AASCIT Communications
Volume 5, Issue 1
ISSN: 2375-3803

AASCIT American Association for Science and Technology

Secure Massive MIMO Transmission for Cognitive Radio Networks

Hefdhallah Sakran Department of Electrical Engineering, IBB University, Yemen

Azzam Al-nahari Department of Electrical Engineering, IBB University, Yemen

Faisal Al-kamali Department of Electrical Engineering, IBB University, Yemen

Sami Tarbosh Department of Electrical Engineering, IBB University, Yemen

Received: January 16, 2018; **Accepted**: February 18, 2018; **Published**: March 14, 2018

Keywords

Cognitive Radio, Massive MIMO, Achievable Secrecy Rate, Secrecy Outage Probability

In this paper, we consider the problem of physical layer security in Cognitive Radio Networks (CRNs), where a Secondary User Transmitter (SU-Tx) sends confidential messages to a Secondary User Receiver (SU-Rx) on the same frequency band of a primary user (PU) in the presence of a multiple antennas Eavesdropper. Massive Multiple Input Multiple Output (M-MIMO) technology is considered a key technology for next generation wireless systems, which provide higher rates and improve the reliability through diversity gains and spectrum efficiencies. We consider the effect of M-MIMO in improving the physical layer security in the presence of multiple antennas eavesdropper in CRNs, which has not yet been clarified. The Channel State Information (CSI) of the SU-Rx is assumed to be available at the transmitter side, whereas the CSI of the eavesdropper is assumed not known. It is found that M-MIMO is able to combat passive eavesdropping. Moreover, in order to investigate the effect of active eavesdropping on the secrecy performance of CRNs, the secrecy rate and the secrecy outage probability of this case is studied. The effects of some parameters such as the transmitted power at SU-Tx, interference temperature limit, and number of PUs are studied.

Introduction

There is an exceptional increase in the usage of wireless devices and continuous increasing demand for wireless applications in the last decade. However, most of the frequency spectrum has already been licensed exclusively to operators by government agencies, such as Federal Communications Commission (FCC). Therefore, spectrum scarcity is one of the most important challenges that the industrial community is facing, due to the increasing demand for the spectrum. Different studies reported that many portions of the spectrum are inefficiently utilized for significant periods of time. The spectral efficiency can be as low as 15% [1, 2]. Recently, CRNs [3, 4] have attracted much attention as a solution for spectrum scarcity, allowing cognitive users (unlicensed users) to coexist with the licensed primary users (PUs) and transmit in the same band, as long as the interference at the primary receivers does not go beyond a certain threshold [5].

The security is an important issue for CRNs and one of the challenges that face next generation services. The problem of secure transmission in the presence of an eavesdropper using an information-theoretic principles was first studied in [6]. In this work, the authors showed that the secure communication is possible without sharing a secret key if the eavesdropper's channel is a degraded version of the main channel (the communication channel between the legitimate users). Information-theoretic physical layer security in CRNs was investigated in [7-10]. Achieving secure transmission using multiple antennas, in which the Secondary User Transmitter (SU-Tx) sends confidential information to Secondary User Receiver (SU-Rx) in the presence of a PU receiver (PU-Rx) and at the same time an eavesdropper receiver (ED-Rx), trying to eavesdrop this information, was addressed in [7-8]. In contrast to [7] and [8] which assumed the perfect CSI knowledge, the authors in [9] proposed robust transmitter design for the secure multiple-input single-output (MISO) CRNs with imperfect CSI. In [10], the authors proposed

a relay selection scheme in CR networks, where the considered scheme selects a trusted decode and forward relay to assist SUs and maximize the secrecy capacity that is subjected to the interference power threshold at the PUs. The authors in [11] studied the relay precoding scheme to improve the secrecy capacity of SUs in CR systems. The problem of Primary User Emulation (PUE) attacks was investigated in [12]. The authors in [13] proposed a relay selection scheme, which jointly considers the best relay selection and dynamic power allocation in order to maximize SC and to minimize energy consumption. In [14], the authors used the SUs' interference to improve the PU's secrecy capacity by decreasing the capacity of the source-eavesdropper channel more than that of the source-destination channel.

M-MIMO has recently merged as a key technology for fifth generation (5G) wireless systems, where a very high user data rates is required [15, 16]. In [17], the authors considered secure downlink transmission in a multi-cell massive multiple-input multiple-output (M-MIMO) system, where the numbers of base station (BS) antennas, mobile terminals, and eavesdropper antennas are asymptotically large. In [18], the authors investigated the potential benefits of the M-MIMO enabled heterogeneous cloud radio access network in terms of the secrecy and energy efficiency. The effect of Ma-MIMO systems on the secrecy performance in the presence of multi-antenna eavesdropper was investigated in [19]. To the best of our knowledge, applying the M-MIMO in physical layer security for CRNs has not been studied until now, which is the main objective of this paper.

In this paper, we examine the M-MIMO for physical layer security in CRNs, in the presence of multiple PUs and multi-antenna eavesdropper that tries to extract information intended for the SU-Rx. In this network setup, the interference power at the PU from the SU-Tx must not exceed a certain interference power threshold. We consider two types of the eavesdroppers: passive eavesdropper that overhears the SU transmit signal but does not transmit any signal, and active eavesdropper (malicious user) that attacks the training phase of the transmission. The CSI of the eavesdropper at the SU-Tx is assumed unknown for all cases.

The remainder of this paper is organized as follows. In Section 2, the system model is introduced. The secrecy rate in the case of passive eavesdropping is presented in Section 3. In section 4, the secrecy rate in case of active eavesdropping is investigated. Section 5 presents the simulation results. Section 6 gives the concluding remarks.

Notation: $(.)^T$ and $(.)^H$ denote transpose and Hermitian transpose operations, respectively. $X \sim \mathcal{CN}(\mu, N_0)$ represents a circularly symmetric Gaussian random vector with mean μ and variance N_0. Moreover, $[x]^+ \triangleq \max(0, x)$.

System and Channel Models

We consider a CRN as shown in Figure 1. The secondary network consists of a SU-Tx and SU-Rx. The primary network consists of *L* PUs. Moreover, it is assumed that an eavesdropper, equipped with *N* antennas is trying to overhear and decode the information transmitted from the SU-Tx to the SU-Rx. The SU-Tx is equipped with an array of *M*-antennas and the SU-Rx with single antenna. The SU-Tx transmits confidential data to the SU-Rx in the presence of PU. The transmission channels between the four terminals experience both types of fading, small-scale and large-scale fading.

We model the transmission channel between the SU-Tx and SU-Rx as $\sqrt{\beta_{SD}}\mathbf{h}_{SD}$, where β_{SD} represents the large-scale fading between SU-Tx and SU-Rx, and $\mathbf{h}_{SD}$ is an 1×M vector, representing the channel gains between SU-Tx and SU-Rx. Similarly, the channel between the SU-Tx and the eavesdropper is given by $\sqrt{\beta_{SE}}\mathbf{H}_{SE}$ where $\mathbf{H}_{SE}$ is an N ×M matrix, which represents the fading channel matrix between SU-Tx and the eavesdropper. The eavesdropper decode the received signal using Antenna Selection (AS), which select the antenna to maximize the channel Signal-to-Noise Ratio (SNR). Also, the channel between SU-Tx and the PU is given by $\sqrt{\beta_{SP}}\mathbf{H}_{SP}$, where $\mathbf{H}_{SP}$ is an K×M matrix, representing the channel matrix between SU-Tx and the PUs, where *K* is the number of PU. A fully reciprocal time division duplexing system is assumed. As a result it is assumed that $\mathbf{h}_{SD} = \mathbf{h}_{DS}^T$. For beamforming in the downlink, SU-Rx transmits a pilot symbol x_p to SU-Tx so that the downlink channel can be estimated at SU-Tx.

