-cell framework [3] in any pairing order [25].

The channel gain of an u$^{th}$ users on a l$^{th}$ cluster of c$^{th}$ cell is given by [12],

$$G_u^{l,c} = \frac{F_u^{l,c}}{\sqrt{P\left(d_u^{l,c}\right)}} \tag{1}$$

where $F_u^{l,c}$ indicates a Rayleigh fading channel, which means $(\sigma_u^{l,c})^2$ is for variance calculations. For N x M dimensions, the channel gain matrices are given as $G_u^{l,c}$.

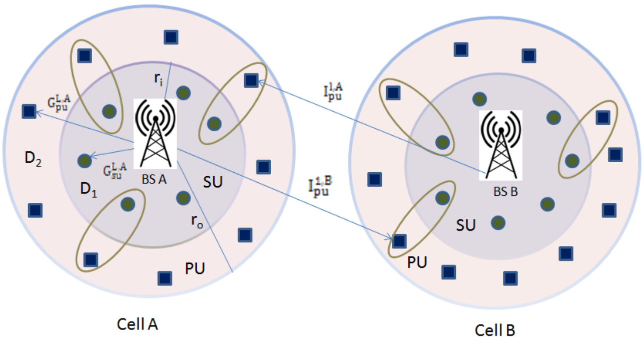

**Figure 4.** A two-cell network of multiple-input-multiple-output0non-orthogonal multiple access (MIMO-NOMA)-based cognitive radio network (CRN).

Let $P(d_u^{l,c}) = (d_u^{l,c})^{\upsilon}$ indicate a large-scale path loss and $\upsilon$ denote the path loss exponent. $d_u^{l,c}$ specifies the distance between the BS and a u$^{th}$ user. Likewise, the inter-cell channel-gain for the PU in the l$^{th}$ cluster of a c$^{th}$ cell is denoted by $I_{pu}^{l,c}$.

The licensed PUs need to be served first in the presence of a several SUs, but they are shared at the same time and frequency. The SU and the PU data in a cluster are retrieved using a SIC. The existing (L−1) clusters are denoted as an intruder in the fundamental clusters. In a multi-cell framework, all the PUs in a cell are specified as an intruder by another cell user. This does not occur in the case of SUs, which are within the same cell. This says that each of the clusters need to be secured from all other cell clusters, as well as in the PUs. This is solved by a proposed technique in the transmitter. The proposed technique consists of an incorporation of a ZFBF and an MMSE method. Nevertheless, the proposed technique implementation in the BS is not possible. This is because of the number of antennas in the BS is lesser than the entire number of antennas present in the clusters. This is also solved by a proposed technique.

### 3.3. Proposed Technique in Cascaded Transmission of MIMO-NOMA Network

The cascaded transmission of this approach is used in MIMO-NOMA-based CRN for the secure communication in the multi-cell framework. The intruders will make an attempt to secretly listen to the channel information. The BS does not want the intruders to prevent the data using receiving beamformers. The proposed technique is applied at the BS for the determination of an information leakage within the same and the adjacent cells. The received signal of the PU and the SU in the l$^{th}$ cluster of a cell A is expressed as [24]

$$R_{su}^{l,A} = G_{su}^{l,\,A} \sum_{m=1}^{L} v^{m,A} + w_{su}^{l,A} \tag{2}$$

$$R_{pu}^{l,A} = G_{pu}^{l,\,A} \sum_{m=1}^{L} v^{m,A} + I_{pu}^{l,A} \sum_{m=1}^{L} v^{m,\,B} + w_{pu}^{l,A} \tag{3}$$

Let $v^{l,\,A}$ be the $M \times 1$ superposition signal vector for the l$^{th}$ cluster of the cell A. Note that $v^{l,A} \in \mathbb{C}^{Mx1}$ is the transmitting pr oposed vector and $w_{pu}^{l,A}, w_{su}^{l,A}$ is the AWGN process. It will be present in the receiver side of the PU and SU of the l$^{th}$ cluster in the cell A. Assume $l \in L \overset{\text{def}}{=} \{1, 2, \ldots, L\}$.

The secrecy Rate of a PU and a SU is derived as

$$S_{su}^{l,A} \overset{\text{def}}{=} \left[ \log_2\!\left(1 + \psi\left|G_{su}^{l,A} v^{l,A}\right|^2\right) - \max_{m,m \neq l} \log_2\!\left(1 + \psi\left|G_{su}^{m,A} v^{m,A}\right|^2\right)\right]^+ \tag{4}$$

$$S_{pu}^{l,A} \overset{\text{def}}{=} \left[ \log_2\!\left(1 + \psi\left|G_{pu}^{l,A} v^{l,A}\right|^2\right) - Y_1 - Y_2\right]^+ \tag{5}$$

where ψ is the signal to noise ratio (SNR) transmission at the BS. The idea of $[e]^+$ is defined as max(0,e). $Y_1 \overset{\text{def}}{=} \max_{m,m\neq l} \log_2\left(1+\psi\left|G_{pu}^{m,A}v^{m,A}\right|^2\right)$ and $Y_2 \overset{\text{def}}{=} \max_{m} \log_2\left(1+\psi\left|I_{pu}^{m,A}v^{m,B}\right|^2\right)$. In Equations (4) and (5), the second term on the right hand side (RHS) contains the formulation of an information leakage for the l$^{\text{th}}$ cluster in the same cell. In Equation (5), the third term on the RHS contains the formulation of an information leakage for the l$^{\text{th}}$ cluster in the neighboring cell. The information leakage will be overcome by applying the proposed technique in the BS, by knowing that the BS has a CSI for all the users. The CSI is evaluated at the receiving end and it responds to the BS by a feedback channel.

