EURASIP Journal on Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

Performance of opportunistic scheduling for physical layer security with transmit antenna selection

Anish Prasad Shrestha and Kyung Sup Kwak*

Abstract

We introduce an opportunistic scheduling to enhance the physical layer security with transmit antenna selection (TAS) in multiuser environment. We consider a wireless communication system composed of a single transmitter and multiple legitimate users in the presence of several eavesdroppers with each node having multiple antennas under quasi-static Rayleigh fading channel. The transmitter selects the best transmitting antenna and the best user to maximize signal-to-noise ratio (SNR) at the selected user. The user and eavesdropper can employ either selection combining (SC) or maximal ratio combining (MRC) to combine the received signals. New closed-form expressions for probability of positive secrecy and outage are derived. Moreover, asymptotic analysis reveals the outage diversity gain and array gain for the proposed scheme. The impact of number of users, eavesdroppers, and antennas on secrecy performance are clearly demonstrated with mathematical analysis and numerical results.

Keywords: Opportunistic scheduling; Transmit antenna selection; Maximal ratio combining; Selection combining; Secrecy outage probability

1 Introduction

The security risks are inherent in any wireless network due to its underlying transmission medium, the airwave, which is exposed to all sorts of unwanted eavesdroppers. Traditionally, cryptographic algorithms are applied at the upper layer to secure information. However, physical layer (PHY) security has recently gained considerable attention as an alternative option to secure information besides the traditional cryptographic schemes. It can exploit the uncorrelated nature of the wireless medium for enhancing the security of wireless systems. The pioneering work in [1] presented that a noisy communication channel offers opportunities for non-zero rate secure communication when the eavesdroppers' channel is on average a degraded version of the main channel. This work was further extended in [2] to characterize the non-degraded channel. The perfect secrecy capacity was defined in [3] as the difference between the capacity of main channel and wiretap channel given that the capacity of the former is greater than the latter one under Gaussian channel. The secrecy capacity will provide the highest value of communication rate for which coding schemes can be designed ensuring the perfect secrecy. Moreover, the existence of the perfect secrecy in wiretap channels was shown in [4] even when the eavesdropper has a better average signal-to-noise ratio (SNR) than the legitimate receiver.

Several aspects of wireless communication field have been studied to improve physical layer security, such as cooperative networks [5,6], multiaccess channel [7], outdated channel state information (CSI) [8,9], channel estimation [10], and cognitive radio [11]. In recent years, usage of diversity has emerged as a common technique to enhance PHY security. Several papers exist in literature [12-19] which employ either transmit or receive diversity to improve PHY security. In [12], the receive diversity technique was studied where both legitimate user and eavesdropper employ maximal ratio combining (MRC). The authors showed that the use of multiple receive antennas can enhance security and that the secrecy outage probability is a function of the ratio between the number of receive antennas at user and

*Correspondence: kskwak@inha.ac.kr
UWB Wireless Communication Research Center, Inha University, Yunghyeon-dong, Nam-gu, Incheon 706-142, South Korea

eavesdropper. Further new results were provided for MRC technique under correlated channels in [13]. The comparison between selection combining (SC) and MRC at eavesdropper was studied in [14]. The authors illustrated that MRC at eavesdropper severely degrades the performance compared to SC at eavesdropper. Beamforming technique is studied in [15] for minimizing the transmit power to a prespecified signal-to-interference-plus-noise-ratio (SINR) at the receiver. However, it should be noted that the transmission side can be highly complex as well as the cost may rise with the increase in the number of antennas. To overcome such issues, transmit antenna selection (TAS) has been proposed in [16-19] which also exploits transmit diversity at the expense of a generally acceptable loss in performance. It uses a single radio frequency (RF) chain instead of several parallel RF sections, which reduces cost, complexity, power consumption, and size.

In [16], performance of TAS was examined in the presence of single receiver and eavesdropper both equipped with single antenna. The authors further extended the work in [17] to a scenario consisting of a sophisticated multiple antenna eavesdropper employing MRC. In [18], use of TAS for security enhancement was examined where the receiver and eavesdropper can employ either MRC or SC under Nakagami-m fading channels. The superiority of MRC over SC was established by the authors. Performance of TAS with antenna correlation at the receiver and eavesdropper has been studied in [19]. The authors demonstrated that when the average SNR of the main channel is at medium and high levels, higher correlation at the receiver exerts more detrimental effects on secrecy than higher correlation at the eavesdropper. Opportunistic scheduling policy for PHY security has been discussed in [20], but the authors have addressed only MAC layer policies.