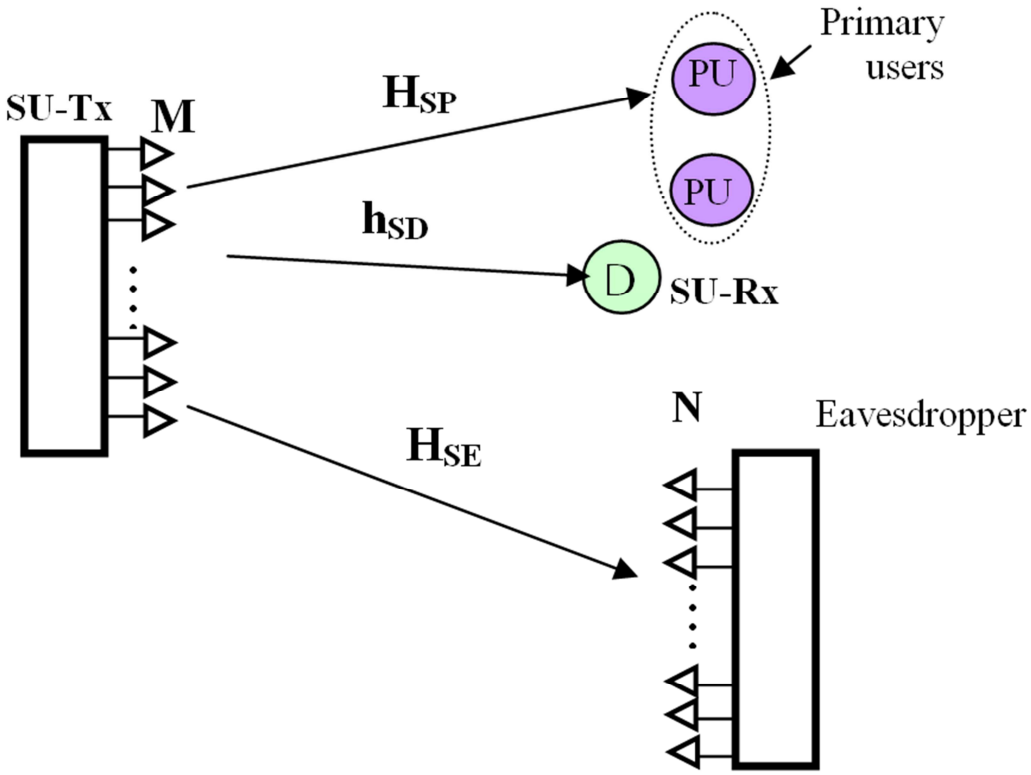

Figure 1. *Illustration of the system model.*

In the following two sections, the achievable secrecy rate and the secrecy outage probability analysis of the above system model considering passive and active eavesdropping are described, respectively. Section 3 presents the case of passive eavesdropping, whereas Section 4 presents active eavesdropping.

Passive Eavesdropping

In this section, the training phase and the data transmission phase of the system model described earlier in Section 2 will be presented, considering passive eavesdropping case.

Training Phase

In this phase, the SU-Tx estimates the downlink channel to the SU-Rx by transmitting training pilots sequences from SU-Rx to SU-Tx. This estimated channel is used for the precoding in the data transmission phase. The passive eavesdropper is operating in the receive mode only and does not send any data in this phase. The received signal at SU-Tx is given by

$$\mathbf{y}_{S,T} = \sqrt{P_D \beta_{DS}}\,\mathbf{h}_{DS} x_p + \mathbf{z}_p \tag{1}$$

where x_p is the transmitted pilot signal from the SU-Rx, P_D is the SU-Rx transmit power per symbol, $\mathbf{z}_d \sim \mathcal{CN}(0, N_0)$ is the AWGN at the SU-Tx, and $\mathbf{h}_{DS}$ is the channel gain vector between SU-Rx and SU-Tx. Moreover, we will assume that $E[|x_p|^2] = 1$. With least square channel estimation, the estimated channel at SU-Tx is given by

$$\hat{\mathbf{h}} = \left(\sqrt{P_D \beta_{DS}}\,\mathbf{h}_{DS} + \mathbf{z}_p\right)^T = \sqrt{P_D \beta_{DS}}\,\mathbf{h}_{SD} x_p + \mathbf{z} \tag{2}$$

The SU-Tx constructs $M\times 1$ precoding vector w as a scaled version of matched filter as follows

$$\boldsymbol{w} = \frac{1}{\sqrt{\gamma}}\hat{\mathbf{h}}^{\mathrm{H}} = \frac{1}{\sqrt{\gamma}}\sqrt{P_D \beta_{DS}}\,\mathbf{h}_{SD}^{\mathrm{H}} + \mathbf{z}^{\mathrm{H}} \tag{3}$$

where γ is a power normalization factor at SU-Tx, which is given as [12]

$$\gamma = tr(\hat{\boldsymbol{h}}\hat{\boldsymbol{h}}^{\mathrm{H}}) = \left\|\hat{\boldsymbol{h}}\right\|^2 \tag{4}$$

Data Transmission Phase

In this phase, the SU-Tx uses w given in (3) to do a beamforming for the data transmission to the SU-Rx. The received signal at the SU-Rx is given as

$$\begin{aligned} y_D &= \sqrt{P_S \beta_{SD}}\,\boldsymbol{h}_{SD}\boldsymbol{w}x_d + z_d = \sqrt{\frac{P_S \beta_{SD}}{\gamma}}\,\boldsymbol{h}_{SD}\hat{\boldsymbol{h}}^H x_d + z_d \\ &= \sqrt{\frac{P_S P_D \beta_{DS} \beta_{SD}}{\gamma}}\,\boldsymbol{h}_{SD}\hat{\boldsymbol{h}}_{SD}^H x_d + \sqrt{\frac{P_S \beta_{SD}}{\gamma}}\,\boldsymbol{h}_{SD}\boldsymbol{z}^H x_d + z_d \end{aligned} \tag{5}$$

where x_d is the transmitted symbol to the SU-Rx, and P_s represents the SU-Tx transmit power. Z_d is the AWGN at SU-Rx, with zero mean and unit variance. The received message vector at the PUs is given by

$$\begin{aligned} \boldsymbol{y}_P &= \sqrt{P_S \beta_{SP}}\,\boldsymbol{h}_{SP}\boldsymbol{w}x_d + z_p = \sqrt{\frac{P_S \beta_{SP}}{\gamma}}\,\boldsymbol{h}_{SP}\hat{\boldsymbol{h}}^H x_d + z_P \\ &= \sqrt{\frac{P_S P_D \beta_{DS} \beta_{SP}}{\gamma}}\,\boldsymbol{h}_{SP}\hat{\boldsymbol{h}}_{SD}^H x_d + \sqrt{\frac{P_S \beta_{SP}}{\gamma}}\,\boldsymbol{h}_{SP}\boldsymbol{z}^H x_d + z_P \end{aligned} \tag{6}$$

