Received December 1, 2020, accepted December 19, 2020, date of publication December 30, 2020,
date of current version January 12, 2021.

Digital Object Identifier 10.1109/ACCESS.2020.3048158

Secure Cognitive MIMO Wiretap Networks With Different Antenna Transmission Schemes

YONG CHEN[1], TAO ZHANG[2], XIAOQIANG QIAO[2], HAO WU[2], AND JIANG ZHANG[2]
[1]College of Communication Engineering, Army Engineering University of PLA, Nanjing 210007, China
[2]The Sixty-third Research Institute, National University of Defense Technology, Nanjing 210007, China

Corresponding authors: Tao Zhang (ztcool@126.com) and Xiaoqiang Qiao (qxq0527@163.com)

This work was supported in part by the Project of Natural Science Foundation of China under Grant 61801496, Grant 61801497, and Grant 61771487; in part by the Defense Science Foundations of China under Grant 2019-JCJQ-JJ-221; and in part by the National University of Defense Technology Youth Innovation Award Research Project under Grant 23200306.

ABSTRACT This paper investigates a secure transmission in the multiple-input multiple-output (MIMO) cognitive wiretap networks, where a secondary transmitter (Alice) sends data to a secondary receiver (Bob) in the presence of an eavesdropper (Eve). In order to solve the problems of inter channel interference and inter antenna synchronization encountered by traditional MIMO technologies, the antenna transmission scheme is adopted at the transmitter. As a comparison, we design two different antenna transmission schemes, namely transmit antenna selection maximal-ratio combining (TAS-MRC) scheme and differential spatial modulation maximal-ratio combining (DSM-MRC) scheme, respectively. Moreover, due to outdated channel state information (CSI) of the interference link from Alice to the primary user (PU), we propose power control mechanism to protect the quality of service (QoS) of PU. Furthermore, the closed-form for the secrecy outage probability and the secrecy throughput with TAS-MRC and DSM-MRC schemes are derived to evaluate the secrecy performance, respectively. What's more, we explore the security diversity gain and coding gain based on the asymptotic secrecy outage probability. As the results, it demonstrates that DSM-MRC requires less CSI and is convenient for modulation and demodulation, but sacrifices some secrecy performance gains between two proposed schemes.

INDEX TERMS Physical layer security, cognitive radio, differential spatial modulation, secrecy outage probability, secrecy throughput.

I. INTRODUCTION

Cognitive radio technology was proposed by J. Mitola in 1999 [1]. It is an intelligent software radio and has more flexible features than traditional software radio. Then in 2003, the Federal Communications Commission (FCC) gave the specification definition as a technology that can guide the communication system to adjust the performance parameters and transmission strategies to effectively use the licensed spectrum. It means that under the premise of not affecting the quality of service (QoS) of primary users (PUs), secondary users detect available frequency bands through spectrum sensing technology, use spectrum judgment to select the best available frequency band, and use spectrum sharing to negotiate with primary users to access the spectrum and carry out their communication tasks [2], [3].

The associate editor coordinating the review of this manuscript and approving it for publication was Liehuang Zhu.

A. BACKGROUND

Due to the openness of wireless communication, private information in the networks is vulnerable to attacks such as eavesdropping. In addition, the cognitive radio networks (CRNs) use a dynamic spectrum access mechanism to enhance spectrum utilization and reduce the scarcity of spectrum resources, but it poses a huge threat to users in the networks [4], [5]. Compared with the traditional cryptographic security strategy, the physical layer security (PLS) transmission strategy is considered to be a simpler and more efficient solution. The current research of PLS is mainly based on the wire-tap channel model proposed by Wyner in 1975 [6]. Over the years, researchers have proposed signal processing technologies such as user scheduling, artificial noise, multi-input and multi-output (MIMO), zero-forcing jamming, and relay coordination to improve the secrecy performance [7]–[11].

In particular, the cognitive radio technology is an necessary requirement for next generation communication. However, the security of wireless networks is critical as it

is easily exposed to external threats, and several works have investigated the security issues from the perspective of the physical layer CRNs [12]–[14]. In [12], the authors design a secure transmission, where cooperative beamforming is used to enhance the secrecy performance for PUs and secondary users. In addition, the authors in [13] guarantee the secrecy performance of the system by controlling the power distribution of jamming relay and forwarding relay to optimize the secrecy rate. Since asymmetric signals have better performance in the interference-limited networks, the authors in [14] propose improper Gaussian signaling (IGS) in order to improve the PLS of CRNs. However, the key limitations of these aforementioned works is that the perfect knowledge of the channel state information (CSI) is assumed. Due to the requirement for more information interaction in CRNs, the impact of outdated CSI of the interference link to PU should be considered. Thus, the authors in [15] researched the secrecy outage performance of a single-input multiple-output (SIMO) underlay cognitive radio networks with outdated CSI. Furthermore, the authors in [16] design a secure transmission in a dual-hop randomize-and-forward (RaF) cognitive MIMO wiretap networks with outdated CSI. Moreover, several works have investigated the security issues from the perspective of the physical layer with different transmit antenna selection schemes [17], [18]. The authors in [17] investigated four transmit antenna selection schemes in a dual-hop relay RF-FSO systems. In [18], Lei et.al considered a NOMA network wiretapped with suboptimal antenna selection and optimal antenna selection schemes.

We note that the difference spatial modulation (DSM) scheme is an effective approach with a low implementation complexity and achieve a tradeoff between performance and delay [19]. In particular, DSM is based on the evolution of spatial modulation (SM) technology. Compared with the traditional multi-antenna transmission schemes, the SM only needs one radio frequency (RF) unit at the transmitter, which can solve the problems of inter channel interference (ISI) and inter antenna synchronization (IAS) [20], [21]. The transmission signals of the SM scheme is made up of two parts, which one part transmitted by symbol modulation and the other part mapped to an antenna to transmit information by selecting an antenna. What's more, each data block actually transmitted depends on the actual data currently and the previously data block, so as to achieve differential modulation in the network using the DSM scheme, thereby eliminating the need for CSI during demodulation by the receiver [19]. Considering the benefits of DSM, authors combine DSM with PLS and investigate the secure transmission based on differential quadrature spatial modulation with artificial noise in MISO wiretap networks in [22]. Despite the above benefits, the PLS by the DSM scheme in MIMO CRNs has not been investigated so far.

B. MOTIVATION AND CONTRIBUTION

In this paper, we investigate secure transmission in the MIMO cognitive wiretap networks with outdated CSI of interference link to PU over Rayleigh fading channels under two different antenna transmission schemes, transmit antenna selection maximal-ratio combining (TAS-MRC) and differential spatial modulation maximal-ratio combining (DSM-MRC) schemes, in which the secondary transmitter (Alice) transmits private information to the secondary receiver (Bob) in the presence of an eavesdropper (Eve). In the network, both Bob and Eve are equipped with multiple antennas and adopt maximal-ratio combining (MRC) to receive the signals from Alice. Significantly, considering the interference from Alice to PU with outdated CSI, power control mechanism is adopted to guarantee the normal communication of PU. The contributions of this paper are summarized as follows.

- We derive the closed-form expressions for the secrecy outage probability and the secrecy throughput of the considered sensor networks with TAS-MRC and DSM-MRC schemes, respectively. Moreover, we explore the impact of the various system parameters on the secrecy outage probability and the secrecy throughput, i.e, the time correlation coefficient, the number of antennas and the interference threshold of PU.
- We derive the asymptotic closed-form expressions for the secrecy outage probability and the secrecy diversity order. And secrecy coding gain is achieved under two different high SNR scenarios. The research results show that the two schemes we considered can obtain the same diversity gain $N_A N_B$, but there is a gap in the coding gain between them.
- Through the analysis for the secrecy outage probability and the secrecy throughput, it has been verified that DSM-MRC achieves the same diversity gain as TAS-MRC with less CSI, sacrificing some coding gain in CRNs. The asymptotic expressions can show the influence of different parameters on the system. Through research we can draw the conclusion that increasing the interference threshold of PU and increasing the number of antennas of Alice and Bob can enhance the secrecy performance.

The remaining parts of this paper is organized as follows. In Section II, the system model are proposed and described. In Section III, the secrecy outage probability of the considered networks is derived. In Section IV, we investigate the asymptotic secrecy outage probability of the considered networks under high SNR and the secrecy throughput. In Section V, the numerical results and discussions are presented. Finally, we make a conclusion in Section VI.

II. SYSTEM MODEL

In this paper, we consider the MIMO cognitive wiretap radio networks, where the secondary transmitter (Alice) sends private information to the secondary receiver (Bob) in the presence of an eavesdropper (Eve) as shown in Fig.1. According to existing researches, there are three main CRNs spectrum sharing strategies, i.e., underlay, overlay and interweave [23]. The underlay CR is the most easily used method to access the licensed spectrum in CRNs. In underlay paradigm,

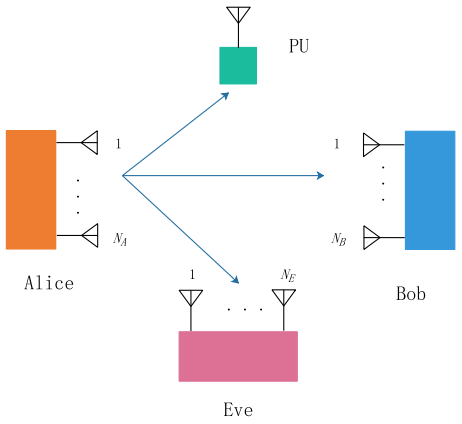

FIGURE 1. System model.

primary users (PUs) allows secondary users (SUs) to transmit concurrently in the same spectrum the interference caused by SUs is below a given threshold [24]. Assume that the cognitive networks adopt the underly spectrum sharing method, which allows primary networks and secondary networks in the same spectrum band. For the cognitive MIMO radio networks, Alice, Bob and Eve are equipped with multiple antennas N_A, N_B and N_E, respectively, whereas the PU is equipped with a single antenna. And we assume that the primary transmitter (PT) is far away from the secondary receivers, thus PT will not interfere the secondary user [25]–[27]. In addition, Eve is an passive eavesdropper [28], [29].