Consider a proposed technique in the BS within the same cell without applying a signal alignment in the interfering channel matrix. A proposed technique is used to secure the data in every cluster within the same cell and in the neighboring cell. A proposed technique of $v^{l,A}$ needs to be designed at the BS as a non-trivial solution in Equation (6). A non-trivial solution will exist if M ≥ 2N (L−1). So, there must be a large number of antennas in the BS. The proposed method will serve as $\lfloor (M+1)/3 \rfloor$ in a multi-cell framework. This indicates that the number of antennas in the BS will be larger than the number of clusters. Therefore, this will reduce the overall throughput. This problem will be overcome by an alignment matrix $Q^A \in \mathbb{C}^{\text{MxS}}$. This will align the interference channel matrix in a cell for a different dimension. Then $v^{l,A} = Q^A V^{l,A}$ where $V^{l,A} \in \mathbb{C}^{\text{Sx1}}$ is a proposed vector for the l$^{\text{th}}$ cluster in a cell A. The BS will perform a precoding in an aligned interference channel matrix. The precoding must be in NxM dimensions for the better generation of a non-trivial solutions. So, there are no limitations in the number of antennas that is used in the BS. At the same time, the number of clusters is restricted by the antenna in the BS is also eliminated. The Equation (6) is derived by applying an alignment matrix $Q^A$. The area of an aligned channel matrix is 2N(L−1) × A, which is derived from the Equation (7). The 'S' value is nominated to get a non-trivial solution of an Equation (7). The alignment matrix $Q^A$ is constituted as $Q_2^A Q_1^A$ where $Q_2^A$ is initialized to align the interference channel matrix in a neighboring cell. Then, $Q_1^A$ is a proposed transmitting vector to overcome the data leakage in the neighboring cell. The proposed transmitting vector $Q_1^A$ for the neighboring cell will satisfy the following term as:

$$\left[G_{pu}^{1,A}\ G_{su}^{1,A}\ \ldots\ G_{pu}^{l-1,A}\ G_{su}^{l-1,A}\ G_{pu}^{l+1,A}\ G_{su}^{l+1,A}\ \ldots\ G_{pu}^{L,A}\ G_{su}^{L,A}\right]^G v^{l,A} = 0 \tag{6}$$

$$\left[G_{pu}^{1,A}Q^A\ G_{su}^{1,A}Q^A\ \ldots\ G_{pu}^{l-1,A}Q^A\ G_{su}^{l-1,A}Q^A\ G_{pu}^{l+1,A}Q^A\ G_{su}^{l+1,A}Q^A\ \ldots\ G_{pu}^{L,A}Q^A\ G_{su}^{L,A}Q^A\right]^G V^{l,A} = 0 \tag{7}$$

$$\left[H_{pu}^{1,B}Q_2^A\ H_{pu}^{2,B}Q_2^A\ \ldots\ H_{pu}^{L,B}Q_2^A\right]^T Q_1^A = 0 \tag{8}$$

where, $H_{pu}^{L,B}Q^A V^{l,A} \in \text{span}\left(H_{pu}^{L,B}\right) \forall\ Q^A V^{l,A}$

A non-trivial solution of $Q_1^A \in \mathbb{C}^{\text{PxS}}$, $Q_2^A \in \mathbb{C}^{\text{MxP}}$ is aligned with the interference channel matrix in a neighboring cell as P > NL for the Equation (8). The solution is given as [24]:

$$X_1^A = \text{span}\left\{\overline{H}^G\left(\overline{HH}^G + \beta I_d\right)^{-1}\overline{H}\right\} \tag{9}$$

where $\overline{H} \overset{\text{def}}{=} \left[H_{pu}^{1,B}Q_2^A\ H_{pu}^{2,B}Q_2^A\ \ldots\ H_{pu}^{L,B}Q_2^A\right]^T$. The condition of M>N is unrelated for a non-trivial solution of $Q_1^A$ in an Equation (9). The regularization term of $\beta$ contains a normalized mean square error (NMSE) method of an optimization that allows the balance between the noise covariance and the transmit power. Let $I_d$ be the identity matrix of NxM dimensions.

Let $V^{l,A}$ represent the determination of a non-trivial solutions for the Equation (7). Assuming $g_{pu}^{L,A} \overset{\text{def}}{=} G_{pu}^{L,A}Q^A$ and $g_{su}^{L,A} \overset{\text{def}}{=} G_{su}^{L,A}Q^A$ in Equation (7), Equation (10) is as follows:

$$\overline{G} \overset{\text{def}}{=} \left[g_{pu}^{1,A}\ g_{su}^{1,A}\ \ldots\ g_{pu}^{l-1,A}\ g_{su}^{l-1,A}\ g_{pu}^{l+1,A}\ g_{su}^{l+1,A}\ \ldots\ g_{pu}^{L,A}\ g_{su}^{L,A}\right]^T \tag{10}$$

Then, the solution is given as

$$\mathrm{V}^{\mathrm{l,A}} = \mathrm{span}\ \{\overline{\mathrm{G}}^{\mathrm{G}}(\overline{\mathrm{GG}}^{\mathrm{G}} + \beta\mathrm{I})^{-1}\overline{\mathrm{G}}\} \tag{11}$$