where $\mathbf{h}_{SP}$ is the $L \times M$ channel matrix between SU-Tx and PUs, $\mathbf{z}_p \sim \mathcal{CN}(0, N_0\mathbf{I}_L)$ is the $L \times M$ noise vector at the PUs, and $\mathbf{I}_L$ is an $L \times L$ identity matrix. The received signal of the selected antenna at the eavesdropper is given as

$$\begin{aligned} \boldsymbol{y}_E &= \sqrt{P_S \beta_{SD}}\,\boldsymbol{h}_{SE_s}\boldsymbol{w}x_d + \boldsymbol{z}_e = \sqrt{\frac{P_S \beta_{SD}}{\gamma}}\,\boldsymbol{h}_{SE_s}\hat{\boldsymbol{h}}^H x_d + z_e \\ &= \sqrt{\frac{P_S P_D \beta_{DS} \beta_{SE}}{\gamma}}\,\boldsymbol{h}_{SE_s}\hat{\boldsymbol{h}}_{SD}^H x_d + \sqrt{\frac{P_S \beta_{SE}}{\gamma}}\,\boldsymbol{h}_{SE_s}\boldsymbol{z}^H x_d + z_e \end{aligned} \tag{7}$$

where $\boldsymbol{h}_{SE_s}$ is the channel vector between the SU-Tx and the selected antenna at Eavesdropper; the antenna selection is performed as follows $\left|\boldsymbol{h}_{SE_s}\boldsymbol{w}\right| = \max_{i \in \{1,2,\ldots\ldots,N\}} \left|\boldsymbol{h}_{SE_i}\boldsymbol{w}\right|^2$.

Achievable Secrecy Rate and Secrecy Outage Probability Analysis

In this subsection, we investigate the effect of M-MIMO on the secrecy rate in terms of the achievable secrecy rate. We consider the case of one eavesdropper as shown in Figure 1. The instantaneous achievable secrecy rate for considered network model is given by [18]

$$R_s = \begin{cases} \left[R_{SD} - R_{SE}\right]^+ = \left[\log_2\left(1+\gamma_{SD}\right) - \log_2\left(1+\gamma_{SE}\right)\right]^+ & , \quad IN_P \le \Gamma \\ 0 & IN_P > \Gamma \end{cases} \tag{8}$$

where

R_{SD}: The obtained rate for the link from SU-Tx to SU-Rx.

R_{SE}: The obtained rate for the link from SU-Tx to Eavesdropper link.

γ_{SD} : The instantaneous SNRs for the link from SU-Tx to SU-Rx.

γ_{SE} : The instantaneous SNRs for the link from SU-Tx to Eavesdropper.

IN_p : The interference power at the primary user from the SU-Tx, and noise.

Γ : The interference temperature limit.

The instantaneous SNR at SU-Rx is given as

$$\gamma_{SD} = P_S \beta_{SD} \left| \boldsymbol{h}_{SD} \frac{\hat{\boldsymbol{h}}}{\left\| \hat{\boldsymbol{h}} \right\|} \right|^2 = P_S \beta_{SD} \left| \boldsymbol{h}_{SD} \frac{\sqrt{P_D \beta_{DS}}\, \mathbf{h}_{SD} x_p + \mathbf{z}_p}{\left\| \sqrt{P_D \beta_{DS}}\, \mathbf{h}_{SD} x_p + \mathbf{z}_p \right\|} \right|^2 \tag{9}$$

The SNR at eavesdropper is given as

$$\gamma_{SE} = P_S \beta_{SE} \left| \boldsymbol{h}_{SE_s} \frac{\hat{\boldsymbol{h}}}{\left\| \hat{\boldsymbol{h}} \right\|} \right|^2 = P_S \beta_{SE} \left| \boldsymbol{h}_{SE_s} \frac{\sqrt{P_D \beta_{DS}}\, \mathbf{h}_{SD} x_p + \mathbf{z}_p}{\left\| \sqrt{P_D \beta_{DS}}\, \mathbf{h}_{SD} x_p + \mathbf{z}_p \right\|} \right|^2 \tag{10}$$

The SNR at the PU is given as

$$\gamma_{SP} = P_S \beta_{SP} \left| \boldsymbol{h}_{SP} \frac{\hat{\boldsymbol{h}}}{\left\| \hat{\boldsymbol{h}} \right\|} \right|^2 = P_S \beta_{SP} \left| \boldsymbol{h}_{SP} \frac{\sqrt{P_D \beta_{DS}}\, \mathbf{h}_{SD} x_p + \mathbf{z}_p}{\left\| \sqrt{P_D \beta_{DS}}\, \mathbf{h}_{SD} x_p + \mathbf{z}_p \right\|} \right|^2 \tag{11}$$

Now, the achievable secrecy rate is investigated when a large number of antennas are used at the SU-Tx, i. e., when M→∞. The SNRs at SU-Rx and eavesdropper are asymptotically expressed as [19]

$$\gamma_{SD}^{\infty} = \lim_{M \to \infty} \gamma_{SE} = \frac{M P_S P_D \beta_{SD} \beta_{DS}}{\left(P_D \beta_{DS} + 1 \right)} \tag{12}$$

$$\gamma_{SE}^{\infty} = \lim_{M \to \infty} \gamma_{SE} = o(1) \tag{13}$$

where $O(1)$ denotes any random variable s with the property $\lim_{M \to \infty} \left(\frac{s}{M^{\theta}} \right) = 0, \quad \theta > 0$

In this paper, the Secrecy Outage Probability (SOP) in a CRN is denoted as P_{sop} . It is the probability that the secrecy rate is less than a given target secrecy rate Rt , subject to the interference power constraints at the PUs or the probability of the interference power at the primary user is larger than a certain interference temperature limit. P_{sop} is given as [10]

$$P_{sop} = \Pr\left\{ R_s^M < R_t \right\} \Pr(IN_p \le \Gamma) + \Pr(IN_p > \Gamma) \tag{14}$$

Active Eavesdropping

In this section, the case of active eavesdropping is considered. In this paper, we assume that the training sequence is fixed and used all the time and so it can be easily obtained by a sophisticated eavesdropper [20]. In other words, the Eavesdropper

can send the same pilot sequence as the SU-Rx.

Training Phase

In this phase, the received signal at SU-Tx is expressed as:

$$\mathbf{y}_{SA} = \sqrt{P_D \beta_{DS}}\mathbf{h}_{DS} x_p + \sqrt{P_E \beta_{ES}}\mathbf{h}_{E_s S} x_p + \mathbf{z}_p \tag{15}$$

where P_E is the power of the transmitted symbol at Eavesdropper. The estimated channel at SU-Tx based on least square channel estimation method is given by:

$$\hat{\mathbf{h}} = \sqrt{P_D \beta_{DS}}\mathbf{h}_{SD} + \sqrt{P_E \beta_{ES}}\mathbf{h}_{SE_s} + \mathbf{z} \tag{16}$$

Now, the precoding vector w is constructed at SU-Tx as follows

$$\boldsymbol{w} = \frac{1}{\sqrt{\gamma}}\hat{\mathbf{h}}^{\mathrm{H}} = \frac{1}{\sqrt{\gamma}}\left(\sqrt{P_D \beta_{DS}}\mathbf{h}_{SD}^{\mathrm{H}} + \sqrt{P_E \beta_{ES}}\mathbf{h}_{SE_s}^{\mathrm{H}} + \mathbf{z}^{\mathrm{H}}\right) \tag{17}$$