In this paper, all the channels are assumed to undergo independent identically distributed (i.i.d.) Rayleigh fading. And the channel coefficient of link $N \rightarrow M$ is defined as h_{NM}, which is exponentially distributed random variable with zero mean and variance λ_{MN}. And we define the channel gains $E\left[|h_{NM}|^2\right] = \lambda_{NM} = d_{NM}^{-\alpha}$, where $E[\cdot]$ is the expectation operation, d_{NM} and α are the distance of the link and the path loss factor, respectively. What's more, in the general CRNs, in order not to cause mutual interference between the primary and secondary networks, the power of the transmitter is limited. It reduces the interaction performance between the primary and secondary networks, and causes the secondary user transmitter to be unable to obtain the perfect CSI between Alice and PU, making the channel inevitably present feedback delay. In this paper, the channel coefficient between Alice and PU can be modeled as [30]

$$\widetilde{h}_{AP} = \rho h_{AP} + \sqrt{1-\rho^2} e_{AP}, \tag{1}$$

where e_{AP} is the complex Gaussian variable having the same variance as h_{AP} and is uncorrelated with h_{AP}, ρ is the time correlation coefficient between $\widetilde{h}_{AP}$ and h_{AP}. According to Jake's autocorrelation model, $\rho = J_0(2\pi f T)$, where f is the represents the maximum Doppler frequency, T is the delay between the selection instant and the transmission instant, and $J_0(\cdot)$ is the zeroth-order Bessel function of the first kind [31].

Suppose Alice encodes the data into a codeword x using a capacity achieving codebook for wiretap channel [32]. To explore the secrecy performance of CRNs, we investigate the transmission process with different antenna transmission schemes i.e. TAS-MRC and DSM-MRC schemes.

A. TAS-MRC SHEME

In the TAS-MRC scheme, Bob adopts MRC receiving mode to combine all received channel's signals, and Alice selects the antenna with maximum channels gain by the information based on the feedback of CSI from Bob. Thus, the instantaneous SNR received at Bob is derived as

$$\gamma_B^{TAS-DSM} = \frac{P_s \left\| h_{A^*B} \right\|^2}{\sigma^2}, \tag{2}$$

where $P_s = \min\left\{\frac{Q}{\left|\widetilde{h}_{A^*P}\right|^2}, P_t\right\}$, in which $\widetilde{h}_{A^*P}$ is the delayed channel from Alice's transmission antenna to PU. P_t and Q denote the maximum transmit power constraint at Alice and the tolerable interference threshold at PU, respectively. In addition, h_{A^*B} denotes the channel vector $\mathbb{C}^{N_B \times 1}$ between the transmit antenna with maximum channels gain at Alice ($\|h_{A^*B}\|^2 = \max\limits_{i=1,\cdots,N_A} \left\|h_{A_iB}\right\|^2$). And σ^2 is the additive white Gaussian noise (AWGN) at Bob.

Moreover, due to the influence of outdated CSI on the interference of Alice to PU, PU will be interrupted half of the time due to exceeding its preset the tolerable interference threshold Q [33]. Alice adaptively adjust the power margin factor κ according to the channel feedback delay coefficient ρ and the primary user constraint interference Q, thereby ensuring the QoS of the primary network [34], [35]. Thus, we set a new interference power constraint κ by power control mechanism to guarantee the QoS of primary user. According to the power control mechanism, we take the probabilistic approach as in [16], where Alice adapts its power such that the PU can maintain a pre-selected outage probability δ_0. Therefore, the transmit powers P_s at Alice can be derived as

$$P_s = \min\left\{\kappa \frac{Q}{\left|\widetilde{h}_{A^*P}\right|^2}, P_t\right\}, \tag{3}$$

where κ is the power margin factor at Alice, the power margin factor κ can be numerically expressed as follows:

$$\begin{aligned}\delta_0 = {} & e^{-\frac{Q}{\lambda_{AP}P_t}} - \frac{t}{r} Q_0\left(\sqrt{\frac{(s-r)Q}{2P_t}}, \sqrt{\frac{(s+r)Q}{2P_t}}\right) \\ & + \frac{1}{2}\left(1+\frac{t}{r}\right) e^{-\frac{sQ}{2P_t}} I_0\left(\frac{2\rho^2 Q\sqrt{\kappa}}{\sqrt{1-\rho^2}\lambda_{AP}P_t}\right) \\ & - e^{-\frac{Q}{\lambda_{AP}P_t}} Q_0\left(\frac{2\rho^2 Q}{\left(1-\rho^2\right)\lambda_{AP}P_t}, \frac{2\kappa Q}{\left(1-\rho^2\right)\lambda_{AP}P_t}\right),\end{aligned} \tag{4}$$

where $s = \frac{2}{\lambda_{AP}}\left(\frac{1+\kappa}{1-\rho^2}\right)$, $t = \frac{2}{\lambda_{AP}}\left(\frac{1-\kappa}{1-\rho^2}\right)$, $r = \sqrt{s^2 - \frac{16\kappa\rho^2}{\lambda_{AP}^2(1-\rho^2)}}$, $Q_0(a,b)$ is the first-order Marcum

Q-function and $I_0(\cdot)$ is the zeroth-order modified Bessel function of the first kind.

In general, MRC scheme is also adopted at Eve for enhancing eavesdropping capabilities. Therefore, the SNR received at Eve can be get as

$$\gamma_E^{TAS-MRC} = \frac{P_s}{\sigma^2} \|h_{A^*E}\|^2, \tag{5}$$

where h_{A^*E} is the channel vector $\mathbb{C}^{N_E \times 1}$ and σ^2 is AWGN at Eve.

B. DSM-MRC SHEME

In the DSM-MRC scheme, Alice adopts DSM to modulate the signal and sends the information to Bob, which means each antenna at Alice sends signals in turn according to the coding order, relative to TAS scheme, there is no need to adjust the sending order based on feedback. And we also assume Bob adopts MRC to combine signals of all received channel. It is noteworthy that using DSM, each information transmission block is constituted of N_A consecutive time slots. Signals are $N_A \times N_A$ space-time matrix block S, which is composed of the signal vector within N_A time instant. The (m, t)th entry of S denotes the symbol s_{mt} transmitted via,which the mth transmit antenna at time instant t. Given that Alice transmits the tth block $S_t \in \mathbb{C}^{N_A \times N_A}$, each antenna is activated only once per space-time block. In other words, only one entry in any column or row of S_t is nonzero. The signals received by the k_1-th antenna of Bob ($(1 \le k_1 \le N_B)$) or the k_2-th antenna Eve ($1 \le k_2 \le N_E$) during the duration of t-th block can be given as:

$$y_{B,k_1} = h_{AB,k_1} S_t + n_{B,k_1}, \tag{6}$$

and

$$y_{E,k_2} = h_{AE,k_2} S_t + n_{E,k_2}, \tag{7}$$

where $y_{B,k_1} \in \mathbb{C}^{1 \times N_B}$ and $y_{E,k_2} \in \mathbb{C}^{1 \times N_E}$ are the received signal vector, $h_{AB,k_1} \in \mathbb{C}^{1 \times N_B}$ and $h_{AE,k_2} \in \mathbb{C}^{1 \times N_E}$ are the channel vector. And n_{B,k_1} and n_{E,k_2} are additive white Gaussian noise (AWGN) vectors at k_1-th antenna of Bob and k_2-th antenna of Eve, respectively. Thus, the received SNR at the k_1-th antenna of Bob and the k_2-th antenna of Eve can be get as

$$\gamma_{B,k_1} = \frac{\left\| h_{AB,k_1} S_t \right\|^2}{N_A \sigma^2}, \tag{8}$$

and

$$\gamma_{E,k_2} = \frac{\left\| h_{AE,k_2} S_t \right\|^2}{N_A \sigma^2}. \tag{9}$$

There's only one non-zero value per row per column in the matrix S_t. As the result, we can get $\left\| h_{AB,k_1} S_t \right\|^2 = P_s \left\| h_{AB,k_1} \right\|^2$, $\left\| h_{AE,k_2} S_t \right\|^2 = P_s \left\| h_{AE,k_2} \right\|^2$. By substituting these into (8) and (9), respectively, the received SNR at the k_1-th antenna of Bob and the k_2-th antenna of Eve can be derived as

$$\gamma_{B,k_1} = \frac{P_s \left\| h_{AB,k_1} \right\|^2}{N_A \sigma^2}, \tag{10}$$

and

$$\gamma_{E,k_2} = \frac{P_s \left\| h_{AE,k_2} \right\|^2}{N_A \sigma^2}. \tag{11}$$

In addition, we assume that Bob and Eve receive the messages by MRC scheme to combine the signals received by each antenna. In this way, the SNR received at Bob and Eve can be derived as

$$\gamma_B^{DSM-MRC} = \frac{P_s \|h_{AB}\|^2}{N_A \sigma^2}, \tag{12}$$

and

$$\gamma_E^{DSM-MRC} = \frac{P_s \|h_{AE}\|^2}{N_A \sigma^2}. \tag{13}$$

where $h_{AB} \in \mathbb{C}^{N_A \times N_B}$ and $h_{AE} \in \mathbb{C}^{N_A \times N_E}$ are the channel matrix. In addition, the transmit powers P_s at Alice is limited to the same as the TAS-MRC sheme and σ^2 is AWGN at Bob and Eve.

Then, according to Shannon's information theory, the capacity of Bob and Eve can be get as $C_B = \log_2(1 + \gamma_B)$ and $C_E = \log_2(1 + \gamma_E)$, respectively. In addition, the achievable secrecy rate of the system is $C_s = [C_B - C_E]^+$ by Wyner's encoding strategy, where $[x]^+ = \max\{x, 0\}$.