In this paper, we consider a single transmitter with multiple active users and several passive eavesdroppers each equipped with multiple antennas in contrast to [16-18] and [20]. We propose an opportunistic scheduling along with TAS at transmitter. A similar case with single eavesdropper is analyzed in [21]. However, we extend the work in [21] to the case of multiple non-colluding eavesdroppers and receivers which can employ either MRC or SC. MRC may be employed to maximize the SNR as it is an optimum combining technique, while SC may be employed for its simplicity. As different users experience different channel environments at a given moment, an opportunistic scheduling can maximize the transmission data rate with an exactly known CSI of all users [22]. With such multiuser diversity, opportunistic scheduling can be a promising technique to improve PHY security where the secrecy capacity is severely limited by SNR of eavesdroppers. In addition, use of TAS with MRC or SC further improves the performance with transmit diversity and receive diversity, respectively. Overall, the proposed scheme allows simultaneous exploitation of multiuser diversity, transmit diversity, and receive diversity.

Notation The superscript $^{\mathrm{T}}$ denotes transposition; $E\{\cdot\}$ denotes statistical expectation; $\mathbf{I}_N$ is the $N \times N$ identity matrix; $\| \mathbf{x} \|$ denotes the norm of a complex valued vector $\mathbf{x}$, i.e., $\sqrt{\mathbf{x}^H\mathbf{x}}$; $\mathcal{CN}(\mu, \sigma^2)$ denotes the complex Gaussian distribution with mean μ and variance σ^2; $P(x)$ denotes the probability of an event x.

2 Proposed scheme

2.1 System model

We consider a wireless network composed of one transmitter referred to as Alice, K as the number of users and W as the number of eavesdroppers as shown in Figure 1. Alice is equipped with L_{A} antennas while each legitimate user and eavesdropper are equipped with L_{B} and L_{E} antennas, respectively. We assume all channels are quasi-static Rayleigh fading. We also assume that there exists a feedback channel between each legitimate user and the transmitter. At the legitimate receiver side, each user selects the best transmit antenna having the highest channel SNR. Each user feedbacks the selected antenna index to Alice. The scheduler at Alice finally selects a single user with corresponding indexed antenna having highest SNR values out of K users. We refer the single selected user as Bob. On the other hand, we consider that Alice possesses only average SNR and no other information about the channel state of eavesdroppers. Moreover, all the channels are considered to be mutually independent. From the eavesdroppers's point of view, the opportunistically selected single best user along with optimum TAS scheme appears to be a random strategy, as the main channel between Bob and Alice and the wiretap channel between eavesdroppers and Alice are uncorrelated. We need to consider the eavesdropper with maximum possible SNR link for our analysis as it denotes the maximal information leakage. We refer the eavesdropper with maximum SNR as Eve from herein.

The message block S is encoded into the codeword $\mathbf{c} = [c(1), .., c(i), .., c(n)]$. The codeword is designed in such a way that it is suitable to be transmitted over the selected channel. We focus on measuring the achievable level of secrecy rather than the actual code design. The channel is assumed to be power limited in the sense that $\frac{1}{n}\Sigma_{i=1}^{n} E\left\{|c(i)|^2\right\} = P$ where P is the average transmit signal power [13].

Alice selects Bob to achieve the largest post-processing SNR when selecting the best transmit antenna based on the information provided by each legitimate users through their respective feedback channels. MRC technique at Bob will combine the multiple received signals from different receiving antennas according to the gain of each channel.

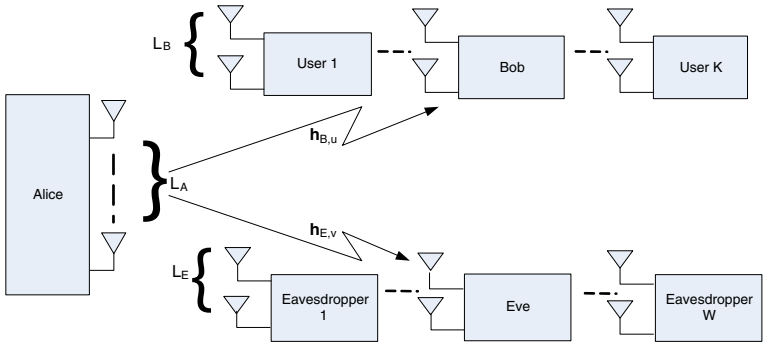

Figure 1 System model for secure opportunistic scheduling with TAS in presence of multiple eavesdroppers.

The received signal at Bob in this case can be expressed as

$$\mathbf{y}_{\mathrm{B}}^{\mathrm{MRC}}(i) = \mathbf{h}_{B,u}c(i) + \mathbf{n}_{B,u}, \tag{1}$$

where $\mathbf{h}_{B,u} = [h_{B,1}, h_{B,2}, ..., h_{B,L_{\mathrm{B}}}]^{\mathrm{T}}$ is a complex channel vector and $\mathbf{n}_{B,u} \sim \mathcal{CN}(\mathbf{0}, \sigma_B^2 \mathbf{I}_{L_{\mathrm{B}}})$. From (1), the instantaneous SNR of Bob with MRC is given by $\gamma_{\mathrm{B}}^{\mathrm{MRC}} = \frac{\|h_{B,u}\|^2 P}{\sigma_B^2}$.