Data Transmission Phase

In this phase, the received signal at SU-Rx is written as follows:

$$\begin{aligned} \boldsymbol{y}_D &= \sqrt{P_S \beta_{SD}}\boldsymbol{h}_{SD}\boldsymbol{w}x_d + z_d \\ &= \sqrt{\frac{P_S P_D \beta_{DS}\beta_{SD}}{\gamma}}\boldsymbol{h}_{SD}\hat{\boldsymbol{h}}_{SD}^{H} x_d \\ &\quad + \sqrt{\frac{P_S P_E \beta_{SD}\beta_{EA}}{\gamma}}\boldsymbol{h}_{SD}\hat{\boldsymbol{h}}_{SE_s}^{H} x_d + \sqrt{\frac{P_S \beta_{SD}}{\gamma}}\boldsymbol{h}_{SD}\boldsymbol{z}^{H} x_d + z_d \end{aligned} \tag{18}$$

The received message at the PUs is given by

$$\begin{aligned} \boldsymbol{y}_P &= \sqrt{P_S \beta_{SP}}\boldsymbol{h}_{SP}\boldsymbol{w}x_d + z_p \\ &= \sqrt{\frac{P_S P_D \beta_{DS}\beta_{SP}}{\gamma}}\boldsymbol{h}_{SP}\boldsymbol{h}_{SD}^{H} x_d \\ &\quad + \sqrt{\frac{P_S P_E \beta_{ES}\beta_{SP}}{\gamma}}\boldsymbol{h}_{SP}\boldsymbol{h}_{SE_s}^{H} x_d + \sqrt{\frac{P_S \beta_{SP}}{\gamma}}\boldsymbol{h}_{SP}\boldsymbol{z}^{H} x_d + z_P \end{aligned} \tag{19}$$

The received signal at the selected antenna at the eavesdropper is expressed as

$$\begin{aligned} \boldsymbol{y}_E &= \sqrt{P_S \beta_{SD}}\boldsymbol{h}_{SE_s}\boldsymbol{w}x_d + z_e \\ &= \sqrt{\frac{P_S P_D \beta_{DS}\beta_{SD}}{\gamma}}\boldsymbol{h}_{SE_s}\boldsymbol{h}_{SD}^{H} x_d \\ &\quad + \sqrt{\frac{P_S P_E \beta_{ES}\beta_{SD}}{\gamma}}\boldsymbol{h}_{SE_s}\boldsymbol{h}_{SE_s}^{H} x_d + \sqrt{\frac{P_S \beta_{SD}}{\gamma}}\boldsymbol{h}_{SE_s}\boldsymbol{z}^{H} x_d + z_e \end{aligned} \tag{20}$$

Note that in the active eavesdropper case, the eavesdropper needs only one antenna as SU-Rx to send the pilot attack. In the receiver side at the eavesdropper, the same antenna is used since it will give the maximum SNR.

Achievable Secrecy Rate and Secrecy Outage Probability Analysis

The instantaneous achievable secrecy rate is expressed as

$$R_s = \begin{cases} \left[\log_2(1+\gamma_{SD}) - \log_2(1+\gamma_{SE})\right]^+ & , \quad IN_P \le \Gamma \\ 0 & IN_P > \Gamma \end{cases} \tag{21}$$

The SNRs at SU-Rx, eavesdropper, and PU are given as

$$\gamma_{SD} = P_S \beta_{SD} \left| \boldsymbol{h}_{SD} \frac{\sqrt{P_D \beta_{DS}}\mathbf{h}_{SD} + \sqrt{P_E \beta_{ES}}\mathbf{h}_{SE_s} + \mathbf{z}}{\left\| \sqrt{P_D \beta_{DS}}\mathbf{h}_{SD} + \sqrt{P_E \beta_{ES}}\mathbf{h}_{SE_s} + \mathbf{z} \right\|} \right|^2 \tag{22}$$

$$\gamma_{SE} = P_S \beta_{SE} \left| \boldsymbol{h}_{SE_s} \frac{\sqrt{P_D \beta_{DS}}\mathbf{h}_{SD} + \sqrt{P_E \beta_{ES}}\mathbf{h}_{SE_s} + \mathbf{z}}{\left\| \sqrt{P_D \beta_{DS}}\mathbf{h}_{SD} + \sqrt{P_E \beta_{ES}}\mathbf{h}_{SE_s} + \mathbf{z} \right\|} \right|^2 \tag{23}$$

$$\gamma_{SP} = P_S \beta_{SP} \left| \boldsymbol{h}_{SP} \frac{\sqrt{P_D \beta_{DS}}\mathbf{h}_{SD} + \sqrt{P_E \beta_{ES}}\mathbf{h}_{SE_s} + \mathbf{z}}{\left\| \sqrt{P_D \beta_{DS}}\mathbf{h}_{SD} + \sqrt{P_E \beta_{ES}}\mathbf{h}_{SE_s} + \mathbf{z} \right\|} \right|^2 \tag{24}$$

The asymptotic SNRs at SU-Tx and eavesdropper are given as [19]

$$\gamma_{SD}^{\infty} = \lim_{M \to \infty} \gamma_{SE} = \frac{M P_S P_D \beta_{SD} \beta_{DS}}{(P_D \beta_{DS} + P_E \beta_{ES} + 1)} \tag{25}$$

$$\gamma_{SE}^{\infty} = \lim_{M \to \infty} \gamma_{SE} = o(1) \tag{26}$$

The secrecy outage probability for CRN is given as [10]

$$P_{sop} = \Pr\left\{C_s^M < R_s\right\} \Pr(IN_p \le \Gamma) + \Pr(IN_p > \Gamma) \tag{27}$$

Simulation Results

In this section, the effectiveness of the proposed scheme is investigated using Monte Carlo simulation. 10,000 independent trials are performed to show the performance gains of the M-MIMO for PHY in CRN.

Figures 2 and 3 show the secrecy rate with passive eavesdropper versus the number of antennas at SU-Tx for different number of antennas at eavesdropper when Γ = -10 dB and Γ = 0 dB, respectively. P_s=10 dB, P_D=0 dB and $\beta_{DS} = \beta_{SD}$ =1 are assumed for both figures. Also, normalized transmitted power at SU-Tx is assumed. From Figures 2 and 3, it is clearly seen that the secrecy rate significantly improves by increasing the number of antennas at SU-Tx, especially when N is low. This is attributed to the property of channel hardening of M-MIMO. Figure 2 shows that the rate R_{SE} increases by increasing N, regardless of the number of antennas at SU-Tx. Figure 3 illustrates that the rate R_{SE} increases by increasing N and decreases by increasing the number of antennas at SU-Tx. Figure 2 and 3 show that the secrecy rate when Γ is high is higher than that when Γ is low.