To simplify the representation of the following expressions, we define $\mu = \frac{Q}{P_t}$,$\bar{\gamma}_B = \frac{P_t}{\sigma^2}\lambda_{AB} = \frac{Q}{\mu\sigma^2}\lambda_{AB}$, $\bar{\gamma} = \frac{P_t}{\sigma^2}\lambda_{AE} = \frac{Q}{\mu\sigma^2}\lambda_{AE}$ and $G = \left|\widetilde{h}_{AP}\right|^2$.

III. SECRECY PERFORMANCE ANALYSIS

In this section, the closed-form expressions for the secrecy outage probability, which defined as the probability of the secrecy capacity (C_s) is smaller than the given threshold rate (R_s) are investigated. As the result, the secrecy outage probability is written as follows.

$$\begin{aligned} P_{out}(R_s) &= \Pr(C_s < R_s) \\ &= \int_0^\infty F_{\gamma_B}\left(2^{R_s}(1+x) - 1\right) f_{\gamma_E}(x)\, dx. \end{aligned} \tag{14}$$

Then, we derive the closed-form expressions for the secrecy outage probability of CRNs with different antenna transmission schemes, i.e. TAS-MRC and DSM-MRC schemes.

A. TAS-MRC SCHEME

The main challenge in solving the secrecy outage probability of CRNs is that γ_B and γ_E are statistically dependent due to the presence of the common random variable, G. We solve the problem in two steps by first solving the conditional probability, and then using the conditional average method. Thus, we find the cumulative distribution function (CDF) of

the SNR at Bob and the probability density function (PDF) of the SNR at Eve conditioned on the random variable G, respectively.

According to (2), the conditional CDF of $\gamma_B^{TAS-MRC}$ can be expressed as

$$F_{\gamma_B}^{TAS-MRC}(x|G) = \sum_{i=0}^{N_A} \binom{N_A}{i} (-1)^i \exp \times \left(-\frac{i\sigma^2 x}{P_s \lambda_{AB}}\right) \Theta_{N_B,i} \left(\frac{\sigma^2 x}{P_s \lambda_{AB}}\right)^{\phi}, \tag{15}$$

where $\Theta_{N_B,i} = \sum_{n_1=0}^{i} \sum_{n_2=0}^{n_1} \cdots \sum_{n_{N_B-1}=0}^{n_{N_B-2}} \frac{i!}{n_{N_B-1}!} \prod_{t=1}^{N_B-1} \frac{(t!)^{n_{t+1}-n_t}}{(n_{t+1}-n_t)!}$ with $n_0 = i$, $n_{N_B} = 0$ and $\varphi = \sum_{q_0=1}^{N_B-1} n_{q_0}$.

Then, the conditional PDF of $\gamma_E^{TAS-MRC}$ with the help of (5) is given by

$$f_{\gamma_E}^{TAS-MRC}(x|G) = \frac{x^{N_E-1}}{\Gamma(N_E)\left(\frac{P_s\lambda_{AE}}{\sigma^2}\right)^{N_E}} \exp\left(-\frac{\sigma^2 x}{P_s\lambda_{AE}}\right). \tag{16}$$

Next, substituting (15) and (16) into (14), the conditional $P_{out}^{TAS-MRC}(R_s|G)$ can be derived as (17), shown at the bottom of the page.

Finally, the secrecy outage probability of TAS-MRC scheme averaging over G can be computed by mathematical operation.

Theorem 1: By using TAS-MRC scheme, the secrecy outage probability of $P_{out}^{TAS-MRC}(R_s)$ can be get as (18), shown at the bottom of the page.

Where $\Gamma(\cdot,\cdot)$ is the incomplete upper gamma function, as defined in [31, Eq. (8.350.2)].

Proof: See Appendix A.

B. DSM-MRC SCHEME

Similar to TAS-MRC, due to the transmit power P_s is restricted by the PU, $\gamma_B^{DSM-MRC}$ and $\gamma_E^{DSM-MRC}$ are statistically dependent due to the common random variable, G. Thus, we find the conditional CDF of $\gamma_B^{DSM-MRC}$ and the conditional PDF of $\gamma_E^{DSM-MRC}$.

For DSM-MRC scheme, observing from (12), the conditional CDF of $\gamma_B^{DSM-MRC}$ is derived as

$$F_{\gamma_B^{DSM}}(x|G) = 1 - \exp\left(-\frac{N_A\sigma^2 x}{P_s\lambda_{AB}}\right) \sum_{k=0}^{N_A N_B-1} \frac{1}{k!} \left(\frac{N_A\sigma^2 x}{P_s\lambda_{AB}}\right)^k. \tag{19}$$

Then, the conditional PDF of $\gamma_E^{DSM-MRC}$ with the help of (13) can be derived as

$$f_{\gamma_E^{DSM}}(x|G) = \frac{x^{N_A N_E-1}}{\Gamma(N_A N_E)\left(\frac{P_s\lambda_{AE}}{N_A\sigma^2}\right)^{N_A N_E}} \exp\left(-\frac{N_A\sigma^2 x}{P_s\lambda_{AE}}\right). \tag{20}$$

Next, substituting (19) and (20) into (14), the conditional $P_{out}^{DSM-MRC}(R_s|G)$ is derived as (21), shown at the bottom of next page.

Similarly, averaging over G, we can get the result as follows.

Theorem 2: By using DSM-MRC scheme we can calculate the secrecy outage probability of $P_{out}^{DSM-MRC}(R_s)$, which is get as (22), shown at the bottom of next page.

Proof: See Appendix B.

IV. HIGH SNR ANALYSIS AND SECRECY THROUGHPUT

A. HIGH SNR ANALYSIS

Diversity technology is the study of how to make full use of the energy of the multipath signal in transmission to improve the reliability of transmission. It is also a study of how to use

$$P_{out}^{TAS-MRC}(R_s|G) = \sum_{i=0}^{N_A} \binom{N_A}{i} (-1)^i \exp\left(-\frac{i\sigma^2(2^{R_s}-1)}{P_s\lambda_{AB}}\right) \Theta_{N_B,i} \sum_{j=0}^{\varphi} \binom{\varphi}{j} \left(\frac{\sigma^2(2^{R_s}-1)}{P_s\lambda_{AB}}\right)^j \times \left(\frac{\sigma^2 2^{R_s}}{P_s\lambda_{AB}}\right)^{\varphi-j} \frac{1}{\Gamma(N_E)\left(\frac{P_s\lambda_{AE}}{\sigma^2}\right)^{N_E}} (N_E-1+\varphi-j)! \left(\frac{\sigma^2}{P_s\lambda_{AE}} + \frac{i\sigma^2 2^{R_s}}{P_s\lambda_{AB}}\right)^{-(N_E+\varphi-j)}. \tag{17}$$

$$P_{out}^{TAS-MRC}(R_s) = \left(1 - \exp\left(-\frac{\kappa u}{\lambda_{AP}}\right)\right) \sum_{i=0}^{N_A} \binom{N_A}{i} (-1)^i \exp\left(-\frac{i(2^{R_s}-1)}{\overline{\gamma}_B}\right) \Theta_{N_B,i} \sum_{j=0}^{\varphi} \binom{\varphi}{j} \left(\frac{2^{R_s}-1}{\overline{\gamma}_B}\right)^j \times \left(\frac{2^{R_s}}{\overline{\gamma}_B}\right)^{\varphi-j} \frac{1}{\Gamma(N_E)\left(\overline{\gamma}_E\right)^{N_E}} (N_E-1+\varphi-j)! \left(\frac{1}{\overline{\gamma}_E} + \frac{i2^{R_s}}{\overline{\gamma}_B}\right)^{-(N_E+\varphi-j)} + \frac{1}{\lambda_{AP}} \sum_{i=0}^{N_A} \binom{N_A}{i} (-1)^i \Theta_{N_B,i} \sum_{j=0}^{\varphi} \binom{\varphi}{j} \left(\frac{2^{R_s}-1}{\overline{\gamma}_B\kappa\mu}\right)^j \left(\frac{2^{R_s}}{\overline{\gamma}_B\kappa\mu}\right)^{\varphi-j} \frac{1}{\Gamma(N_E)\left(\overline{\gamma}_E\kappa\mu\right)^{N_E}} (N_E-1+\varphi-j)! \times \left(\frac{1}{\overline{\gamma}_E\kappa\mu} + \frac{i2^{R_s}}{\overline{\gamma}_B\kappa\mu}\right)^{-(N_E+\varphi-j)} \left(\frac{i(2^{R_s}-1)}{\overline{\gamma}_B\kappa\mu} + \frac{1}{\lambda_{AP}}\right)^{-j-1} \Gamma\left(j+1, \left(\frac{i(2^{R_s}-1)}{\overline{\gamma}_B\kappa\mu} + \frac{1}{\lambda_{AP}}\right)\kappa\mu\right), \tag{18}$$

the basic parameters of the signal in the time domain, frequency domain and space domain, how to disperse and how to collect them technology [36]–[38]. In order to describe the relationship between system performance and various parameters more intuitively, we studied the asymptotic performance of the security outage probability under high SNR conditions, and then obtain the diversity gain. Thus, we gain more insight on secrecy performance of CRNs by the high SNR analysis expression. Specifically, we consider two scenarios: 1) $\overline{\gamma}_B \to \infty$ and fixed $\overline{\gamma}_E$, i.e., the SNR at Bob outperforms the SNR at Eve. 2) $\overline{\gamma}_B \to \infty$ and $\overline{\gamma}_E \to \infty$, i.e., both Bob and Eve are close to Alice. It means that both the wiretap channel and secondary transmission channel are equipped with better SNR. In addition, the secrecy performance of CRNs can be expressed by the diversity gain and coding gain.