Under this scenario, Eve can apply either MRC or SC to decode the intercepted signal. The received signal for Eve by applying MRC can be written as

$$\mathbf{y}_{\mathrm{E}}^{\mathrm{MRC/MRC}}(i) = \mathbf{h}_{E,v}c(i) + \mathbf{n}_{E,v}, \tag{2}$$

where $\mathbf{h}_{E,v} = [h_{E,1}, h_{E,2}, ..., h_{E,L_{\mathrm{E}}}]^{\mathrm{T}}$ is a complex channel vector and $\mathbf{n}_{E,v} \sim \mathcal{CN}(\mathbf{0}, \sigma_E^2 \mathbf{I}_{L_{\mathrm{E}}})$. From (2), the instantaneous SNR of Eve is given by $\gamma_{\mathrm{E}}^{\mathrm{MRC/MRC}} = \frac{\|h_{E,v}\|^2 P}{\sigma_E^2}$. On the other hand, the received signal for Eve by applying SC can be written as

$$y_{\mathrm{E}}^{\mathrm{MRC/SC}}(i) = h_E c(i) + n_E, \tag{3}$$

where h_E is a complex channel coefficient and n_E is additive white Gaussian noise (AWGN) with noise variance σ_E^2. From (3), the instantaneous SNR of Eve is given by $\gamma_{\mathrm{E}}^{\mathrm{MRC/SC}} = \frac{|h_E|^2 P}{\sigma_E^2}$.

Considering the simplicity and cost effectiveness, Bob can employ SC instead of MRC. The received signal at Bob for such scenario can be expressed as

$$y_{\mathrm{B}}^{\mathrm{SC}}(i) = g_B c(i) + n_B, \tag{4}$$

where g_B is a complex channel coefficient and n_B is AWGN with noise variance σ_B^2. The instantaneous SNR of Bob with SC is given by $\gamma_B^{SC} = \frac{|g_B|^2 P}{\sigma_B^2}$.

As mentioned above, Eve can apply either MRC or SC to decode the messages under this scenario as well. For Bob with SC, the received signal at Eve while applying MRC can be expressed as

$$\mathbf{y}_{\mathrm{E}}^{\mathrm{SC/MRC}}(i) = \mathbf{g}_{E,v}c(i) + \mathbf{n}_{E,v}, \tag{5}$$

where $\mathbf{g}_{E,v} = [g_{E,1}, g_{E,2}, ..., g_{E,L_{\mathrm{E}}}]^{\mathrm{T}}$ is a complex channel vector and $\mathbf{n}_{E,v} \sim \mathcal{CN}(0, \sigma_E^2 \mathbf{I}_{L_{\mathrm{E}}})$. From (5), the instantaneous SNR of Eve for this scheme is given by $\gamma_{\mathrm{E}}^{\mathrm{SC/MRC}} = \frac{\|g_{E,v}\|^2 P}{\sigma_E^2}$.

Likewise, the received signal for Eve by applying SC can be written as

$$y_{\mathrm{E}}^{\mathrm{SC/SC}}(i) = g_E c(i) + n_E, \tag{6}$$

where g_E is a complex channel coefficient and n_E is AWGN with noise variance σ_E^2. From (6), the instantaneous SNR of Eve with SC/SC is given by $\gamma_{\mathrm{E}}^{\mathrm{SC/SC}} = \frac{|g_E|^2 P}{\sigma_E^2}$.

2.2 SNR distribution

We deduce the probability density function (PDF) and cumulative distribution function (CDF) in this section to facilitate the analysis of secrecy performance. The PDF and CDF of instantaneous SNR for the kth user employing MRC with L_{B} antennas can be expressed in the form of Chi-square distribution and Gamma function [23] respectively as

$$f_k^{\mathrm{MRC}}(\gamma_k) = \frac{\gamma_k^{L_{\mathrm{B}}-1}}{\bar{\gamma}_B^{L_{\mathrm{B}}} \Gamma(L_{\mathrm{B}})} e^{-\frac{\gamma_k}{\bar{\gamma}_B}}, \tag{7}$$

$$\begin{aligned} F_k^{\mathrm{MRC}}(\gamma_k) &= 1 - \frac{\Gamma\left(L_{\mathrm{B}}, \frac{\gamma_k}{\bar{\gamma}_B}\right)}{\Gamma(L_{\mathrm{B}})} \\ &= 1 - e^{-\frac{\gamma_k}{\bar{\gamma}_B}} \sum_{i=0}^{L_{\mathrm{B}}-1} \frac{1}{i!} \left(\frac{\gamma_k}{\bar{\gamma}_B}\right)^i, \end{aligned} \tag{8}$$

where $\Gamma(\cdot)$ and $\Gamma(\cdot,\cdot)$ are complete and incomplete gamma functions, respectively (Equations (8.339.1) and (8.352.2) in [24]).