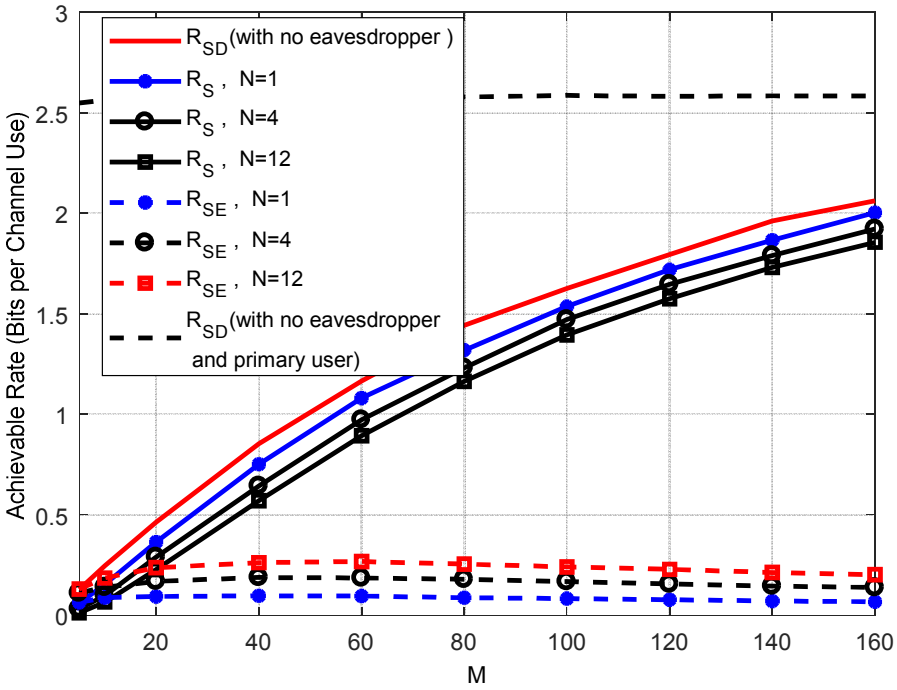

Figure 2. *Secrecy rate performance vs. M,* Γ *= -10 dB, for passive eavesdropper case.*

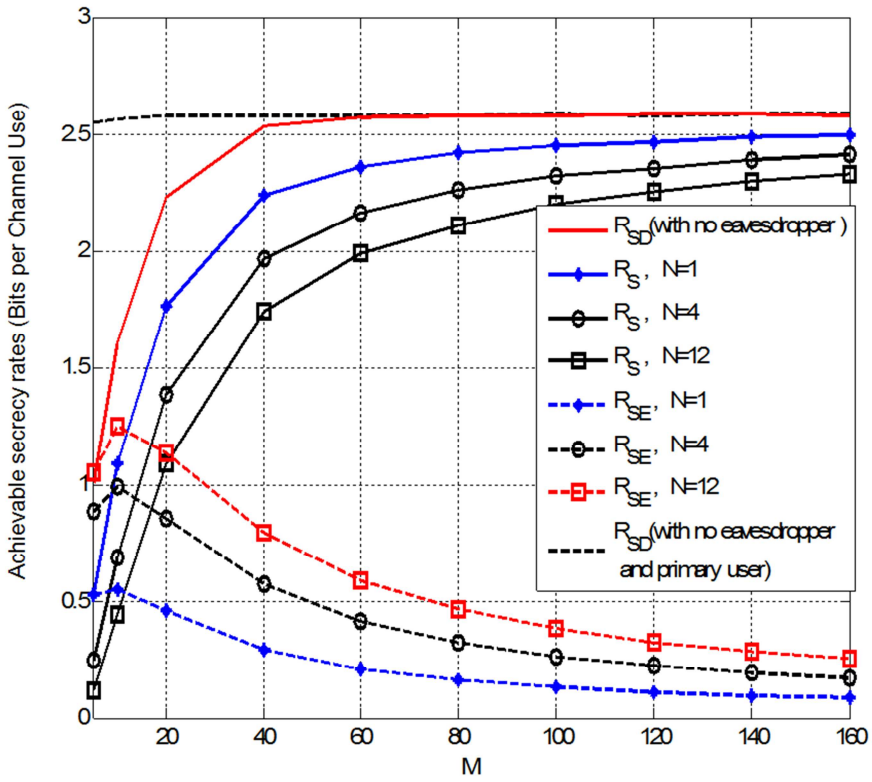

Figure 3. *Secrecy rate performance vs. M,* Γ *= 0 dB, for passive eavesdropper case.*

The achievable secrecy rate against the SU-Tx transmit power for different number of antenna at SU-Tx, single antenna at eavesdropper, and single PU is shown in Figure 4. As can be seen, the massive MIMO scheme significantly enhances the achievable secrecy rate. Moreover, the achievable rate first increases to a certain power value, and then it decreases. This is because the interference at the PU increases when the transmitted power of the SU-Tx increases.

The impact of the number of antennas at the eavesdropper N, and the SU-Tx transmit power P_s on the performance of the proposed system is studied and shown in Figure 5. It clears from this figure that as the number of antennas at the eavesdropper increases, the secrecy rate decreases.