1) SCENARIO I: $\overline{\gamma}_B \to \infty$ AND FIXED $\overline{\gamma}_E$

a: TAS-MRC SCHEME

Corollary 1: The asymptotic secrecy outage probability of TAS-MRC scheme under $\overline{\gamma}_B \to \infty$ and *fixed* $\overline{\gamma}_E$ can be given as

$$P_{out}^{TAS-MRC}(R_s) \approx \Delta_{TAS-MRC}\overline{\gamma}_B^{-N_A N_B}, \tag{23}$$

Similarly, by simple calculation, $\Delta_{TAS-MRC}$ is given as

$$\begin{aligned}
&\Delta_{TAS-MRC} \\
&= \left(1-\exp\left(-\frac{\kappa u}{\lambda_{AP}}\right)\right)\frac{1}{(N_B!)^{N_A}\Gamma(N_E)(\bar{\gamma}_E)^{N_E}} \\
&\times \sum_{i=0}^{N_A N_B}\left(2^{R_s}-1\right)^{i}\left(2^{R_s}\right)^{N_A N_B-i}(N_A N_B-i+N_E-1)! \\
&\times \frac{1}{\bar{\gamma}_E}^{-(N_A N_B-i+N_E)} + \frac{1}{(N_B!)^{N_A}\Gamma(N_E)(\bar{\gamma}_E)^{N_E}}\left(\frac{1}{Q\mu\kappa}\right)^{N_A N_B} \\
&\times \sum_{i=0}^{N_A N_B}\left(2^{R_s}-1\right)^{i}\left(2^{R_s}\right)^{N_A N_B-i}(N_A N_B-i+N_E-1)! \\
&\times \frac{1}{\bar{\gamma}_E}^{-(N_A N_B-i+N_E)} \frac{1}{\lambda_{AP}}^{-N_A N_B+1}\Gamma\left(N_A N_B+1,\frac{\kappa\mu}{\lambda_{AP}}\right).
\end{aligned} \tag{24}$$

Proof: See Appendix C.

b: DSM-MRC SCHEME

Corollary 2: The secrecy outage probability for DSM-MRC scheme under $\overline{\gamma}_B \to \infty$ and *fixed* $\overline{\gamma}_E$ can be given as

$$P_{out}^{DSM-MRC}(R_s) \approx \Delta_{DSM-MRC}\overline{\gamma}_B^{-N_A N_B}, \tag{25}$$

Then, $\Delta_{DSM-MRC}$ is given as

$$\begin{aligned}
&\Delta_{DSM-MRC} \\
&= \left(1-\exp\left(-\frac{\kappa\mu}{\lambda_{AP}}\right)\right)\frac{1}{(N_A N_B)!} \\
&\times \sum_{i=0}^{N_A N_B}\binom{N_A N_B}{i}\left(2^{R_s}-1\right)^{N_A N_B-i}2^{R_s i}\frac{(N_A)^{N_A N_B}}{\Gamma(N_A N_E)(\bar{\gamma}_E)^{N_A N_E}} \\
&\times (N_A N_E+i-1)!\left(\frac{1}{\bar{\gamma}_E}\right)^{-(N_A N_E+i)} + \frac{1}{\lambda_{AP}}\frac{1}{(N_A N_B)!} \\
&\times \left(\frac{N_A}{\mu\kappa}\right)^{N_A N_B}\frac{1}{\Gamma(N_A N_E)(\bar{\gamma}_E)^{N_A N_E}}\sum_{i=0}^{N_A N_B}\binom{N_A N_B}{i} \\
&\times \left(2^{R_s}-1\right)^{N_A N_B-i}2^{R_s i}(N_A N_E+i-1)! \\
&\times \left(\frac{1}{\bar{\gamma}_E}\right)^{-(N_A N_E+i)}\left(\frac{1}{\lambda_{AP}}\right)^{-N_A N_B-1}\Gamma\left(N_A N_B+1,\frac{\mu\kappa}{\lambda_{AP}}\right).
\end{aligned} \tag{26}$$

Proof: See Appendix D.

$$\begin{aligned}
P_{out}^{DSM-MRC}(R_s|G) &= 1-\exp\left(-\frac{N_A\sigma^2\left(2^{R_s}-1\right)}{P_s\lambda_{AB}}\right)\frac{1}{\Gamma(N_A N_E)\left(\frac{P_s\lambda_{AE}}{N_A\sigma^2}\right)^{N_A N_E}}\sum_{k=0}^{N_A N_B-1}\frac{1}{k!}\left(\frac{N_A\sigma^2}{P_s\lambda_{AB}}\right)^{k} \\
&\times \sum_{i=0}^{k}\binom{k}{i}\left(2^{R_s}-1\right)^{k-i}\left(2^{R_s}\right)^{i}(N_A N_E-1+i)!\left(\frac{N_A\sigma^2 2^{R_s}}{P_s\lambda_{AB}}+\frac{N_A\sigma^2}{P_s\lambda_{AE}}\right)^{-N_A N_E-i}.
\end{aligned} \tag{21}$$

$$\begin{aligned}
P_{out}^{DSM-MRC}(R_s) &= 1-\left(1-\exp\left(-\frac{\kappa\mu}{\lambda_{AP}}\right)\right)\exp\left(-\frac{N_A\left(2^{R_s}-1\right)}{\overline{\gamma}_B}\right)\frac{1}{\Gamma(N_A N_E)\left(\frac{\overline{\gamma}_E}{N_A}\right)^{N_A N_E}}\sum_{k=0}^{N_A N_B-1}\frac{1}{k!}\left(\frac{N_A}{\overline{\gamma}_B}\right)^{k} \\
&\times \sum_{i=0}^{k}\binom{k}{i}\left(2^{R_s}-1\right)^{k-i}\left(2^{R_s}\right)^{i}(N_A N_E-1+i)!\left(\frac{N_A 2^{R_s}}{\overline{\gamma}_B}+\frac{N_A}{\overline{\gamma}_E}\right)^{-N_A N_E-i} \\
&- \frac{1}{\lambda_{AP}}\frac{1}{\Gamma(N_A N_E)\left(\frac{\mu\kappa\overline{\gamma}_E}{N_A}\right)^{N_A N_E}}\sum_{k=0}^{N_A N_B-1}\frac{1}{k!}\left(\frac{N_A}{\mu\kappa\overline{\gamma}_B}\right)^{k}\sum_{i=0}^{k}\binom{k}{i}\left(2^{R_s}-1\right)^{k-i}\left(2^{R_s}\right)^{i}(N_A N_E-1+i)! \\
&\times \left(\frac{N_A\left(2^{R_s}-1\right)}{\mu\kappa\overline{\gamma}_B}+\frac{1}{\lambda_{AP}}\right)^{-k+i-1}\left(\frac{N_A 2^{R_s}}{\mu\kappa\overline{\gamma}_B}+\frac{N_A}{\mu\kappa\overline{\gamma}_E}\right)^{-N_A N_E-i}\Gamma\left(k-i+1,\left(\frac{N_A\left(2^{R_s}-1\right)}{\mu\kappa\overline{\gamma}_B}+\frac{1}{\lambda_{AP}}\right)\kappa\mu\right).
\end{aligned} \tag{22}$$

Remark 1: The secrecy diversity gain of the TAS-MRC and DSM-MRC schemes is $N_A N_B$, which is only determined by the number of N_A and N_B. Moreover, the quality of the secondary transmission channel and wiretap channel influence the system secrecy performance through the coding gain, i.e., $G_{code}^{*} = {\Delta_*}^{-1/N_A N_B}$, in which $* \in$ (TAS-MRC, DSM-MRC), respectively.

According to the results in Remark 1 achieve the same diversity gain,it demonstrates that the difference between the two schemes depends on the coding gain. Then, we characterize the gap between two schemes as a simple ratio of their respective coding gain, which can be obtained as follows.

$$\frac{G_{code}^{TAS-MRC}}{G_{code}^{DSM-MRC}} = \left(\frac{\Delta_{TAS-MRC}}{\Delta_{DSM-MRC}}\right)^{-\frac{1}{N_A N_B}}. \tag{27}$$

Remark 2: Furthermore, by finding the logarithm of the simple ratio of their coding gains, the result indicates that for the same condition, the TAS-MRC scheme outperforms the DSM-MRC scheme by an gap of $-\frac{10}{N_A N_B} \lg\left(\frac{\Delta_{TAS-MRC}}{\Delta_{DSM-MRC}}\right)$ dB.

2) Scenario II: $\overline{\gamma}_B \to \infty$ AND $\overline{\gamma}_E \to \infty$

a: TAS-MRC SCHEME

Corollary 3: The asymptotic secrecy outage probability of the TAS-MRC scheme under $\overline{\gamma}_B \to \infty$ and $\overline{\gamma}_E \to \infty$ is derived as follows.

$$\begin{aligned} P_{out}^{TAS-MRC}(R_s) &\approx \sum_{i=0}^{N_A} \binom{N_A}{i} (-1)^i \Theta_{N_B,i} \left(\frac{2^{R_s}}{\bar{\gamma}_B}\right)^{\phi} \\ &\times \frac{1}{\Gamma(N_E)(\bar{\gamma}_E)^{N_E}} (N_E - 1 + \phi)! \left(\frac{1}{\bar{\gamma}_E} + \frac{i 2^{R_s}}{\bar{\gamma}_B}\right)^{-(N_E+\phi)}. \end{aligned} \tag{28}$$

Proof: Due to $\overline{\gamma}_B \to \infty$ and $\overline{\gamma}_E \to \infty$, the impact of the tolerable interference threshold Q can be ignored. With the help of (17), the asymptotic secrecy outage probability can be derived after the approximate computation.

b: DSM-MRC SCHEME

Corollary 4: The asymptotic secrecy outage probability of the DSM-MRC scheme under $\overline{\gamma}_B \to \infty$ and $\overline{\gamma}_E \to \infty$ can be written as

$$\begin{aligned} P_{out}^{DSM-MRC}(R_s) \approx 1 &- \frac{1}{\Gamma(N_A N_E)\left(\frac{\bar{\gamma}_E}{N_A}\right)^{N_A N_E}} \sum_{k=0}^{N_A N_B - 1} \frac{1}{k!} \\ &\times \left(\frac{N_A}{\bar{\gamma}_B}\right)^{k} \left(2^{R_s}\right)^{k} (N_A N_E - 1 + k)! \\ &\times \left(\frac{N_A 2^{R_s}}{\bar{\gamma}_B} + \frac{N_A}{\bar{\gamma}_E}\right)^{-N_A N_E - k}. \end{aligned} \tag{29}$$

Proof: Similar to the above scheme, according to (21), the asymptotic secrecy outage probability is derived without considering the impact of the tolerable interference threshold Q.