Using order statistics [25], we can derive the CDF and PDF of SNR for MRC at Bob as follows

$$F_{\mathrm{B}}^{\mathrm{MRC}}(\gamma_B) = \left[F_k^{\mathrm{MRC}}(\gamma_B)\right]^{KL_{\mathrm{A}}} = \sum_{m=0}^{KL_{\mathrm{A}}} \sum_{i=0}^{m(L_{\mathrm{B}}-1)} \binom{KL_{\mathrm{A}}}{m} \frac{(-1)^m a_i}{\bar{\gamma}_B^i} \gamma_B^i e^{-\gamma_B \frac{m}{\bar{\gamma}_B}}, \tag{9}$$

$$f_{\mathrm{B}}^{\mathrm{MRC}}(\gamma_B) = KL_{\mathrm{A}} \left[F_k^{\mathrm{MRC}}(\gamma_B)\right]^{KL_{\mathrm{A}}-1} f_k^{\mathrm{MRC}}(\gamma_B) = KL_{\mathrm{A}} \sum_{m=0}^{KL_{\mathrm{A}}-1} \sum_{i=0}^{m(L_{\mathrm{B}}-1)} \binom{KL_{\mathrm{A}}-1}{m} \times \frac{(-1)^m a_i}{\bar{\gamma}_B^{i+L_{\mathrm{B}}} \Gamma(L_{\mathrm{B}})} \gamma_B^{L_{\mathrm{B}}+i-1} e^{-\gamma_B \alpha}, \tag{10}$$

where $\bar{\gamma}_B$ is the average SNR of Bob's channel given by $\frac{P}{\sigma_B^2} E\left\{\| \mathbf{h}_{B,u} \|^2\right\}$ and $\alpha = \frac{m+1}{\bar{\gamma}_B}$. Likewise, a_i denotes the coefficient of $\left(\frac{\gamma_B}{\bar{\gamma}_B}\right)^i$ in the expansion of $\left\{\sum_{i=0}^{(L_{\mathrm{B}}-1)} \frac{1}{i!} \left(\frac{\gamma_B}{\bar{\gamma}_B}\right)^i\right\}^m$, where a_i can be recursively calculated by

$$\begin{aligned} &a_0 = 1, \qquad a_1 = m, \\ &a_i = \frac{1}{i} \sum_{t=1}^{\min(i, L_{\mathrm{B}}-1)} \frac{t(m+1)-i}{t!} a_{i-t}, \ \textit{for } 2 \le i < m(L_{\mathrm{B}}-1), \\ &a_i = \frac{1}{[(L_{\mathrm{B}}-1)!]^m}, \ \textit{for } i = m(L_{\mathrm{B}}-1). \end{aligned} \tag{11}$$

The expressions in (9) and (10) can be obtained by using binomial expansion at first which results the term with power series raised to power $\left\{\sum_{i=0}^{(L_{\mathrm{B}}-1)} \frac{1}{i!} \left(\frac{\gamma_B}{\bar{\gamma}_B}\right)^i\right\}^m$. The power series can be further expanded by using Equation 0.314 in [24]. This finite series expansion is possible as the first term within incomplete gamma function in (8), i.e., the number of antennas at Bob L_{B} has always integer value [26].

In a similar fashion, by using the order statistics, we can derive the CDF and PDF of Bob's channel for SC case as

$$F_{\mathrm{B}}^{\mathrm{SC}}(\gamma_B) = \sum_{n=0}^{KL_{\mathrm{A}}L_{\mathrm{B}}} \binom{KL_{\mathrm{A}}L_{\mathrm{B}}}{n} (-1)^n e^{-\gamma_B \frac{n}{\bar{\gamma}_B}}, \tag{12}$$

$$f_{\mathrm{B}}^{\mathrm{SC}}(\gamma_B) = \frac{KL_{\mathrm{A}}L_{\mathrm{B}}}{\bar{\gamma}_B} \sum_{n=0}^{KL_{\mathrm{A}}L_{\mathrm{B}}-1} \binom{KL_{\mathrm{A}}L_{\mathrm{B}}-1}{n} (-1)^n e^{-\gamma_B \frac{n+1}{\bar{\gamma}_B}}. \tag{13}$$

The selection of best antenna at Alice seems random from Eve's point of view. As there are W number of eavesdroppers in the network each equipped with L_{E} antennas, the diversity for Eve limits to multiuser diversity and receive diversity while there is no transmit diversity. The PDF and CDF for Eve employing MRC irrespective of MRC or SC at Bob can be obtained using similar order statistics and mathematical steps as in (9) and (10) by replacing $KL_{\mathrm{A}} = W$ and $L_{\mathrm{B}} = L_{\mathrm{E}}$, respectively which is shown below:

$$F_E^{\mathrm{MRC}}(\gamma_E) = \sum_{p=0}^{W} \sum_{j=0}^{p(L_{\mathrm{E}}-1)} \binom{W}{p} \frac{(-1)^p b_j}{\bar{\gamma}_E^j} \gamma_E^j e^{-\gamma_E \frac{p}{\bar{\gamma}_E}}, \tag{14}$$