The MMSE method, along with the transmitting ZFBF approach, is spanned to obtain a proposed solution in the Equation (11). The regularization term of β contains a stability in the transmit power and a noise variance [24] which is denoted as $C_x$ and $C_v$. Then, the term β for a cell A is expressed as

$$\beta\mathrm{I} = \frac{\mathrm{C_x}}{\mathrm{MC_vS}}\mathrm{I} \tag{12}$$

Assume S be the data symbol that contains a $\mathrm{s}^{\mathrm{l,A}}_{\mathrm{pu}}$, $\mathrm{s}^{\mathrm{l,A}}_{\mathrm{su}}$ for the cluster l of cell A. Let $C_x$ be the transmit power and is expressed as [26],

$$\mathrm{C_x} = \mathrm{E}\Big[\omega\omega^{\mathrm{G}}\Big] \approx \left[\frac{1}{\mathrm{L}}\sum_{\mathrm{l}=1}^{\mathrm{L}}\omega_{\mathrm{l,u}}\omega^{\mathrm{G}}{}_{\mathrm{l,u}}\right] \odot \mathrm{I}_{\mathrm{d_{NxM}}} \tag{13}$$

Then, ω be the power allocation coefficient that contains a $\omega^{\mathrm{l,A}}_{\mathrm{pu}}$, $\omega^{\mathrm{l,A}}_{\mathrm{su}}$ for the PUs and the SUs and is assumed as $\omega^{\mathrm{l,A}}_{\mathrm{pu}} + \omega^{\mathrm{l,A}}_{\mathrm{su}} = 1$.

Let l be the number of clusters, ⊙ be the Hadamard product, and $\mathrm{I}_{\mathrm{d_{NxM}}}$ be the N×xM identity matrix. Equation (13) assumes that the signal source from different positions are uncorrelated. Let $C_v$ be the noise covariance matrix, expressed as

$$\mathrm{C_v} = \mathrm{E}\Big[\mathrm{ww}^{\mathrm{G}}\Big] \approx \sigma^2_{\mathrm{w}}\mathrm{I}_{\mathrm{d_{NxM}}} \tag{14}$$

where $\sigma^2_{\mathrm{w}}$ is a variance of the thermal noise and is assumed as additive white Gaussian noise (AWGN). The MMSE strikes the balance of obtaining a maximum signal amplification and then reducing the interference. This view that the signal processing complexity will help to obtain a good solution.

In the proposed method, the re-iteration of a transmit power $\mathrm{C_x}$ has taken place in the MMSE iterative solutions [26]. The iteration is declared through a data symbol.

$$\mathrm{C}_{\mathrm{x(s-1)}} = \left[\frac{1}{\mathrm{L}}\sum_{\mathrm{l}=1}^{\mathrm{L}}\omega_{\mathrm{l}}\omega^{\mathrm{G}}{}_{\mathrm{l}}\right] \odot \mathrm{I}_{\mathrm{d_{NxM}}} \tag{15}$$

The iteration has been terminated by the NMSE solutions and is expressed as [26]

$$\mathrm{C_x}\Big|\mathrm{C}_{\mathrm{x(s-1)}} = \vartheta_{\mathrm{s}} = \frac{1}{\mathrm{u}}\sum_{\mathrm{u=pu}}^{\mathrm{su}}\left[\frac{\sum_{\mathrm{l}=1}^{\mathrm{L}}||\hat{\omega}^{(\mathrm{s})}_{\mathrm{l,u}} - \hat{\omega}^{(\mathrm{s}-1)}_{\mathrm{l,u}}||^2}{\sum_{\mathrm{l}=1}^{\mathrm{L}}||\hat{\omega}^{(\mathrm{s}-1)}_{\mathrm{l,u}}||^2}\right] \odot \mathrm{I}_{\mathrm{d_{NxM}}} \tag{16}$$

So, instead of the Equation (13), we apply an iterated transmitted power [26] as shown in the above Equation (16) for the better MMSE solutions. Therefore, the proposed technique obtains an enhanced solution compared with the existing method.

The above proposed solution is situated at the BS and the derivation for the secrecy rate is calculated as follows [12]:

$$\mathrm{S}^{\mathrm{l,A}}_{\mathrm{su}} \overset{\mathrm{def}}{=} \log_2\Big(1 + \psi\Big|\mathrm{G}^{\mathrm{l,A}}_{\mathrm{su}}\mathrm{v}^{\mathrm{l,A}}\Big|^2\Big) \tag{17}$$

$$\mathrm{S}^{\mathrm{l,A}}_{\mathrm{pu}} \overset{\mathrm{def}}{=} \log_2\Big(1 + \psi\Big|\mathrm{G}^{\mathrm{l,A}}_{\mathrm{pu}}\mathrm{v}^{\mathrm{l,A}}\Big|^2\Big) \tag{18}$$

The total secrecy rate in a cluster is given by

$$\mathrm{S}_{\mathrm{total}}^{\mathrm{l,A}} = \mathrm{S}_{\mathrm{pu}}^{\mathrm{l,A}} + \mathrm{S}_{\mathrm{su}}^{\mathrm{l,A}} \tag{19}$$

The proposed method in an Equation (16) will convert a total secrecy rate of a cluster to the total throughput of a cluster.

The BER from the above formulation is calculated as

$$\mathrm{BER}_{\mathrm{u}} = \frac{1}{2}\mathrm{Q}\left(\frac{2*\mathrm{E}\left[\left|\mathrm{v}^{\mathrm{l,\ A}}\right|\right]^{2}}{\mathrm{w}_{\mathrm{u}}^{\mathrm{l,A}}}\right)$$

where Q (.) is the Gaussian Q-function and is defined as

$$Q(W) = \frac{1}{2\pi}\int_{w}^{\infty} e^{-\frac{z^2}{2}} dz$$

The channel capacity is also greatly increased by the proposed method and is formulated as

$$C_u = ChB * log_2\left(1 + \frac{\mathrm{v}^{\mathrm{l,\ A}}}{\mathrm{w}_{\mathrm{u}}^{\mathrm{l,A}}\mathrm{ChB}}\right)$$

where B is the channel bandwidth, which is taken at 1 MHz.