Remark 3: When $\overline{\gamma}_B \to \infty$ and $\overline{\gamma}_E \to \infty$, both two schemes reach the secrecy outage probability floor, which turns out that the system secrecy performance can only be enhanced by the secrecy coding gain under the scenario II.

B. SECRECY THROUGHPUT

In order to measure the reliability and security of CRNs more comprehensively, the secrecy throughput is proposed, which represents the amount of average secrecy information transmitted per unit time [22], [39]. As the result, the throughput expression for the two schemes of the considered networks can be given as

$$T_{out}^{*}(R_s) = \left(1 - P_{out}^{*}(R_s)\right) R_s, \tag{30}$$

where $* \in$ (TAS-MRC, DSM-MRC).

Remark 4: We can find out by analysis that $T_{out}^{*}(R_s)$ exist an optimal value in a given range of R_s by the equation (30). When R_s is small, $T_{out}^{*}(R_s)$ is small. However, when R_s is large enough, the secrecy outage probability tends to 1, and the $T_{out}^{*}(R_s)$ tends to 0. Therefore, determining the optimal value, R_s^{max}, which can achieve the local optimal secrecy throughput.

V. NUMERICAL RESULTS

In this section, the numerical results prove the correctness of the TAS-MRC and DSM-MRC schemes in the theoretical derivation of system secrecy performance. A detailed investigation on the effect of various system parameters, such as the number of antennas N_A, N_B and N_E, the time correlation coefficient ρ, and the interference threshold Q. In generally, $R_s = 1$ and $\sigma^2 = 1$ are set. In addition, the simulation results are obtained through 300000 independent Monte Carlo trials.

Fig. 2 plots the effects of the secrecy outage probability versus P_t/σ^2 of TAS-MRC and DSM-MRC schemes with different time correlation coefficient ρ. The figures show that when P_t/σ^2 is low, the secrecy outage probabilities of TAS-MRC and DSM-MRC schemes keep decreasing while P_t/σ^2 increasing. When P_t/σ^2 is high, the secrecy outage probabilities appear to be leveled, which means that the P_t/σ^2 is limited by interference threshold Q. In addition,

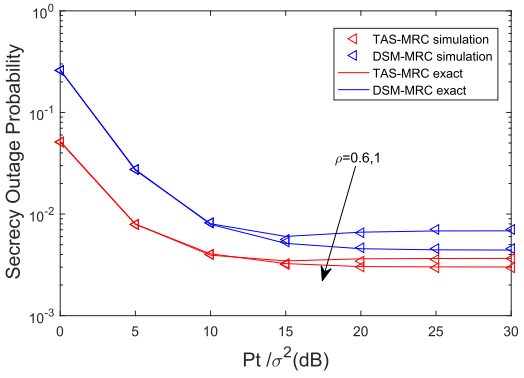

FIGURE 2. Secrecy outage probability of TAS-MRC and DSM-MRC scheme for different time correlation coefficient ρ when $N_A = 4$, $N_B = N_E = 2$ and $Q = 20dB$.

due to the outdated CSI of the interference link ($\rho = 0.6$), the transmit power P_t/σ^2 is limited by Alice. So P_t/σ^2 is simultaneously restricted by the interference threshold Q and the power margin factor κ. Since the constraints of Q and κ are not synchronized, the secrecy performance will have a minimum value when $\rho = 0.6$. As we can see from Fig. 3, the more deterministic the interference channels the κ is large, which means that the control constraints on P_s is lower and the secrecy performance is better. What's more, when P_t/σ^2 and Q are fixed, TAS-MRC scheme can attain better secrecy performance than DSM-MRC scheme in CRNs.

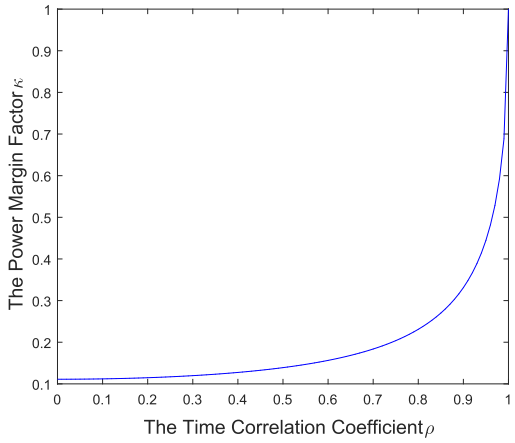

FIGURE 3. The power margin factor κ versus the time correlation coefficient ρ when $N_A = 4$, $N_B = N_E = 2$ and $Q = 20dB$ in high SNR.

Fig. 4 and 5 plot the influence for different numbers of N_A and the interference threshold Q on the secrecy outage performance of the TAS-MRC and DSM-MRC schemes, respectively. From both figures, the Monte Carlo simulation results are in good agreement with theoretical results. It shows that both schemes can enhance the secrecy performance by increasing the number of antennas or Q. In addition, as Q is larger, the secrecy performance gradually approaches that of traditional non-cognitive wiretap sensor networks without Q constraints. In addition, TAS-MRC scheme achieve better

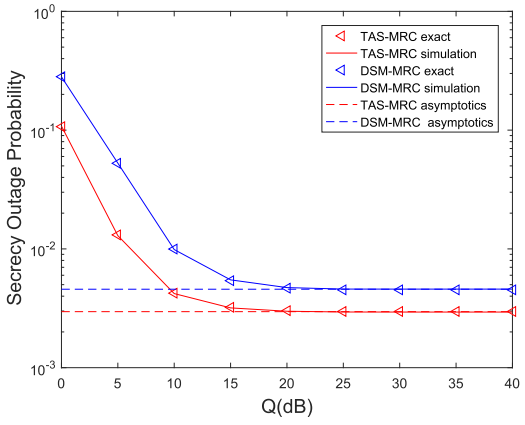

FIGURE 4. Secrecy outage probabilities of TAS-MRC and DSM-MRC schemes versus Q when $N_A = 4$, $N_B = N_E = 2$ and $P_t = 20$dB.

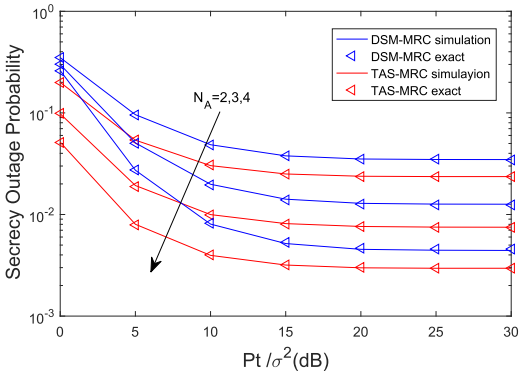

FIGURE 5. Secrecy outage probability of TAS-MRC and DSM-MRC schemes versus the tranmit power P_t/σ^2 for different number N_A.

secrecy performance than the DSM-MRC scheme, no matter what the number of antennas or Q.

Fig. 6 shows the influence of the secrecy outage probability versus P_t/σ^2 of TAS-MRC and DSM-MRC schemes under different eavesdropping strategies, which Eve is equipped with single-antenna or multiple-antennas using selection combining (SC) and MRC strategies. With the increase of transmit power P_t, the cures of secrecy outage probability under the three eavesdropping strategies decreases, and converges to a fixed value under the interference constraint Q. Moreover, we can see from the figure that, similar to the previous analysis, Eve has the best eavesdropping effect by adopting MRC, SC takes the second place, and single antenna eavesdropping is the worst. In addition, we can find that TAS-MRC scheme is always better than DSM-MRC scheme.

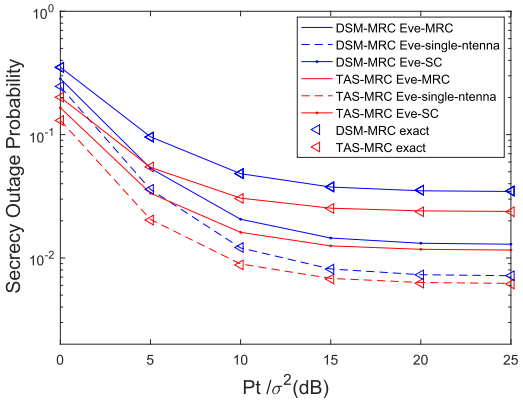

FIGURE 6. Secrecy outage probability for the TAS-MRC and DSM-MRC schemes under different eavesdropping strategies.