$$f_E^{\mathrm{MRC}}(\gamma_E) = W \sum_{p=0}^{W-1} \sum_{j=0}^{p(L_{\mathrm{E}}-1)} \binom{W-1}{p} \times \frac{(-1)^p b_j}{\bar{\gamma}_E^{j+L_{\mathrm{E}}} \Gamma(L_{\mathrm{E}})} \gamma_E^{L_{\mathrm{E}}+j-1} e^{-\gamma_E \beta}, \tag{15}$$

where b_j is the coefficient of $\left(\frac{\gamma_E}{\bar{\gamma}_E}\right)^j$ in the expansion of $\left[\sum_{j=0}^{L_{\mathrm{E}}-1} \frac{1}{j!} \left(\frac{\gamma_E}{\bar{\gamma}_E}\right)^j\right]^p$, $\beta = \left(\frac{p+1}{\bar{\gamma}_E}\right)$; and $\bar{\gamma}_E$ is average SNR of the eavesdroppers' channel. We note that the coefficient b_j can be recursively calculated as a_i described in (11).

Finally, the CDF and PDF of Eve with SC can be obtained as in (12) and (13), respectively, which is shown below:

$$F_{\mathrm{E}}^{\mathrm{SC}}(\gamma_E) = \sum_{q=0}^{WL_{\mathrm{E}}} \binom{WL_{\mathrm{E}}}{q} (-1)^q e^{-\gamma_E \frac{q}{\bar{\gamma}_E}}, \tag{16}$$

$$f_{\mathrm{E}}^{\mathrm{SC}}(\gamma_E) = \frac{WL_{\mathrm{E}}}{\bar{\gamma}_E} \sum_{q=0}^{WL_{\mathrm{E}}} \binom{WL_{\mathrm{E}}-1}{q} (-1)^q e^{-\gamma_E \frac{q+1}{\bar{\gamma}_E}}. \tag{17}$$

2.3 Secrecy capacity

From [3], the secrecy capacity over Gaussian wiretap channel is given by the difference between the main channel capacity and wiretap channel capacity. Since block-faded channel is assumed in our system model, both the channels can be regarded as complex Gaussian channels. The capacity of Bob's channel is given by

$$C_{\mathrm{B}} = \log_2(1 + \max_{1 \le i \le KL_{\mathrm{A}}} \gamma_{B_i}) = \log_2(1 + \gamma_B). \tag{18}$$

Similarly, the capacity of Eve's channel is given by

$$C_{\mathrm{E}} = \log_2(1 + \max_{1 \le j \le W} \gamma_{E_j}) = \log_2(1 + \gamma_E), \tag{19}$$

where γ_B and γ_E are the instantaneous SNR of Bob and Eve, respectively, regardless of any receive diversity scheme.

Hence, under perfect secrecy constraint, the instantaneous secrecy capacity of Bob in the presence of multiple

eavesdroppers equipped with multiple antennas can be expressed as

$$C_s = \begin{cases} C_B - C_E, & \text{if } \gamma_B \geq \gamma_E \\ 0, & \text{otherwise.} \end{cases} \tag{20}$$

3 Performance metrics

3.1 Positive secrecy probability

Since the main channel between Alice and Bob is independent from the wiretap channel between Alice and Eve, the existence probability of a non-zero secrecy capacity can be calculated as

$$\begin{aligned} P(C_s > 0) &= P(\gamma_B > \gamma_E) \\ &= \int_0^\infty \int_0^{\gamma_B} f_B(\gamma_B) f_E(\gamma_E) d\gamma_E d\gamma_B \\ &= \int_0^\infty f_B(\gamma_B) F_E(\gamma_B) d\gamma_B \end{aligned} \tag{21}$$

where $f_B(\cdot)$ and $F_E(\cdot)$ are the PDF and CDF of γ_B and γ_E, respectively. As we have already derived the PDF of γ_B and CDF of γ_E for respective schemes in Section 2.2, the probability of positive secrecy for each scheme can be easily derived by simply substituting the values and using Equation 3.351.3 in [24] as shown in (22) to (25):

$$\begin{aligned} P(C_s > 0)^{\text{MRC/MRC}} = KL_A \sum_{m=0}^{KL_A-1} \sum_{i=0}^{m(L_B-1)} \binom{KL_A - 1}{m} \\ \times \frac{(-1)^m a_i}{\bar{\gamma}_B^{L_B+i} \Gamma(L_B)} \sum_{p=0}^{W} \sum_{j=0}^{p(L_E-1)} \binom{W}{p} (-1)^p \\ \times \frac{b_j}{\bar{\gamma}_E^j} \Gamma(L_B + i + j) \left(\frac{m+1}{\bar{\gamma}_B} + \frac{p}{\bar{\gamma}_E} \right)^{-L_B - i - j}, \end{aligned} \tag{22}$$