The throughput of the channel can be expressed as

$$T_u = \psi\left[\left|\mathrm{G}_{\mathrm{u}}^{\mathrm{l,A}}\mathrm{v}^{\mathrm{l,\ A}}\right|\right]^2$$

The proposed technique is skillful in allocating the multi-cells and multi-clusters in which the number of antennas is not limited at the BS.

### 3.4. Secrecy Outage Probability

The secrecy outage probability of the PU and the SU in a cluster was analyzed in consent with the CR power allocation policy. This says that the PU permits the SU to reuse the spectrum by assuring a PUs quality of service. The PU will obtain a target data rate of $\mathrm{D}_{\mathrm{pu}}^{\mathrm{l,\ A}}$ by modifying the power allocation coefficient of $\omega_{pu}^{l,A}$. Then, the limitation is given by

$$\frac{\psi\left|\mathrm{G}_{\mathrm{pu}}^{\mathrm{l,A}}\mathrm{v}^{\mathrm{l,A}}\right|^2\omega_{\mathrm{pu}}^{\mathrm{l,A}}}{\psi\left|\mathrm{G}_{\mathrm{pu}}^{\mathrm{l,A}}\mathrm{v}^{\mathrm{l,A}}\right|^2\omega_{\mathrm{su}}^{\mathrm{l,A}} + 1} > \varepsilon_{\mathrm{pu}}^{\mathrm{l,A}} \tag{20}$$

where $\varepsilon_{\mathrm{pu}}^{\mathrm{l,A}} = 2^{\mathrm{D}_{\mathrm{pu}}^{\mathrm{l,\ A}}} - 1$. This gives a following alternative as

$$\omega_{\mathrm{su}}^{\mathrm{l,A}} = \max(0, \frac{\psi\left|\mathrm{G}_{\mathrm{pu}}^{\mathrm{l,A}}\mathrm{v}^{\mathrm{l,A}}\right|^2 - \varepsilon_{\mathrm{pu}}^{\mathrm{l,A}}}{(1+\varepsilon_{\mathrm{pu}}^{\mathrm{l,A}})\psi\left|\mathrm{G}_{\mathrm{pu}}^{\mathrm{l,A}}\mathrm{v}^{\mathrm{l,A}}\right|^2}) \tag{21}$$

The target data rate is not achieved, even when the full power is assigned to it. Thus, the secrecy outage probability of the PU and the SU is implied as follows:

$$\mathrm{SOP}_{\mathrm{pu}}^{\mathrm{l,A}} \overset{\mathrm{def}}{=} \mathrm{Pr}\left[\log_2\left(1 + \psi\left|\mathrm{G}_{\mathrm{pu}}^{\mathrm{l,A}}\mathrm{v}^{\mathrm{l,A}}\right|^2\right) < \mathrm{D}_{\mathrm{pu}}^{\mathrm{l,\ A}}\right] \tag{22}$$

$$\mathrm{SOP}_{\mathrm{su}}^{\mathrm{l,A}} \overset{\mathrm{def}}{=} \mathrm{Pr}\left[\log_2\left(1 + \psi\left|\mathrm{G}_{\mathrm{su}}^{\mathrm{l,A}}\mathrm{v}^{\mathrm{l,A}}\right|^2\right) < \mathrm{D}_{\mathrm{su}}^{\mathrm{l,\ A}}\right] \tag{23}$$

Let the asymptotic expression of channel gain and proposed vector will be taken as

$$\left|\mathrm{G}_{\mathrm{pu}}^{\mathrm{l,A}}\mathrm{v}^{\mathrm{l,A}}\right|^2 \sim \Gamma(N(S-1),\ (\sigma_{pu}^{l,A})^2) \tag{24}$$

$$\left|\mathrm{G}_{\mathrm{su}}^{\mathrm{l,A}}\mathrm{v}^{\mathrm{l,A}}\right|^2 \sim \Gamma(N(S-1),\ (\sigma_{su}^{l,A})^2) \tag{25}$$

Then, applying the gamma function in the above assumption is given [12] as

$$\frac{1}{\Gamma(N(S-1))}\gamma\left(N(S-1),\ \frac{J_3}{(\sigma_{pu}^{k,A})^2}\right) \approx \frac{1}{\Gamma q}\left(\frac{r}{\psi}\right)^q \sum_{f=1}^{6} \theta_f \varnothing_f \tag{26}$$

Let $q \sim \Gamma(N(S-1))$ and $r \sim \frac{J_3}{(\sigma_{pu}^{l,A})^2}$, where $\gamma(q,\ r) \overset{\text{def}}{=} \int_0^r \varphi^{q-1}\exp(-\varphi)d\varphi$ denotes the lower incomplete gamma function as $\varphi = \frac{fr}{6\psi}$ and $\theta_f = \left(\frac{i}{6}\right)^{a-1}$, $\varnothing_f = e^{\frac{fr}{6\psi}}$. The asymptotic expression of Equation (12) is obtained by applying the Simpson's 1/3 numerical integration method [12]. Here, $J_3 \overset{\text{def}}{=} \frac{\varepsilon_{pu}^{l,A}}{\psi\omega_{pu}^{l,A}}$ and $\left|G_{\mathrm{pu}}^{l,A}v^{l,A}\right|^2 \overset{\text{def}}{=} Z \sim (N(S-1),\ (\sigma_{pu}^{l,A})^2)$. The secrecy outage at PU is same as the conventional orthogonal multiple-access systems [5]. Then, the secrecy outage at SU is found in three different scenarios as: Event $T_1$ for $\omega_{su}^{k,A} = 0$, Event $T_2$ for $\omega_{su}^{l,A} > 0$ where the SU is unable to decode the message for both the PU and the SU [5], and Event $T_3$ for $\omega_{su}^{l,A} > 0$ where the SU is unable to decode its own message but it is able to decode the message for PU [5]. The probability of a $T_1$ is expressed as

$$P(T_1) = P[\psi Z - \varepsilon_{pu}^{l,A} < 0] \approx \frac{1}{\Gamma q}\left(\frac{r}{\psi}\right)^q \sum_{f=1}^{6} \theta_f \varnothing_f \tag{27}$$