Fig. 7 shows the influence of the secrecy outage probability versus P_t/σ^2 of TAS-MRC and DSM-MRC schemes and the asymptotic expressions curves of the secrecy outage probability attained from (23) and (25) under the $\overline{\gamma}_B \to \infty$ and fixed $\overline{\gamma}_E$, respectively, where $\overline{\gamma}_E = 10$dB. We can see from the figure that the diversity order is the same of two schemes, which confirms the asymptotic results in (23) and (25). In addition, when the number of antennas of Alice or Bob

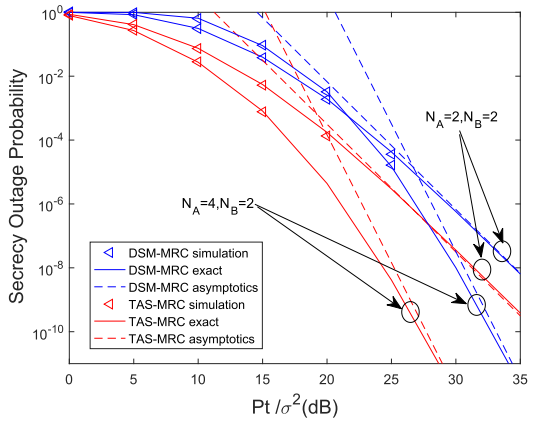

FIGURE 7. Exact and asymptotic secrecy outage probability for the TAS-MRC and DSM-MRC schemes under Scenario I.

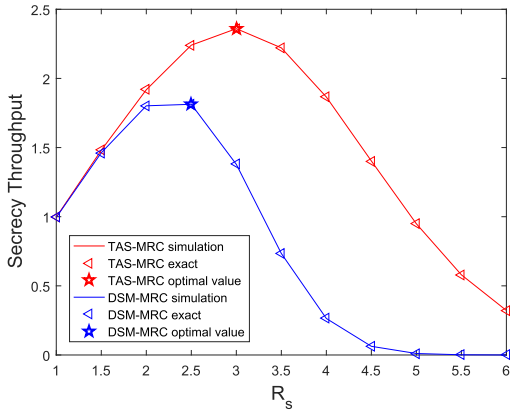

FIGURE 9. Secrecy outage probability of TAS-MRC and DSM-MRC schemes versus R_s.

is increased, the diversity gain increases, and the slope of the diversity order increases. And it shows that two schemes achieve the same secrecy diversity order of $N_A N_B$. Further, the TAS-MRC scheme always gets better secrecy performance than the DSM-MRC scheme. Moreover, the secrecy outage probability will be improved with N_A and N_B increase, which indicates that using the DSM or TAS schemes at Alice or MRC at Bob will enhance the secrecy array gain of CRNs by increaing the number of antennas.

Fig. 8 plots the influence of the secrecy outage probability versus P_t/σ^2 of the two schemes when $\overline{\gamma}_B/\overline{\gamma}_E = 1$. The asymptotic expressions of secrecy outage probability are achieved from (28) and (29) under the $\overline{\gamma}_B \to \infty$ and $\overline{\gamma}_E \to \infty$, respectively. The simulation results shows that the TAS-MRC scheme has better secrecy performance than DSM-MRC scheme. For fixed $\overline{\gamma}_B/\overline{\gamma}_E$, increasing N_A and N_B lead to reduce the values of secrecy outage probability. When P_t/σ^2 in high region, the asymptotic secrecy outage probability reaches the secrecy outage probability floor. Thus,

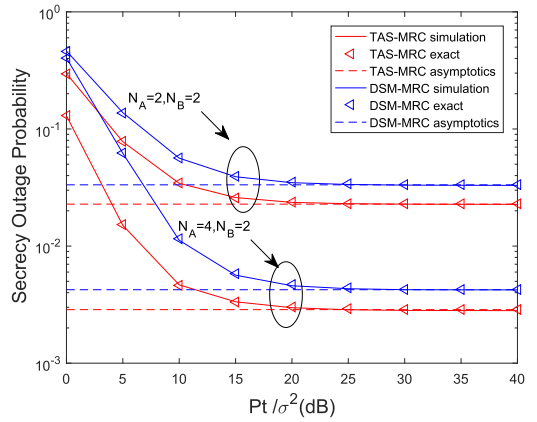

FIGURE 8. Exact and asymptotic secrecy outage probabilities for the TAS-MRC and DSM-MRC schemes under Scenario II with different values N_A and N_B.

the secrecy coding gain of TAS-MRC is better than that of DSM-MRC scheme, we can enhance the secrecy performance of CRNs by increasing the secrecy coding gain.

Fig. 9 plots the secrecy throughput versus R_s with TAS-MRC and DSM-MRC schemes when $N_A = 4$ and $N_B = 2$. In the figure, the theoretical analysis were obtained from (30) is the same as the simulation curves. We can clear see that the secrecy throughput of two schemes increases at the beginning, and then decreases with the increase of R_s. It shows that the two schemes have an optimal value R_s^{max} to make the secrecy throughput reach the maximum value. What is more, we observe that the system with TAS-MRC scheme can get higher secrecy throughput than DSM-MRC, while R_s^{max} can be obtained by global search.

VI. CONCLUSION

This paper investigated the secrecy performance of the cognitive MIMO wiretap networks with different antenna transmission schemes. Considering the influence of outdated CSI on the interference from Alice to PU, power control mechanism is adopted to guarantee the QoS of PU over Rayleigh channels. In addition, in order to solve the problems of ICI and IAS faced by traditional MIMO technology, DSM technology was introduced at the Alice to facilitate the modulation and demodulation at Bob without CSI. As a comparison, we also introduced TAS technology that requires feedback CSI to compare and select antennas at Alice. To assess the secrecy performance of the CRNs based on TAS-MRC and DSM-MRC schemes, the closed-form expressions for secrecy outage probability and secrecy throughput were derived. And we studied the influence of different transmission parameters on secrecy performance. Moreover, the diversity gain and coding gain of the CRNs were analyzed based on the asymptotic expression for secrecy outage probability. As the results, it demonstrates that DSM-MRC requires less CSI and is convenient for modulation and demodulation, but sacrifices some secrecy performance gains between two proposed schemes.

.

APPENDIX A

From (17), the secrecy outage probability of the TAS-MRC scheme can be expressed as

$$
\begin{aligned}
&P_{out}^{TAS-MRC}(R_s)\\
&=\int_0^{\infty} P_{out}(R_s|G) f_G(g) dg\\
&=\int_0^{\kappa\mu} \frac{1}{\lambda_{AP}} e^{-\frac{1}{\lambda_{AP}}g} dg \sum_{i=0}^{N_A} \binom{N_A}{i} (-1)^i \exp\left(-\frac{i\sigma^2(2^{Rs}-1)}{P_t\lambda_{AB}}\right)\\
&\quad\times \Theta_{N_B,i} \sum_{j=0}^{\phi} \binom{\phi}{j} \left(\frac{\sigma^2(2^{R_s}-1)}{P_t\lambda_{AB}}\right)^j \left(\frac{\sigma^2 2^{R_s}}{P_t\lambda_{AB}}\right)^{\phi-j}\\
&\quad\times \frac{1}{\Gamma(N_E)\left(\frac{P_t\lambda_{AE}}{\sigma^2}\right)^{N_E}} (N_E-1+\phi-j)!\\
&\quad\times \left(\frac{\sigma^2}{P_t\lambda_{AE}}+\frac{i\sigma^2 2^{R_s}}{P_t\lambda_{AB}}\right)^{-(N_E+\phi-j)} + \int_{\kappa\mu}^{\infty} \frac{1}{\lambda_{AP}} e^{-\frac{1}{\lambda_{AP}}g}\\
&\quad\times \sum_{i=0}^{N_A} \binom{N_A}{i} (-1)^i \exp\left(-\frac{i\sigma^2(2^{Rs}-1)}{\kappa Q\lambda_{AB}}g\right)\\
&\quad\times \Theta_{N_B,i} \sum_{j=0}^{\phi} \binom{\phi}{j} \left(\frac{\sigma^2(2^{R_s}-1)}{\kappa Q\lambda_{AB}}g\right)^j \left(\frac{\sigma^2 2^{R_s}}{\kappa Q\lambda_{AB}}g\right)^{\phi-j}\\
&\quad\times \frac{1}{\Gamma(N_E)\left(\frac{\kappa Q\lambda_{AE}}{\sigma^2 g}\right)^{N_E}} (N_E-1+\phi-j)!\\
&\quad\times \left(\frac{\sigma^2}{\kappa Q\lambda_{AE}}g+\frac{i\sigma^2 2^{R_s}}{\kappa Q\lambda_{AB}}g\right)^{-(N_E+\phi-j)} dg. \qquad (31)
\end{aligned}
$$

Then, substituting $f_G(g)$ in (31), the $P_{out}^{TAS-MRC}(R_s)$ can be get as (18) with the help of [31, Eq. (3.381.3)] and some mathematical integration operations.

APPENDIX B

From (21), the secrecy outage probability of the DSM-MRC scheme can be expressed as

$$
\begin{aligned}
&P_{out}(R_s)\\
&=\int_0^{\infty} P_{out}^{DSM-MRC}(R_s|G) f_G(g) dg\\
&=1-\int_0^{\kappa\frac{Q}{P_t}} \exp\left(-\frac{N_A\sigma^2(2^{R_s}-1)}{P_t\lambda_{AB}}\right) \frac{1}{\Gamma(N_AN_E)\left(\frac{P_t\lambda_{AE}}{N_A\sigma^2}\right)^{N_AN_E}}\\
&\quad\times \sum_{k=0}^{N_AN_B-1} \frac{1}{k!} \left(\frac{N_A\sigma^2}{P_t\lambda_{AB}}\right)^k \sum_{i=0}^{k} \binom{k}{i} \left(2^{R_s}-1\right)^{k-i} \left(2^{R_s}\right)^i\\
&\quad\times (N_AN_E-1+i)! \left(\frac{N_A\sigma^2 2^{R_s}}{P_t\lambda_{AB}}+\frac{N_A\sigma^2}{P_t\lambda_{AE}}\right)^{-N_AN_E-i} f_G(g) dg\\
&\quad-\int_{\kappa\frac{Q}{P_t}}^{\infty} exp\left(-\frac{N_A\sigma^2(2^{R_s}-1)}{\kappa Q\lambda_{AB}}g\right) \frac{1}{\Gamma(N_AN_E)\left(\frac{\kappa Q\lambda_{AE}}{N_A\sigma^2}g\right)^{N_AN_E}}\\
&\quad\times \sum_{k=0}^{N_AN_B-1} \frac{1}{k!} \left(\frac{N_A\sigma^2}{\kappa Q\lambda_{AB}}g\right)^k \sum_{i=0}^{k} \binom{k}{i} \left(2^{R_s}-1\right)^{k-i} \left(2^{R_s}\right)^i\\
&\quad\times (N_AN_E-1+i)! \left(\frac{N_A\sigma^2 2^{R_s}}{\kappa Q\lambda_{AB}}+\frac{N_A\sigma^2}{\kappa Q\lambda_{AE}}\right)^{-N_AN_E-i}\\
&\quad\times \left(\frac{\kappa Q}{g}\right)^{N_AN_E+i} f_G(g) dg. \qquad (32)
\end{aligned}
$$

Then, substituting $f_G(g)$ in (32), the desired $P_{out}^{DSM-MRC}(R_s)$ can be get as (22) with the help of [31, Eq. (3.381.3)] and some mathematical integration operations.