$$\begin{aligned} P(C_s > 0)^{\text{MRC/SC}} = KL_A \sum_{m=0}^{KL_A-1} \sum_{i=0}^{m(L_B-1)} \binom{KL_A - 1}{m} \frac{(-1)^m a_i}{\bar{\gamma}_B^{L_B+i} \Gamma(L_B)} \\ \times \sum_{q=0}^{WL_E} \binom{WL_E}{q} (-1)^q \Gamma(L_B + i) \\ \times \left(\frac{m+1}{\bar{\gamma}_B} + \frac{q}{\bar{\gamma}_E} \right)^{-L_B - i}, \end{aligned} \tag{23}$$

$$\begin{aligned} P(C_s > 0)^{\text{SC/MRC}} = \frac{KL_A L_B}{\bar{\gamma}_B} \sum_{n=0}^{KL_A L_B - 1} \binom{KL_A L_B - 1}{n} (-1)^n \\ \times \sum_{p=0}^{W} \sum_{j=0}^{p(L_E-1)} \binom{W}{p} (-1)^p \frac{b_j}{\bar{\gamma}_E^j} \Gamma(j+1) \\ \times \left(\frac{n+1}{\bar{\gamma}_B} + \frac{p}{\bar{\gamma}_E} \right)^{-j-i}, \end{aligned} \tag{24}$$

$$\begin{aligned} P(C_s > 0)^{\text{SC/SC}} = \frac{KL_A L_B}{\bar{\gamma}_B} \sum_{n=0}^{KL_A L_B - 1} \binom{KL_A L_B - 1}{n} (-1)^n \\ \times \sum_{q=0}^{WL_E} \binom{WL_E}{q} (-1)^q \left(\frac{n+1}{\bar{\gamma}_B} + \frac{q}{\bar{\gamma}_E} \right)^{-1}. \end{aligned} \tag{25}$$

3.2 Secrecy outage probability

Since Alice does not have full CSI of any eavesdropper, we have to characterize the outage probability of secrecy capacity. The secrecy outage probability can be defined as the probability that the achievable secrecy rate is less than a given rate of transmission R_s such that $R_s > 0$. The transmission rate below R_s cannot ensure the secure transmission. The outage can occur in two ways: firstly, when SNR at Eve exceeds to that of Bob and Eve is able to decode the message; secondly, when SNR at Bob exceeds to that of Eve but still Bob is unable to decode the message. As such, we can formulate the secrecy outage probability [18,19] using the total probability theorem as follows:

$$\begin{aligned} P_{\text{out}}(R_s) = P(C_s < R_s | \gamma_B > \gamma_E) P(\gamma_B > \gamma_E) \\ + P(C_s < R_s | \gamma_B \leq \gamma_E) P(\gamma_B \leq \gamma_E). \end{aligned} \tag{26}$$

Since the secrecy capacity does not exist when $\gamma_B \leq \gamma_E$ and we always assume that $R_s > 0$, we get $P(C_s < R_s | \gamma_B \leq \gamma_E) = 1$. Therefore, (26) becomes

$$P_{\text{out}}(R_s) = P(C_s < R_s | \gamma_B > \gamma_E) P(\gamma_B > \gamma_E) + P(\gamma_B \leq \gamma_E). \tag{27}$$

The first term in (27) can be simplified as

$$\begin{aligned} P(C_s < R_s | \gamma_B > \gamma_E) P(\gamma_B > \gamma_E) &= P(\log_2(1+\gamma_B) - \log_2(1+\gamma_E) \\ &\quad < R_s | \gamma_B > \gamma_E) P(\gamma_B > \gamma_E) \\ &= P(\gamma_B < 2^{R_s}(1+\gamma_E) - 1 | \gamma_B > \gamma_E) \\ &\quad \times P(\gamma_B > \gamma_E) \\ &= \int_0^\infty \int_{\gamma_E}^{d(1+\gamma_E)-1} \\ &\quad \times f_E(\gamma_E) f_B(\gamma_B) d\gamma_B d\gamma_E, \end{aligned} \tag{28}$$

where $d = 2^{R_s}$. The second term in (27) can be simplified as

$$P(\gamma_B \leq \gamma_E) = \int_0^\infty \int_0^{\gamma_E} f_E(\gamma_E) f_B(\gamma_B) d\gamma_B d\gamma_E. \tag{29}$$

Substituting (28) and (29) in (27), we get

$$P_{\text{out}}(R_s) = \int_0^\infty f_E(\gamma_E) F_B(d(1+\gamma_E) - 1) d\gamma_E, \tag{30}$$

where $F_B(\cdot)$ is the CDF of γ_B and $f_E(\cdot)$ is the PDF of γ_E. As we have already derived the CDF of γ_B and PDF of γ_E for respective schemes, we simply proceed to obtain the outage probability expression for each scheme by replacing the respective values in (30). New closed-form expression

of the exact secrecy outage probability for each scheme is provided from (31) to (34) as follows:

$$P_{\text{out}}^{\text{MRC/MRC}}(R_{\text{s}}) = \sum_{m=0}^{KL_{\text{A}}} \sum_{i=0}^{m(L_{\text{B}}-1)} \sum_{u=0}^{i} \binom{KL_{\text{A}}}{m} (-1)^m \frac{a_i}{\bar{\gamma}_B^i} \binom{i}{u} \times d^u (d-1)^{i-u} e^{-\frac{(d-1)m}{\bar{\gamma}_B}} \; W \sum_{p=0}^{W-1} \sum_{j=0}^{p(L_{\text{E}}-1)} \times \binom{W-1}{p} \frac{(-1)^p b_j}{\bar{\gamma}_E^{L_{\text{E}}+j}\Gamma(L_{\text{E}})} \Gamma(L_{\text{E}}+j+u) \times \left(\frac{p+1}{\bar{\gamma}_E} + \frac{dm}{\bar{\gamma}_B}\right)^{-L_{\text{E}}-j-u}, \tag{31}$$

$$P_{\text{out}}^{\text{MRC/SC}}(R_{\text{s}}) = \sum_{m=0}^{KL_{\text{A}}} \sum_{i=0}^{m(L_{\text{B}}-1)} \sum_{u=0}^{i} \binom{KL_{\text{A}}}{m} (-1)^m \frac{a_i}{\bar{\gamma}_B^i} \binom{i}{u} \times d^u (d-1)^{i-u} e^{-\frac{(d-1)m}{\bar{\gamma}_B}} \; \frac{WL_{\text{E}}}{\bar{\gamma}_E} \sum_{q=0}^{WL_{\text{E}}-1} \times \binom{WL_{\text{E}}-1}{q} (-1)^q \Gamma(u+1) \times \left(\frac{q+1}{\bar{\gamma}_E} + \frac{dm}{\bar{\gamma}_B}\right)^{-u-1} \tag{32}$$

$$P_{\text{out}}^{\text{SC/MRC}}(R_{\text{s}}) = \sum_{n=0}^{KL_{\text{A}}L_{\text{B}}} \binom{KL_{\text{A}}L_{\text{B}}}{n} (-1)^n e^{-\frac{(d-1)n}{\bar{\gamma}_B}} \times W \sum_{p=0}^{W-1} \sum_{j=0}^{p(L_{\text{E}}-1)} \binom{W-1}{p} \frac{(-1)^p b_j}{\bar{\gamma}_E^{L_{\text{E}}+j}\Gamma(L_{\text{E}})} \Gamma(L_{\text{E}}+j) \times \left(\frac{p+1}{\bar{\gamma}_E} + \frac{dn}{\bar{\gamma}_B}\right)^{-L_{\text{E}}-j} \tag{33}$$

$$P_{\text{out}}^{\text{SC/SC}}(R_{\text{s}}) = \sum_{n=0}^{KL_{\text{A}}L_{\text{B}}} \binom{KL_{\text{A}}L_{\text{B}}}{n} (-1)^n e^{-\frac{(d-1)}{\bar{\gamma}_B}} \times \frac{WL_{\text{E}}}{\bar{\gamma}_E} \sum_{q=0}^{WL_{\text{E}}-1} \binom{WL_{\text{E}}-1}{q} (-1)^q \Gamma(n+1) \times \left(\frac{q+1}{\bar{\gamma}_E}\right)^{-n-1} \tag{34}$$

Remark 1. By substituting $K = W = L_{\text{A}} = L_{\text{B}} = L_{\text{E}} = 1$ in (31) to (34), all the schemes reduce to the special case of single transmitter, user, and eavesdropper with single antenna which corresponds to Equation 9 in [4].

Remark 2. A special case of single transmitter and user with single antenna and an eavesdropper with multiple antennas can be obtained with $K = W = L_{\text{A}} = L_{\text{B}} = 1$ in (31) to (34) such that (31) and (33) corresponds to Equation 10 in [14] while (32) and (34) corresponds to Equation 11 in [14].

This verifies that the expression derived is consistent with the results from the existing literature.

3.3 Asymptotic behavior

Although the closed-form expression for the outage probability derived in (31) to (34) enable us to evaluate the performance of TAS scheme, its complex forms do not allow us to gain valuable insights on how the parameter K, W, L_{A}, L_{B}, and L_{E} affect the overall performance. Therefore, we perform asymptotic analysis in the sequel.

As $\bar{\gamma}_B \to \infty$ in the high SNR regime, the asymptotic outage probability for both Bob and Eve's channel with MRC is given by

$$P_{\text{out}}^{\text{MRC/MRC(a)}}(R_{\text{s}}) = (\Psi^{\text{MRC/MRC}} \bar{\gamma}_B)^{-\Delta}, \tag{35}$$

where diversity order is $\Delta = KL_{\text{A}}L_{\text{B}}$ and array gain $\Psi^{\text{MRC/MRC}}$ is given by

$$\Psi^{\text{MRC/MRC}} = \left(W \sum_{m=0}^{\Delta} \binom{\Delta}{m} \frac{d^m (d-1)^{\Delta-m}}{(L_{\text{B}}!)^{KL_A}} \sum_{p=0}^{W-1} \sum_{j=0}^{p(L_{\text{E}}-1)} \binom{W-1}{p} \times \frac{(-1)^p b_j}{\bar{\gamma}_E^{L_{\text{E}}+j}\Gamma(L_{\text{E}})} \Gamma(L_{\text{E}}+j+m) \left(\frac{p+1}{\bar{\gamma}_E}\right)^{-L_{\text{E}}-j-m} \right)^{-\frac{1}{\Delta}}. \tag{36}$$