The probability of $T_2$ is found as $P(T_2) = 0$. Then, the probability of $T_3$ is calculated as [12]

$$P(T_3) = P\left[X\frac{\psi Z - \varepsilon_{pu}^{l,A}}{\left(1+\varepsilon_{pu}^{l,A}\right)Z} < \varepsilon_{su}^{l,A},\ Z > \frac{\varepsilon_{pu}^{l,A}}{\psi}\right] \tag{28}$$

where $D_{su}^{k,A}$ is the target data rate of SU and $\varepsilon_{su}^{l,A} \overset{\text{def}}{=} D_{su}^{l,A} - 1$ and $\left|\mathrm{G}_{\mathrm{su}}^{\mathrm{l,A}}\mathrm{v}^{\mathrm{l,A}}\right|^2 \overset{\text{def}}{=} X \sim \psi\Gamma(N(S-1), (\sigma_{su}^{l,A})^2)$. Then, P($E_3$) [12] will be

$$P(T_3) = \int_0^{\infty}\int_{\frac{\varepsilon_{pu}^{l,A}}{\psi}}^{J_4} f_Z(z)f_X(x)dzdx \tag{29}$$

where, $J_4 \overset{\text{def}}{=} \frac{\varepsilon_{su}^{l,A}\left(1+\varepsilon_{pu}^{l,A}\right)x}{y\psi - \varepsilon_{pu}^{l,A}}$. Combining P($E_1$), P($E_2$), and P($E_3$), one can obtain the asymptotic expression for the secrecy outage probability of SU as in [12] as

$$SOP_{su}^{k,A} \approx \frac{1}{\Gamma q}\left(\frac{r}{\psi}\right)^q \sum_{f=1}^{6} \theta_i \varnothing_i + \left(\frac{\varepsilon_{pu}^{k,A}}{\psi}\right)^q \left[1 + \frac{J_5}{\psi}\right] \tag{30}$$

where

$$J_5 = \left(\varepsilon_{su}^{k,A}\left(1+\varepsilon_{pu}^{k,A}\right)\left(\sigma_{pu}^{k,A}\right)^2\right)\left(\sigma_{pu}^{k,A}\right)^{2(q-1)}\Gamma q \tag{31}$$

The above equation was taken from the reference [12] and was applied here to obtain the analytical solutions for both the PU and the SUs. The asymptotic outage performance of the PU and the SU is shown in the simulation results.

## 4. Numerical Evaluation

The numerical rating of the proposed method was conducted in this section and the results were compared with the existing cascaded ZFBF techniques [12]. A proposed technique has a greater performance than the existing technique. The simulation parameter, which is used in the proposed technique, is shown in Table 1.

**Table 1.** Simulation parameters.

| Parameter | Value |
|---|---|
| Network Size | $200 \times 200$ m$^2$ |
| Channel Bandwidth | 1 MHz |
| Rayleigh fading channel, $\sigma_u^2$ | 0.8 |
| Path-loss exponent, $\upsilon$ | 3 |
| Radius of inner disc, $\mathrm{r_i}$ | 10 |
| Radius of outer disc, $\mathrm{r_o}$ | 20 |
| Data rate for PU, $\mathrm{D_{pu}^{l,\,A}}$ | 0.25, 1 |
| Data rate for SU, $\mathrm{D_{su}^{l,\,A}}$ | 1, 4 |
| Number of antennas for BS, M | 2 |
| Number of antennas for user, N | 2 |
| Number of clusters of each cell, L | 4 |
| Number of cells, C | 2 |
| Number of bits/symbols, $\mathrm{B_i}$ | $10^6$ bits |

This article was implemented using the software named 'Matlab' (The MathWorks, Inc., Natick, MA, USA) of version R2017b in the platform of 64-bit version in the x86 instruction set.

In Figure 5, the secrecy rate of the PU and the SU is plotted to the transmitting SNR. The proposed method was also compared with the existing method of coordinated beamforming (CoBF) technique [3] and the cascading ZFBF techniques [12], respectively. The secrecy rate of the proposed method is increased with the SNR and its performances are higher than the existing methods. The CoBF technique is implemented in both the transmitting and receiving beamformers. The interference channel matrix is aligned by the transmitting beamforming technique and nullified by the receiving beamformer. Likewise, the cascaded ZFBF technique performs better than the CoBF technique [3], but the proposed performance provides a better result compared with the cascaded ZFBF method [12]. Nevertheless, an eavesdropper obstructs the interference in which the receiving beamformer is not used. The interference alignment and the proposed method are applied at the BS. Therefore, the secrecy rate increases with the SNR.

The secrecy outage probability for the PU and the SU estimates for the different target data rate as, $\mathrm{D_{pu}^{l,\,A}}$ and $\mathrm{D_{su}^{l,\,A}}$. Then, the secrecy outage probability of the SU is $\mathrm{SOP_{su}^{l,A}}$, which is higher than the secrecy outage probability of the PU as, $\mathrm{SOP_{pu}^{l,A}}$. The probability of the secrecy outage will be increased, as the target data rate has a larger value.