APPENDIX C

When $\overline{\gamma}_B \to \infty$, the conditional CDF of $\gamma_B^{TAS-MRC}$ can be desired as

$$
\begin{aligned}
&F_{\gamma_B}^{TAS-MRC}(x|G)\\
&\quad=\sum_{i=0}^{N_A} \binom{N_A}{i} (-1)^i \exp\left(-\frac{i\sigma^2 x}{P_s\lambda_{AB}}\right) \Theta_{N_B,i} \left(\frac{\sigma^2 x}{P_s\lambda_{AB}}\right)^{\phi}. \qquad (33)
\end{aligned}
$$

Then, the conditional PDF of $\gamma_E^{TAS-MRC}$ is desired as

$$
f_{\gamma_E}^{TAS-MRC}(x|G) = \frac{x^{N_E-1}}{\Gamma(N_E)\left(\frac{P_s\lambda_{AE}}{\sigma^2}\right)^{N_E}} \exp\left(-\frac{\sigma^2 x}{P_s\lambda_{AE}}\right). \qquad (34)
$$

Substituting (33) and (34) into (14), the asymptotic $P_{out}^{TAS-MRC}(R_s|G)$ can be desired as

$$
\begin{aligned}
&P_{out}^{TAS-MRC}(R_s|G)\\
&\quad=\sum_{i=0}^{N_A} \binom{N_A}{i} (-1)^i \exp\left(-\frac{i\sigma^2(2^{Rs}-1)}{P_s\lambda_{AB}}\right)\\
&\quad\times \Theta_{N_B,i} \sum_{j=0}^{\phi} \binom{\phi}{j} \left(\frac{\sigma^2(2^{R_s}-1)}{P_s\lambda_{AB}}\right)^j \left(\frac{\sigma^2 2^{R_s}}{P_s\lambda_{AB}}\right)^{\phi-j}\\
&\quad\times \frac{1}{\Gamma(N_E)\left(\frac{P_s\lambda_{AE}}{\sigma^2}\right)^{N_E}} (N_E-1+\phi-j)!\\
&\quad\times \left(\frac{\sigma^2}{P_s\lambda_{AE}}+\frac{i\sigma^2 2^{R_s}}{P_s\lambda_{AB}}\right)^{-(N_E+\phi-j)}. \qquad (35)
\end{aligned}
$$

Now, the desired result $P_{out}^{TAS-MRC}(R_s)$ based on $f_G(g)$ can be get as

$$
\begin{aligned}
&P_{out}^{TAS-MRC}(R_s)\\
&=\left(1-\exp\left(-\frac{\kappa u}{\lambda_{AP}}\right)\right) \sum_{i=0}^{N_A} \binom{N_A}{i} (-1)^i \exp\left(-\frac{i(2^{R_s}-1)}{\bar{\gamma}_B}\right)\\
&\quad\times \Theta_{N_B,i} \sum_{j=0}^{\varphi} \binom{\varphi}{j} \left(\frac{2^{R_s}-1}{\bar{\gamma}_B}\right)^j \left(\frac{2^{R_s}}{\bar{\gamma}_B}\right)^{\varphi-j}\\
&\quad\times \frac{1}{\Gamma(N_E)(\bar{\gamma}_E)^{N_E}} (N_E-1+\varphi-j)! \left(\frac{1}{\bar{\gamma}_E}+\frac{i2^{R_s}}{\bar{\gamma}_B}\right)^{-(N_E+\varphi-j)}
\end{aligned}
$$

$$+\frac{1}{\lambda_{AP}}\sum_{i=0}^{N_A}\binom{N_A}{i}(-1)^i\,\Theta_{N_B,i}\sum_{j=0}^{\varphi}\binom{\varphi}{j}\left(\frac{2^{R_s}-1}{\bar{\gamma}_B\kappa\mu}\right)^j$$
$$\times\left(\frac{2^{R_s}}{\bar{\gamma}_B\kappa\mu}\right)^{\varphi-j}\frac{1}{\Gamma(N_E)(\bar{\gamma}_E\kappa\mu)^{N_E}}(N_E-1+\varphi-j)!$$
$$\times\left(\frac{1}{\bar{\gamma}_E\kappa\mu}+\frac{i2^{R_s}}{\bar{\gamma}_B\kappa\mu}\right)^{-(N_E+\varphi-j)}\left(\frac{i(2^{Rs}-1)}{\bar{\gamma}_B\kappa\mu}+\frac{1}{\lambda_{AP}}\right)^{-j-1}$$
$$\times\Gamma\left(j+1,\left(\frac{i(2^{R_s}-1)}{\bar{\gamma}_B\kappa\mu}+\frac{1}{\lambda_{AP}}\right)\kappa\mu\right). \quad (36)$$

By using (36), $\Delta_{TAS-MRC}$ is given by (24).

APPENDIX D

As $\bar{\gamma}_B\to\infty$, the conditional CDF of $\gamma_B^{DSM-MRC}$ is approximated as

$$F_{\gamma_B^{DSM}}(x\,|G)\approx\frac{1}{(N_AN_B)!}\left(\frac{N_A\sigma^2x}{P_s\lambda_{AB}}\right)^{N_AN_B}. \quad (37)$$

Similarly, when $\gamma_E^{DSM-MRC}$ is fixed, the conditional PDF of $\gamma_E^{DSM-MRC}$ is desired as

$$f_{\gamma_E^{DSM}}(x\,|G)=\frac{x^{N_AN_E-1}}{\Gamma(N_AN_E)(\bar{\gamma}_E)^{N_AN_E}}\exp\left(-\frac{x}{\bar{\gamma}_E}\right). \quad (38)$$

Substituting (37) and (38) into (14), the conditional asymptotic secrecy outage probability based on DSM-MRC can be desired as

$$\begin{aligned}P_{out}^{DSM-MRC}(R_s\,|G)&=\int_0^\infty F_{\gamma_B^{DSM}}\left(2^{R_s}(1+x)-1\,|G\right)f_{\gamma_E^{DSM}}(x\,|G)\,dx\\&=\int_0^\infty\frac{1}{(N_AN_B)!}\left(\frac{N_A\sigma^2\left(2^{R_s}(1+x)-1\right)}{P_s\lambda_{AB}}\right)^{N_AN_B}\\&\quad\times\frac{x^{N_AN_E-1}}{\Gamma(N_AN_E)\left(\frac{\bar{\gamma}_E}{N_A}\right)^{N_AN_E}}\exp\left(-\frac{N_Ax}{\bar{\gamma}_E}\right)dx\\&=\frac{1}{(N_AN_B)!}\left(\frac{N_A\sigma^2}{P_s\lambda_{AB}}\right)^{N_AN_B}\frac{1}{\Gamma(N_AN_E)\left(\frac{\bar{\gamma}_E}{N_A}\right)^{N_AN_E}}\\&\quad\times\sum_{i=0}^{N_AN_B}\binom{N_AN_B}{i}\left(2^{R_s}-1\right)^{N_AN_B-i}2^{R_si}\\&\quad\times(N_AN_E+i-1)!\left(\frac{N_A}{\bar{\gamma}_E}\right)^{-(N_AN_E+i)}.\end{aligned} \quad (39)$$

Finally, the asymptotic expression for secrecy outage probability can be get as

$$\begin{aligned}P_{out}(R_s)&=\int_0^\infty P_{out}^{DSM-MRC}(R_s\,|G)f_G(g)\,dg\\&=\left(1-\exp\left(-\frac{\kappa\mu}{\lambda_{AP}}\right)\right)\frac{1}{(N_AN_B)!}\left(\frac{N_A}{\bar{\gamma}_B}\right)^{N_AN_B}\\&\quad\times\frac{1}{\Gamma(N_AN_E)(\bar{\gamma}_E)^{N_AN_E}}\\&\quad\times\sum_{i=0}^{N_AN_B}\binom{N_AN_B}{i}\left(2^{R_s}-1\right)^{N_AN_B-i}2^{R_si}\\&\quad\times(N_AN_E+i-1)!\left(\frac{1}{\bar{\gamma}_E}\right)^{-(N_AN_E+i)}\\&\quad+\frac{1}{\lambda_{AP}}\frac{1}{(N_AN_B)!}\left(\frac{N_A}{\mu\kappa\bar{\gamma}_B}\right)^{N_AN_B}\frac{1}{\Gamma(N_AN_E)(\bar{\gamma}_E)^{N_AN_E}}\\&\quad\times\sum_{i=0}^{N_AN_B}\binom{N_AN_B}{i}\left(2^{R_s}-1\right)^{N_AN_B-i}2^{R_si}(N_AN_E+i-1)!\\&\quad\times\left(\frac{1}{\bar{\gamma}_E}\right)^{-(N_AN_E+i)}\left(\frac{1}{\lambda_{AP}}\right)^{-N_AN_B-1}\Gamma\left(N_AN_B+1,\frac{\mu\kappa}{\lambda_{AP}}\right).\end{aligned} \quad (40)$$

By using (40), $\Delta_{DSM-MRC}$ is given by (26).