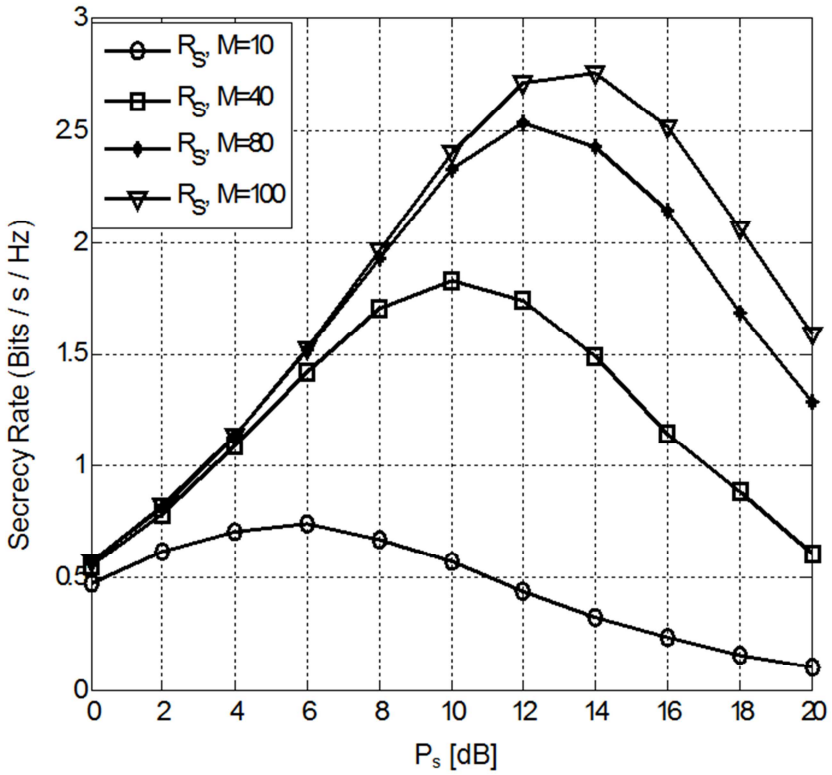

Figure 4. *Secrecy rate performance versus SU-Tx transmit power, N=1.*

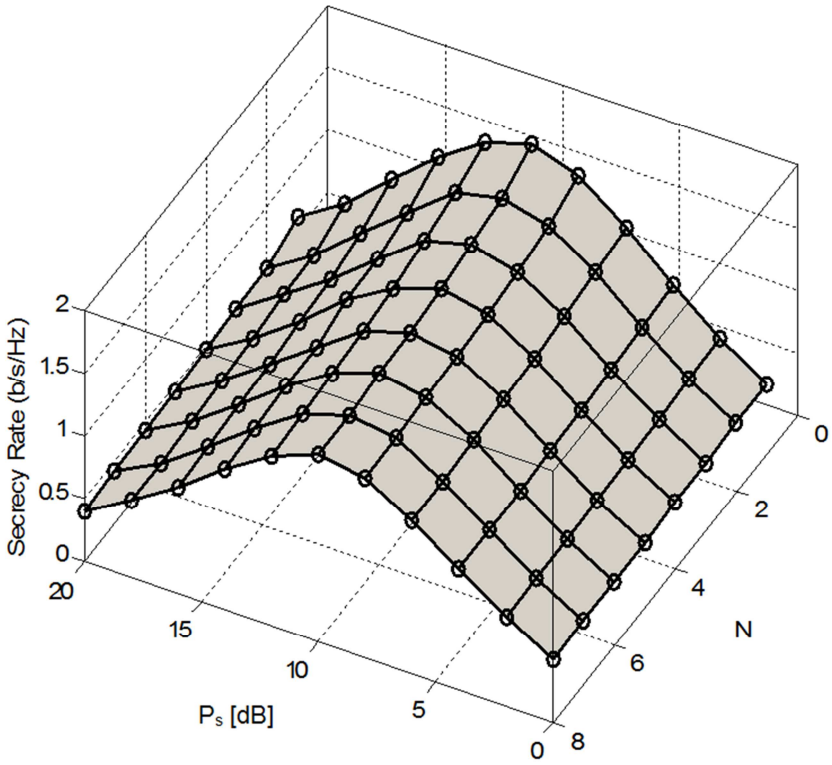

Figure 5. *Variation of the Secrecy rate with both SU-Tx transmit power and N.*

Now, we use the secrecy outage probability as a performance metric to verify the effectiveness of the massive MIMO for achieving secure transmissions in CRNs. Figure 6 shows the performance of M-MIMO in CRN in terms of secrecy outage probability against SU-Tx transmit power for single PU and different value of *M*. A target secrecy rate of 0.5 bits/s/Hz is considered. We observe from this figure that the robustness of the M-MIMO is achieved.

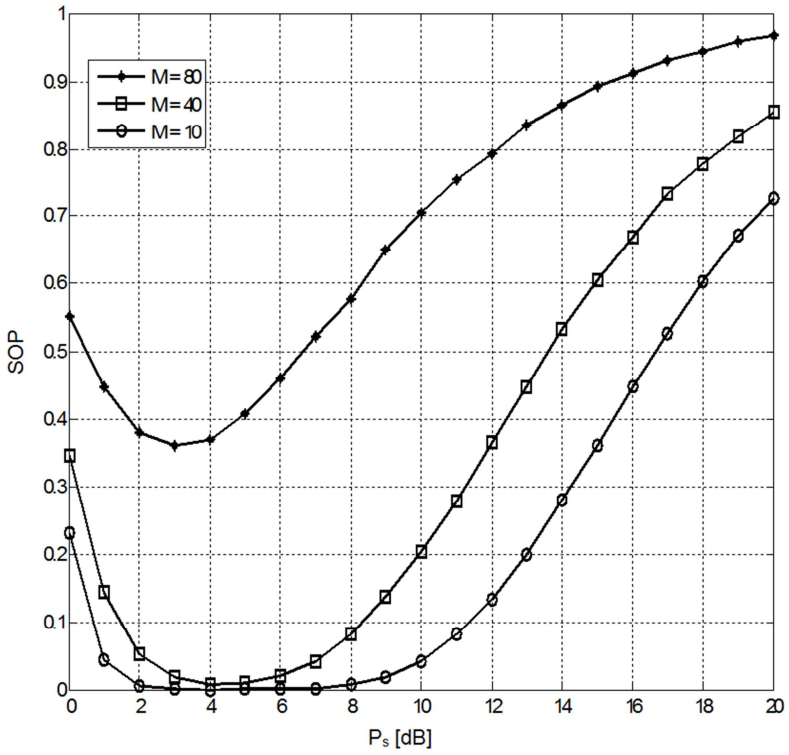

Figure 6. *SOP against SU-Tx transmit power for different value of M, single PU.*

Now, we study the impact of the number of PUs on the secrecy performance for M-MIMO in CRN. Figure 7 depicts the secrecy rate against the SU-Tx transmit power for different number of antenna at SU-Tx, single antenna at eavesdropper, and two PUs. We observe from this figure that the secrecy rate decreases with the increase in the number of PUs for different number of antenna at SU-Tx. But, we observe that the difference on achievable secrecy rate begin at SU-Tx transmit power at 6 dB of CRN. This is due to the varies of the fading channels between SU-Tx and two primary users is notified when SU-Tx transmit power is larger than 6 dB. Moreover, we observe from figure 7 that the increasing the number of antennas at SU-Tx significantly improves the secrecy rate with increasing *M*.

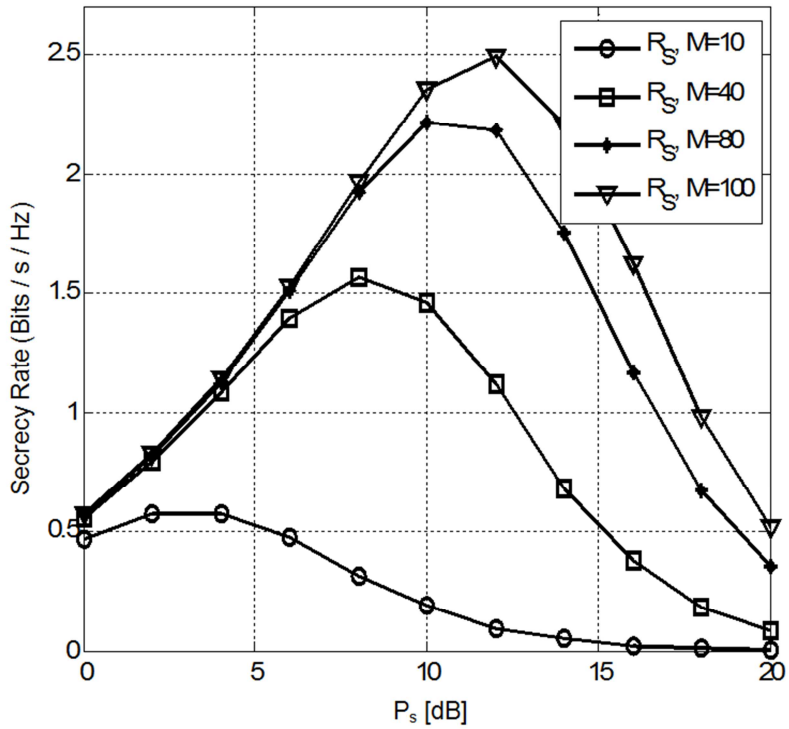

Figure 7. *Secrecy rate performance vs. SU-Tx transmit power, N=1, and two primary users.*

The secrecy rate against the SU-Tx transmit power for different number of antenna at SU-Tx, multi antenna at eavesdropper N=4, and two PU is shown in Figure 8. Figure 9 depicts the secrecy outage probability vs SU-Tx transmit power for different value of M, and two PUs. A target secrecy rate of 0.5 bits/s/Hz is considered for evaluating the secrecy outage probability.