The output results, which are shown in Figures 5–9, respectively, show the effectiveness of the proposed method.

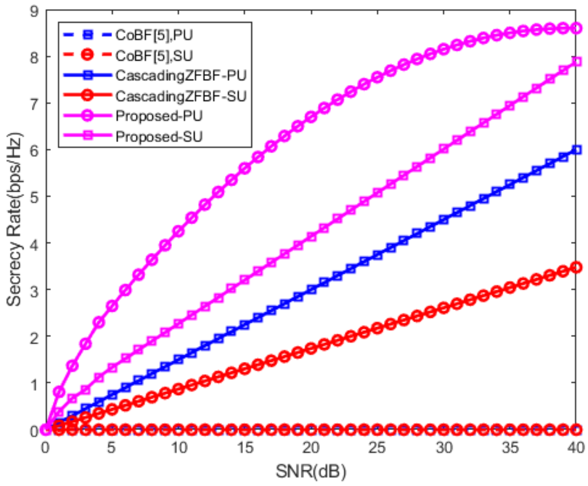

**Figure 5.** Secrecy rate.

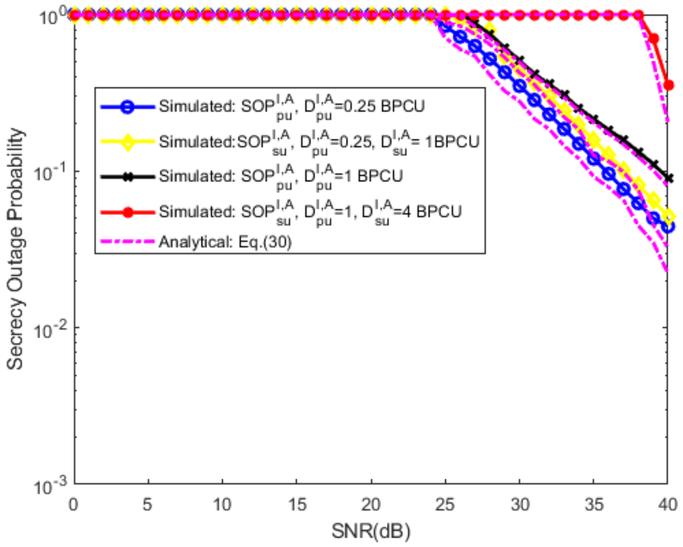

**Figure 6.** Secrecy outage probability.

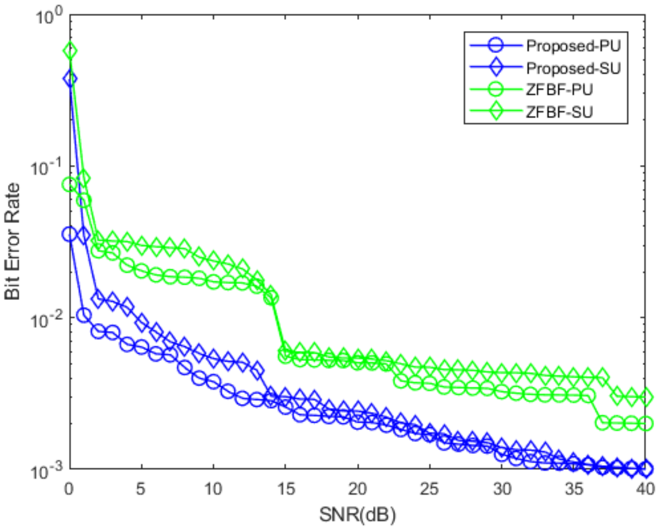

**Figure 7.** Bit error rate of the ZFBF and the proposed technique.

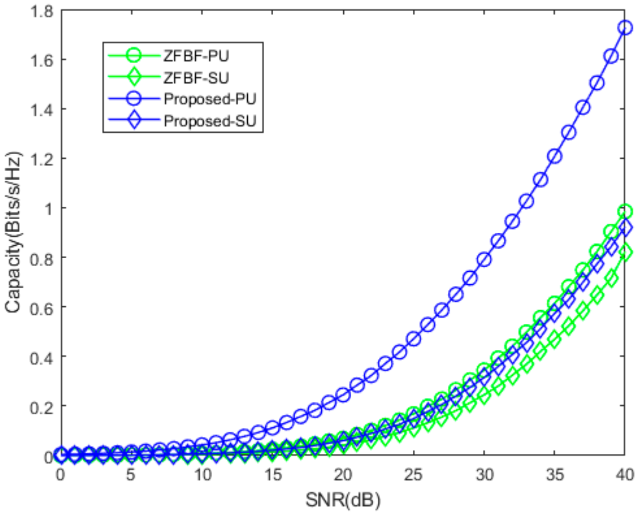

**Figure 8.** Channel capacity of zero forcing beamforming (ZFBF) and the proposed technique.

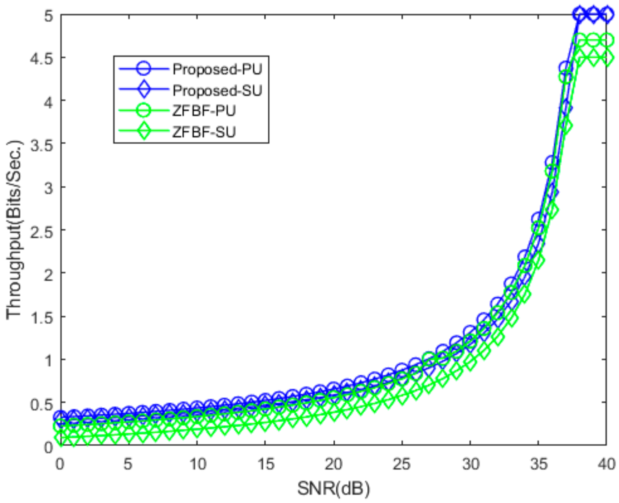

**Figure 9.** Throughput of the ZFBF and the proposed technique.

## 5. Motivation and Contribution of the Article

This article clearly described the proposed technique, which is one of the best beamforming techniques to reduce the interference in the MIMO-NOMA-based CRN. The MMSE method, along with the NMSE iterations, were used to limit the power transmission for the better exposure of the proposed performance. The number of antennas at the BS was not limited because the signal alignment matrix was used at the BS to align the channel matrix. The motivation of an article was to enhance the secure transmission of the data packets by reducing the interference as effectively as possible. The simulation results show the effectiveness of the proposed technique.

## 6. Discussion

This article shows the highlighted secrecy rate and effectively reduces the outage probability compared with the previous results [12]. The proposed technique in the article was used in securing the beamforming in the 5G technology without causing interference during a data transmission between a cluster from one cell to another cell. The findings of the proposed method are oriented to the MMSE technique, which belongs to one of the beamforming techniques in the MIMO. Here, the proposed MMSE iterative technique was used to enhance the secrecy rate by cancelling the interference as possible.

The proposed method normally uses the technique that is oriented to MMSE will enhance the total secrecy rate of the system than the preceding method of the ZFBF [12]. The SOP and BER were also reduced. The capacity and throughput were significantly increased in the proposed method, which is shown in Simulation results. Therefore, this new beamforming technique shows the performance of their robustness, which may be used in another part of technology, like Internet of Things (IoT)-based CRN, to secure the communication as possible.

## 7. Conclusions

In this paper, a downlink beamforming technique was proposed for the secure communication in a two-cell MIMO-NOMA-based CRN. There were no other limitations for the number of antennas at the BS. This was achieved by the signal alignment matrix that aligns the interference channel matrix, before the implementation of the proposed method. The proposed technique is very effective in enlarging the total secrecy rate of the CRN systems.