REFERENCES

[1] J. Mitola and G. Q. Maguire, "Cognitive radio: Making software radios more personal," *IEEE Pers. Commun.*, vol. 6, no. 4, pp. 13–18, Aug. 1999.

[2] A. Ali and W. Hamouda, "Advances on spectrum sensing for cognitive radio networks: Theory and applications," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1277–1304, 2nd Quart., 2017.

[3] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

[4] H. Wen, S. Li, X. Zhu, and L. Zhou, "A framework of the PHY-layer approach to defense against security threats in cognitive radio networks," *IEEE Netw.*, vol. 27, no. 3, pp. 34–39, May 2013.

[5] Y. Zou, J. Zhu, L. Yang, Y.-C. Liang, and Y.-D. Yao, "Securing physical-layer communications for cognitive radio networks," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 48–54, Sep. 2015.

[6] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[7] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2nd Quart., 2019.

[8] M. Yang, D. Guo, Y. Huang, T. Q. Duong, and B. Zhang, "Physical layer security with threshold-based multiuser scheduling in multi-antenna wireless networks," *IEEE Trans. Commun.*, vol. 64, no. 12, pp. 5189–5202, Dec. 2016.

[9] B. Wang, P. Mu, and Z. Li, "Artificial-noise-aided beamforming design in the MISOME wiretap channel under the secrecy outage probability constraint," *IEEE Trans. Wireless Commun.*, vol. 16, no. 11, pp. 7207–7220, Nov. 2017.

[10] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, Jun. 2012.

[11] Z. Cao, X. Ji, J. Wang, S. Zhang, Y. Ji, and J. Wang, "Security-reliability tradeoff analysis for underlay cognitive two-way relay networks," *IEEE Trans. Wireless Commun.*, vol. 18, no. 12, pp. 6030–6042, Dec. 2019.

[12] F. Zhu and M. Yao, "Improving physical-layer security for CRNs using SINR-based cooperative beamforming," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1835–1841, Mar. 2016.

[13] H. A. Shah and I. Koo, "A novel physical layer security scheme in OFDM-based cognitive radio networks," *IEEE Access*, vol. 6, pp. 29486–29498, 2018.

[14] G. Oliveira, E. Fernandez, S. Mafra, and S. Montejo-Sanchez, "Physical layer security in cognitive radio networks using improper Gaussian signaling," *IEEE Commun. Lett.*, vol. 22, no. 9, pp. 1886–1889, Sep. 2018.

[15] H. Lei, J. Zhang, K.-H. Park, I. S. Ansari, G. Pan, and M.-S. Alouini, "Secrecy performance analysis of SIMO underlay cognitive radio systems with outdated CSI," *IET Commun.*, vol. 11, no. 12, pp. 1961–1969, Aug. 2017.

[16] T. Zhang, Y. Cai, Y. Huang, T. Q. Duong, and W. Yang, "Secure transmission in cognitive MIMO relaying networks with outdated channel state information," *IEEE Access*, vol. 4, pp. 8212–8224, 2016.
[17] H. Lei, H. Luo, K.-H. Park, I. S. Ansari, W. Lei, G. Pan, and M.-S. Alouini, "On secure mixed RF-FSO systems with TAS and imperfect CSI," *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 4461–4475, Jul. 2020.
[18] H. Lei, J. Zhang, K.-H. Park, P. Xu, I. S. Ansari, G. Pan, B. Alomair, and M.-S. Alouini, "On secure NOMA systems with transmit antenna selection schemes," *IEEE Access*, vol. 5, pp. 17450–17464, 2017.
[19] Y. Bian, X. Cheng, M. Wen, L. Yang, H. V. Poor, and B. Jiao, "Differential spatial modulation," *IEEE Trans. Veh. Technol.*, vol. 64, no. 7, pp. 3262–3268, Jul. 2015.
[20] R. Y. Mesleh, H. Haas, S. Sinanovic, C. W. Ahn, and S. Yun, "Spatial modulation," *IEEE Trans. Veh. Technol.*, vol. 57, no. 4, pp. 2228–2241, Jul. 2008.
[21] E. Basar, "Index modulation techniques for 5G wireless networks," *IEEE Commun. Mag.*, vol. 54, no. 7, pp. 168–175, Jul. 2016.
[22] Y. Wang, T. Zhang, W. Yang, J. Guo, Y. Liu, and X. Shang, "Secure transmission for differential quadrature spatial modulation with artificial noise," *IEEE Access*, vol. 7, pp. 7641–7650, 2019.
[23] M. Song, C. Xin, Y. Zhao, and X. Cheng, "Dynamic spectrum access: From cognitive radio to network radio," *IEEE Wireless Commun.*, vol. 19, no. 1, pp. 23–29, Feb. 2012.
[24] H. Lei, C. Gao, I. S. Ansari, Y. Guo, Y. Zou, G. Pan, and K. A. Qaraqe, "Secrecy outage performance of transmit antenna selection for MIMO underlay cognitive radio systems over Nakagami-*m* channels," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2237–2250, Mar. 2017.
[25] T. Zhang, Y. Huang, Y. Cai, C. Zhong, W. Yang, and G. K. Karagiannidis, "Secure multiantenna cognitive wiretap networks," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 4059–4072, May 2017.
[26] W. Zeng, Y. R. Zheng, and C. Xiao, "Multiantenna secure cognitive radio networks with finite-alphabet inputs: A global optimization approach for precoder design," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 3044–3057, Apr. 2016.
[27] H. Zhao, Y. Tan, G. Pan, Y. Chen, and N. Yang, "Secrecy outage on transmit antenna Selection/Maximal ratio combining in MIMO cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 10236–10242, Dec. 2016.
[28] M. Qin, S. Yang, H. Deng, and M. H. Lee, "Enhancing security of primary user in underlay cognitive radio networks with secondary user selection," *IEEE Access*, vol. 6, pp. 32624–32636, 2018.
[29] Z. Xiang, W. Yang, G. Pan, Y. Cai, and Y. Song, "Physical layer security in cognitive radio inspired NOMA network," *IEEE J. Sel. Topics Signal Process.*, vol. 13, no. 3, pp. 700–714, Jun. 2019.
[30] Y. Huang, F. S. Al-Qahtani, C. Zhong, Q. Wu, J. Wang, and H. M. Alnuweiri, "Cognitive MIMO relaying networks with primary User's interference and outdated channel state information," *IEEE Trans. Commun.*, vol. 62, no. 12, pp. 4241–4254, Dec. 2014.
[31] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. San Diego, CA, USA: Academic, 2007.
[32] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
[33] J. Xing, X. Zhang, J. Wang, Z. Zhang, and W. Wang, "Performance analysis of cognitive relay networks with imperfect channel knowledge over Nakagami-m fading channels," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Istanbul, Turkey, Apr. 2014, pp. 839–844.
[34] J. Chen, J. Si, Z. Li, and H. Huang, "On the performance of spectrum sharing cognitive relay networks with imperfect CSI," *IEEE Commun. Lett.*, vol. 16, no. 7, pp. 1002–1005, Jul. 2012.
[35] K. Ho-Van, "Exact outage analysis of underlay cooperative cognitive networks with reactive relay selection under imperfect channel information," *Wireless Pers. Commun.*, vol. 84, no. 1, pp. 565–585, 2015.
[36] Z. Yi and I.-M. Kim, "Diversity order analysis of the decode-and-forward cooperative networks with relay selection," *IEEE Trans. Wireless Commun.*, vol. 7, no. 5, pp. 1792–1799, May 2008.
[37] M. Z. Win, G. Chrisikos, and N. R. Sollenberger, "Performance of RAKE reception in dense multipath channels: Implications of spreading bandwidth and selection diversity order," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 8, pp. 1516–1525, Aug. 2000.
[38] S. Wei, "Diversity–multiplexing tradeoff of asynchronous cooperative diversity in wireless networks," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 4150–4172, Nov. 2007.
[39] J. Hu, Y. Cai, N. Yang, and W. Yang, "A new secure transmission scheme with outdated antenna selection," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 11, pp. 2435–2446, Nov. 2015.

YONG CHEN received the B.S. degree in communications engineering from Xiamen University, Xiamen, China, in 2018. He is currently pursuing the M.S. degree in information and communications engineering with the Army Engineering University of PLA, Nanjing, China. His research interests include cognitive radio systems, NOMA systems, and physical layer security.

TAO ZHANG received the B.S. degree in communications engineering and the Ph.D. degree in communications and information systems from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2011 and 2016, respectively. Since 2017, he has been an Engineer with The Sixty-third Research Institute, National University of Defense Technology, Nanjing. His current research interests include cooperative communications, wireless sensor networks, physical layer security, and cognitive radio systems.

XIAOQIANG QIAO received the B.S. and M.S. degrees from the PLA University of Science and Technology, Nanjing, China, in 2002 and 2005, respectively. He is currently a Senior Engineer with The Sixty-third Research Institute, National University of Defense Technology. His research interests include electromagnetic spectrum management, spectrum security, and communication anti-jamming.

HAO WU received the M.S. degree in communication engineering from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2008, where he is currently pursuing the Ph.D. degree in systems. He is also an Associate Professor with The Sixty-third Research Institute, National University of Defense Technology. His current research interests include spectrum sensing and signal processing in communications.

JIANG ZHANG received the Ph.D. degree in communications and information systems from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2013. Since 2014, he has been an Engineer with The Sixty-third Research Institute, National University of Defense Technology, Nanjing. His current research interests include blind sources separation, anti-jamming communication, and cognitive radio systems.