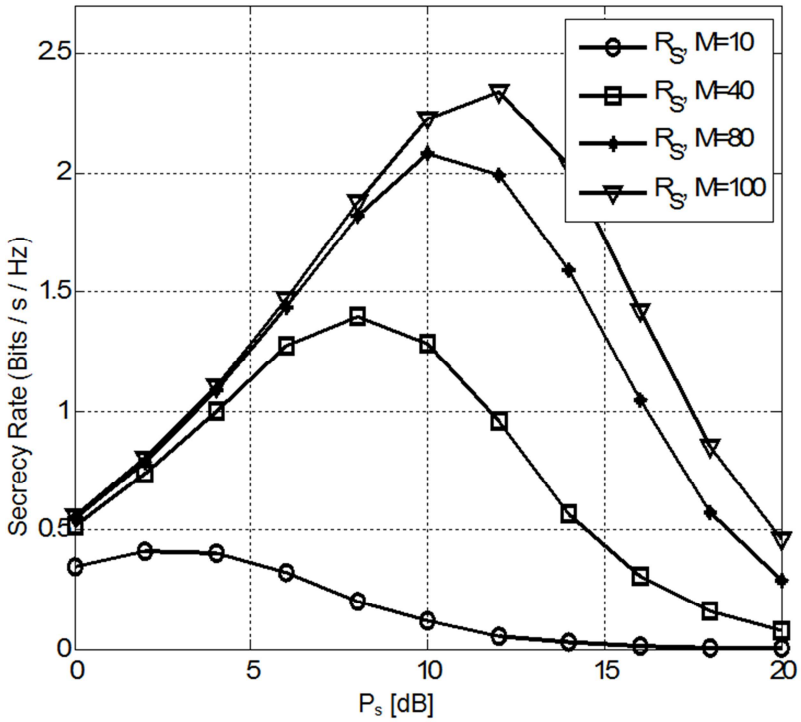

Figure 8. *Secrecy rate performance vs. SU-Tx transmit power, N=4, and two primary users.*

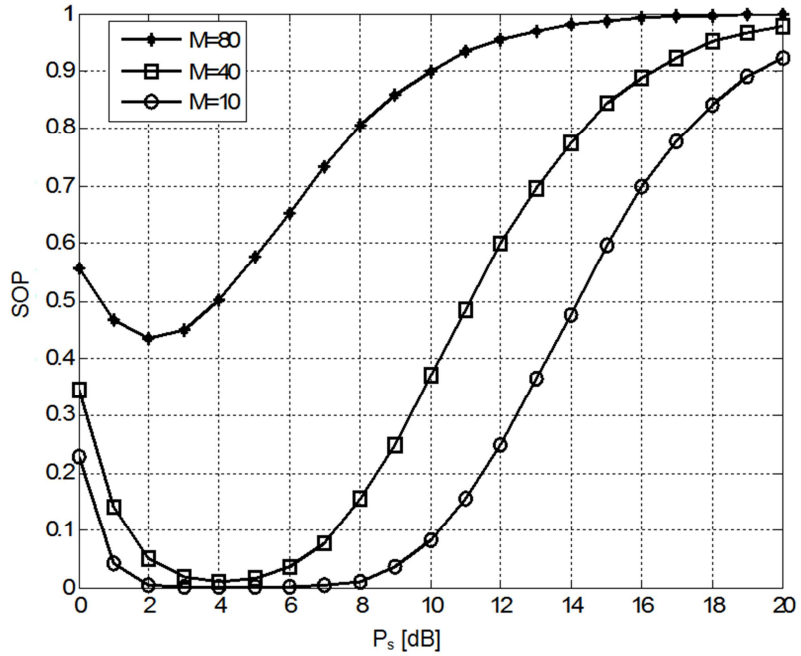

Figure 9. *SOP against SU-Tx transmit power for different value of M, Two PU.*

Finally, we investigate the performance of the proposed system for the case of active eavesdropper, that attacks the training phase and send the same pilot sequence as SU-Rx. Figure 10 depicts the secrecy rate performance vs M under different values of P_E. We observe from this figure that the secrecy rate degrades when the power at eavesdropper P_E increases. We conclude from this figure that the secrecy rate performance depends on the eavesdropper transmit power P_E in the training phase.

Figure 11 shows the achievable secrecy rate vs SU-Tx transmit power, with active eavesdropper for M =40 and 100, and the power at eavesdropper P_E = - 5 dB. The secrecy rate increases to a certain value, and then it decreases as shown on the figure; this is due to the power interference constraints at the primary users.

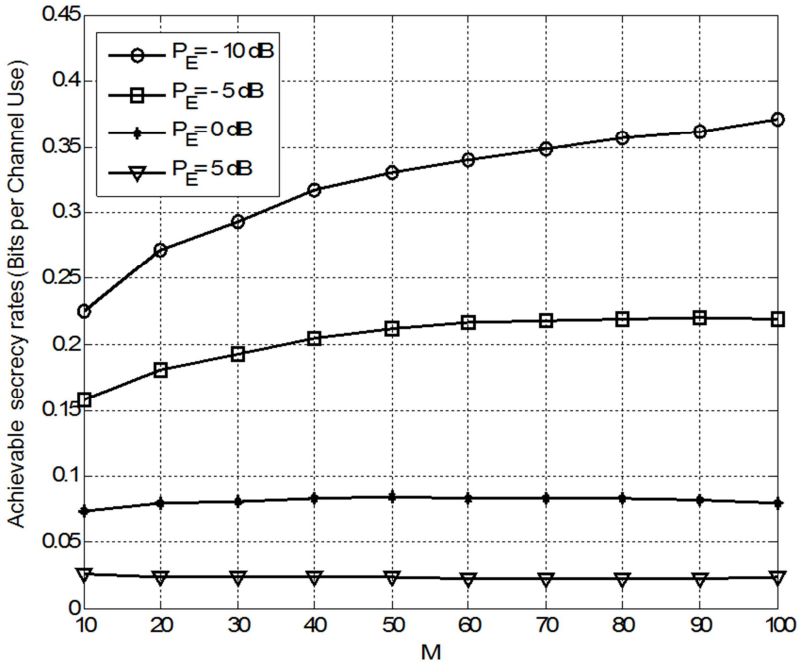

Figure 10. *Achievable secrecy rate vs. M under different values of Eavesdropper's power P_E for active eavesdropper case.*

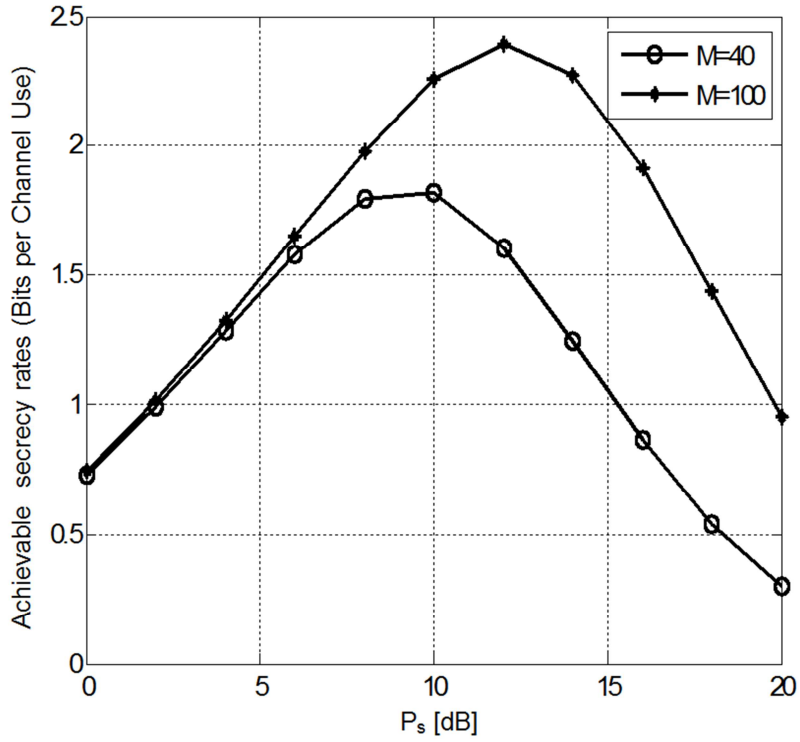

Figure 11. *Achievable secrecy rate vs. SU-Tx transmit power under different values of M and P_E = -5 dB for active eavesdropper case.*