For the future work, the proposed method may be used in IoT-based cognitive radio networks. The IoT users in the CRN are sensed as per the RF spectrum slot to give the logistic and disaster response. So, there is a need for the accurate spectrum decision framework in 5G engineering.

The spectrum decision, which is taken by an unlicensed SUs of a CRN, holds an important role in CR-based IoT in 5G network. The proposed method can be very useful for taking the optimistic spectrum decision in IoT-based cognitive radio networks.

**Author Contributions:** Conceptualization, H.S.M.A.; methodology, H.S.M.A.; formal analysis, H.S.M.A. and T.L.; investigation, H.S.M.A. and T.L.; data curation, H.S.M.A.; writing-original draft preparation, H.S.M.A.; writing-review and editing, H.S.M.A. and T.L.; software, H.S.M.A. and T.L.; supervision, T.L.; project administration, H.S.M.A. and T.L.

**Funding:** This research received no external funding.

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

## Abbreviations

| | |
|---|---|
| CRN | cognitive radio network |
| NOMA | non-orthogonal multiple access |
| MIMO | multiple-input-multiple-output |
| 5G | fifth generation |
| SUs | secondary users |
| PUs | primary users |
| SC | subcarrier |
| CJ | cooperative jamming |
| SSPA | smart sensor protocol algorithm |
| PLS | physical layer security |
| ZFBF | zero forcing beamforming |
| BF | beamforming |
| CSTN | cognitive satellite terrestrial network |
| SDA | software defined architecture |
| MISOME-SWIPT | multiple input, single output multiple-eavesdropper simultaneous wireless information and power transferring |
| SEE | secrecy energy efficiency |
| CSI | channel state information |
| UPA | uniform planar array |
| BS | base station |
| AoA | angle of arrival |
| Eves | eavesdropper |

| | |
|---|---|
| SR | secrecy rate |
| IPF | iterative penalty function |
| MISO | multi-input single-output |
| ST | secondary transmitter |
| SR | secondary receiver |
| PS | power splitting |
| SDR | software defined radio |
| PSO | particle swarm optimization |
| EPS | equal power splitting |
| MMSE | minimum mean square error |
| NMSE | normalized mean square error |
| ML | maximum likelihood |
| SIC | successive interference cancellation |
| OTP | opportunistic transmission protocol |
| MUD | multiuser detection |
| MC DS-CDMA | multicarrier direct-sequence code-division multiple access |
| IC | interference cancellation |
| UE | user equipment |
| AWGN | additive white Gaussian noise |
| CoBF | coordinated beamforming |
| SNR | signal to noise ratio |
| RF | radio frequency |
| IoT | Internet of Things |
| SOP | secrecy outage probability |

## References

1. Zeng, M.; Yadav, A.; Dobre, O.A.; Tsiropoulos, G.I.; Poor, H.V. Capacity comparison between MIMO-NOMA and MIMO-OMA with multiple users in a cluster. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 2413–2424. [CrossRef]
2. Islam, S.M.R.; Zeng, M.; Dobre, O.A.; Kwak, K.S. Resource allocation for downlink NOMA systems: Key techniques and open issues. *IEEE Wirel. Commun.* **2018**, *25*, 40–47. [CrossRef]
3. Shin, W.; Vaezi, M.; Lee, B.; Love, D.J.; Lee, J.; Poor, H.V. Coordinated beamforming for multi-cell MIMO-NOMA. *IEEE Commun. Lett.* **2017**, *21*, 84–87. [CrossRef]
4. Ding, Z.; Adachi, F.; Poor, H.V. The application of MIMO to nonorthogonal multiple access. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 537–552. [CrossRef]
5. Ding, Z.; Schober, R.; Poor, H.V. A general MIMO framework for NOMA downlink and uplink transmission based on signal alignment. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 4438–4454. [CrossRef]
6. Xu, L.; Nallanathan, A.; Pan, X.; Yang, J.; Liao, W. Security-Aware Resource Allocation with Delay Constraint for NOMA-Based Cognitive Radio Network. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 366–376. [CrossRef]
7. Duan, W.; Jiang, X.Q.; Wen, M.; Wang, J.; Zhang, G. Two-Stage Superposed Transmission for Cooperative Noma Systems. *IEEE Access* **2018**, *6*, 3920–3931. [CrossRef]
8. Liu, Y.; Qin, Z.; Elkashlan, M.; Gao, Y.; Hanzo, L. Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 1656–1672. [CrossRef]
9. Jiang, M.; Li, Y.; Zhang, Q.; Li, Q.; Qin, J. Secure beamforming in downlink MIMO nonorthogonal multiple access networks. *IEEE Signal Process. Lett.* **2017**, *24*, 1852–1856. [CrossRef]
10. Zhang, H.; Yang, N.; Long, K.; Pan, M.; Karagiannidis, G.K.; Leung, V.C. Secure Communications in NOMA System: Subcarrier Assignment and Power Allocation. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 1441–1452. [CrossRef]
11. Chen, J.; Yang, L.; Alouini, M.S. Physical layer security for cooperative NOMA systems. *IEEE Trans. Veh. Technol.* **2018**, *67*, 4645–4649. [CrossRef]
12. Nibedita, N.; Sudhan, M.; Hsiao-Chun, W. Secure Beamforming for MIMO-NOMA Based Cognitive Radio Network. *IEEE Commun. Lett.* **2018**, *22*, 1708–1711.
13. Lin, M.; Lin, Z.; Zhu, W.P.; Wang, J.B. Joint Beamforming for Secure Communication in Cognitive Satellite Terrestrial Networks. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 1017–1029. [CrossRef]

14. Dong, Y.; Hossaini, M.J.; Cheng, J.; Leung, V.C. Robust Energy Efficient Beamforming in MISOME-SWIPT Systems with Proportional Secrecy Rate. *IEEE J. Sel. Areas Commun.* **2018**, *37*, 202–215. [CrossRef]
15. Lin, Z.; Lin, M.; Wang, J.B.; Huang, Y.; Zhu, W.P. Robust Secure Beamforming for 5G Cellular Networks Coexisting with Satellite Networks. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 932–945. [CrossRef]
16. Pham, V.T.; Koo, I. Optimal Multiuser MISO Beamforming for Power-Splitting SWIPT Cognitive Radio Networks. *IEEE Access* **2017**, *5*, 14141–14153.
17. Irfan, A.; Hedi, K.; Adnan, S.; Ahmed, M.; Kwang, S.K.; Eli De, P.; Ingrid, M. A Survey on Hybrid Beamforming Techniques in 5G: Architecture and System Model Perspectives. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3060–3097.
18. Deepanramkumar, P.; Karuppiah, M.; Hafizul, I.S.K.; Mohammad, S.O. Secure cognitive radio-based synchronized transmission of 5G signals using massive MIMO-OFDM-ES. *Int. J. Commun. Syst.* **2018**, *31*, e3805.
19. Ehab, A.; Mahamod, I.; Rosdiadee, N.; Nor, F.A. Beamforming techniques for massive MIMO systems in 5G: Overview, classification, and trends for future research. *Front. Inf. Technol. Electron. Eng.* **2017**, *18*, 753–772.
20. Ju, M.; Qian, J.; Li, Y.; Tan, G.; Li, X. Comparison of multiuser MIMO systems with MF, ZF and MMSE receivers. In Proceedings of the IEEE Third International Conference on Information Science and Technology (ICIST), Yangzhou, China, 23–25 March 2013.
21. Lin, H.; Shin, W.Y. Non-Orthogonal Random Access in MIMO Cognitive Radio Networks: Beamforming, Power Allocation, and Opportunistic Transmission. *PLoS ONE* **2017**, *12*, e0169902. [CrossRef]
22. Sun, F.; de Elisabeth, C. Leakage-Based MMSE Beamforming Design for a MIMO Interference Channel. *IEEE Signal Process. Lett.* **2012**, *19*, 368–371. [CrossRef]
23. Yang, L.L.; Wang, L.C. Zero-Forcing and Minimum Mean-Square Error Multiuser Detection in Generalized Multicarrier DS-CDMA Systems for Cognitive Radio. *EURASIP J. Wirel. Commun. Netw.* **2008**, *2008*, 541410. [CrossRef]
24. Masterson, C. Massive MIMO and Beamforming: The Signal Processing Behind the 5G Buzzwords. *Analog Dialogue* **2017**, *51*, 10.
25. Yang, Z.; Ding, Z.; Fan, P.; Al-Dhahir, N. A general power allocation scheme to guarantee quality of service in downlink and uplink NOMA systems. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 7244–7257. [CrossRef]
26. Eiichi, Y.; Tomoo, U.; Zen, K.; Satoru, Y.; Takeshi, M.; Fumihiko, M.; Masakazu, W. MMSE Beam Forming on Fast-Scanning Phased Array Weather Radar. *IEEE Trans. Geosci. Remote Sens.* **2013**, *51*, 3077–3088.