Conclusions

In this paper, we investigated the physical layer security for information transfer between SU-Tx and SU-Rx in cognitive radio networks using massive MIMO under several constraints such as primary interference threshold power. We have studied

the massive MIMO in cognitive radio networks for different number primary users. Our results show that the massive MIMO in CRN increases the achievable secrecy rate significantly and reduces the secrecy outage probability. Furthermore, we have concluded that increasing the number of antennas at the eavesdropper has small effect on the system performance of cognitive radio networks with massive MIMO. We tested the network for the cases of passive and active eavesdropping and we have shown that active eavesdropping degrades the secrecy rate significantly due to the pilot attack at the training phase. ■

Hefdhallah Sakran

Hefdhallah Sakran received his B.Sc. degree in Electrical Engineering (Communications & Electronics) from Jordan university of Science and Technology, Jordan, in 2003. He received his M.Sc. degree and Ph.D. degree from the Faculty of Electronic Engineering at El-Minufiya University, Egypt, in 2008 and 2013, respectively. Currently, he is assistant with the Department of Electrical Engineering, Ibb University, Yemen. His research areas include PAPR in OFDM system, MIMO communication, WiMAX, cognitive radio, game theory and most recent SC-FDMA based cognitive radio and Massive MIMO. Email address: hefdh_sakran@ yahoo.com.

Azzam Al-nahari

Azzam Al-Nahari received the B.Sc. degree in electronic and communication engineering from the University of Technology, Iraq, and the M.Sc. and Ph.D. degrees in electrical communications from the Faculty of Electronic Engineering, Menoufia University, Egypt, in 2008 and 2011, respectively. In 2012, he held a post-doctoral position with the Department of Electrical and Information Technology, Lund University, Sweden. He also held a post-doctoral position with University at Buffalo, Buffalo, NY, USA, in 2014. He is currently an Associate Professor with the Department of Electrical Engineering, Ibb University, Yemen. His current research interests include massive MIMO systems, and physical layer security.

Faisal Al-kamali

Faisal S. Al-kamali has received the B.Sc. degree in Electronics and Communications Engineering from the Faculty of Engineering, Baghdad University, Baghdad, Iraq, in 2001. He has received the M.Sc. and Ph.D. degrees from the Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 2008 and 2011, respectively. His research areas of interest include Equalization, interference cancellation, spread spectrum techniques, and digital communication over fading dispersive channels.

Sami Tarbosh

Dr. Sami S. Tarbosh received his BSc degree in electronics and communications engineering from Applied Science University, Amman, Jordan, in 1998 and the MSc degree in communications from University of Jordan, Amman, Jordan, in 2002. He joined Ibb University, Yemen, in 2002, where he worked as senior lecturer in the Department of Electrical Engineering (2002-2007). In March 2013, he obtained his Ph.D. degree in Mobile Communication at Universiti Teknologi Malaysia, Johor, Malaysia. Currently, he is assistant professor in Ibb University. His research interests concern channel estimation and ICI reduction for OFDM systems. He can be contacted through email: sami.tarbosh@gmail.com.

References

[1] Federal Communications Commission, “Spectrum Policy Task Force Report,” FCC Document ET Docket no. 02-155, Nov. 2002.

[2] Notice of Proposed Rulemaking on Cognitive Radio, Federal Communications Commission (FCC) Std. no. 03-322, Dec. 2003.

[3] J. Mitola, “Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio,” Ph.D. Thesis, KTH, Stockholm, Sweden, 2000.

[4] S. Haykin, “Cognitive Radio: Brain-Empowered Wireless Communications,” *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

[5] P. J. Kolodzy, “Interference Temperatue: a Metric for Dynamic Spectrum Utilization,” *International Journal of Network Management*, vol. 16, pp. 103–113, Apr. 2006.

[6] A. Wyner, “The Wire-tap Channel,” *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[7] Y. Pei, Y.-C. Liang, K. C. Teh and K. H. Li, “Achieving Cognitive and Secure Transmissions Using Multiple Antennas,” *IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 1–5, Sep. 2009.

[8] Y. Pei, Y.-C. Liang, K. C. Teh and K. H. Li, "Secure Communication over MISO Cognitive Radio Channels," *IEEE Transaction on Wireless Communications*, vol. 9, no. 4, pp. 1494–1502, Apr. 2010.

[9] Y. Pei, Y. Liang, K. Chan and K. Li "Secure Communication in Multiantenna Cognitive Radio Networks With Imperfect Channel State Information," *IEEE Transactions on Signal Processing,* vol. 59, no. 4, Apr. 2011.

[10] H. Sakran, M. Shokair, O. Nasr, S. El-Rabaie, and A. A. El-Azm,"Proposed relay selection scheme for physical layer security incognitive radio networks," *IET Communications*, vol. 6, no. 16, pp. 2676–2687, 2012.

[11] M. Z. I. Sarkar and T. Ratnarajah, "Enhancing security in the cognitive relay assisted co-existing radio systems with interferences," *in Proceedings of the IEEE International Conference on Communications (ICC '13)*, pp. 4729–4733, June 2013.

[12] Y. Yu, L. Hu, H. Li, Y. Zhang, F. Wu, and J. Chu, "The Security of Physical Layer in Cognitive Radio Networks," *Journal of Communications,* vol. 9, No. 12, December 2014.

[13] L. Jiang and H. Tian, "Energy-Efficient Relay Selection Scheme for Physical Layer Security in Cognitive Radio Networks," *Hindawi Publishing Corporation*, vol. 2015, 2015.

[14] H. Zhang, T. Wang, L. Song, Z. Han, "Interference Improves PHY Security for Cognitive Radio Network," *IEEE Transactions on Information Forensics and Security*, vol. 11, pp. 609 – 620, 2016.

[15] T. Marzetta, "Noncooperative cellular wireless with unlimited numbers of base station antennas," *IEEE Trans. Wirel. Commun.,* pp. 3590–3600, 2010.

[16] F. Rusek, D. Persson, B. K. Lau, et al. "Scaling up MIMO: opportunities and challenges with very large arrays," *IEEE Signal Process. Mag*., pp. 40–60, 2013.

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

[18] L. Wang, K. K. Wong, M. Elkashlan, A. Nallanathan, and S. Lambotharan, "Secrecy and energy efficiency in massive MIMO aided heterogeneous C-RAN: A new look at interference", *IEEE Journal of Selected Topics in Signal Processing*, 10 (8), pp. 1375-1389, 2016.

[19] A. Al-nahari, "Physical layer security using massive multiple-input and multiple-output: passive and active eavesdroppers," *IET Communications,* vol. 10, pp. 50–56, 2016.

[20] X. Zhou, B. Maham, A., Hjørungnes, "Pilot contamination for active eavesdropping," *IEEE Trans. Wirel. Commun.,* vol. 11, pp. 903–907, 2012.