Proof. Further discussion of proof of (35) is presented in Appendix 1. □

Following the similar steps in Appendix 1, we can obtain the asymptotic outage probability for Bob with MRC and Eve with SC as follows

$$P_{\text{out}}^{\text{MRC/SC(a)}}(R_{\text{s}}) = (\Psi^{\text{MRC/SC}} \bar{\gamma}_B)^{-\Delta}, \tag{37}$$

where diversity order is $\Delta = KL_{\text{A}}L_{\text{B}}$ and array gain $\Psi^{\text{MRC/SC}}$ is given by

$$\Psi^{\text{MRC/SC}} = \left(\frac{WL_{\text{E}}}{\bar{\gamma}_E} \sum_{m=0}^{\Delta} \binom{\Delta}{m} \frac{d^m (d-1)^{\Delta-m}}{(L_{\text{B}}!)^{KL_{\text{A}}}} \sum_{q=0}^{WL_{\text{E}}-1} \binom{WL_{\text{E}}-1}{q} \times (-1)^q \Gamma(m+1) \left(\frac{q+1}{\bar{\gamma}_E}\right)^{-m-1} \right)^{-\frac{1}{\Delta}}. \tag{38}$$

Similarly, the asymptotic outage probability for Bob with SC and Eve with MRC can be obtained as

$$P_{\text{out}}^{\text{SC/MRC(a)}}(R_{\text{s}}) = (\Psi^{\text{SC/MRC}} \bar{\gamma}_B)^{-\Delta}, \tag{39}$$

where diversity order is $\Delta = KL_{\mathrm{A}}L_{\mathrm{B}}$ and array gain $\Psi^{\mathrm{SC/MRC}}$ is given by

$$\Psi^{\mathrm{SC/MRC}} = \left(W \sum_{n=0}^{\Delta} \binom{\Delta}{n} \frac{d^n (d-1)^{\Delta-n}}{W} \sum_{p=0}^{W-1} \sum_{j=0}^{p(L_{\mathrm{E}}-1)} \binom{W-1}{p} \times \frac{(-1)^p b_j}{\bar{\gamma}_E^{L_{\mathrm{E}}+j} \Gamma(L_{\mathrm{E}})} \Gamma(L_{\mathrm{E}}+j+n) \left(\frac{p+1}{\bar{\gamma}_E} \right)^{-L_{\mathrm{E}}-j-n} \right)^{-\frac{1}{\Delta}}. \tag{40}$$

Proof. Further discussion of proof of (37) is presented in Appendix 2. □

Following the similar steps in Appendix 2, we can obtain the asymptotic outage probability for both Bob and Eve with SC as follows:

$$P_{\mathrm{out}}^{\mathrm{SC/SC(a)}}(R_{\mathrm{s}}) = (\Psi^{\mathrm{SC/SC}} \bar{\gamma}_B)^{-\Delta}, \tag{41}$$

where diversity order is $\Delta = KL_{\mathrm{A}}L_{\mathrm{B}}$ and array gain $\Psi^{\mathrm{SC/SC}}$ is given by

$$\Psi^{\mathrm{SC/SC}} = \left(\sum_{n=0}^{\Delta} \binom{\Delta}{n} d^n (d-1)^{\Delta-n} \frac{WL_{\mathrm{E}}}{\bar{\gamma}_E} \sum_{q=0}^{WL_{\mathrm{E}}-1} \binom{WL_{\mathrm{E}}-1}{q} \times (-1)^q \Gamma(n+1) \left(\frac{q+1}{\bar{\gamma}_E} \right)^{-n-1} \right)^{-\frac{1}{\Delta}}. \tag{42}$$

We compare the performance difference between MRC and SC at Bob in terms of simple ratio of secrecy array gains as in [18]. The difference in performance is characterized as

$$\frac{\Psi^{\mathrm{MRC/MRC}}}{\Psi^{\mathrm{SC/MRC}}} = \frac{\Psi^{\mathrm{MRC/SC}}}{\Psi^{\mathrm{SC/SC}}} = (L_{\mathrm{B}}!)^{\frac{1}{L_{\mathrm{B}}}}. \tag{43}$$

It is obvious that MRC/MRC is superior to SC/MRC and MRC/SC is superior to SC/SC by an SNR gap of $\frac{10}{L_{\mathrm{B}}} \log (L_{\mathrm{B}}!)$. Moreover, as $\bar{\gamma}_E \to \infty$, the outage probability becomes one resulting absolute absence of secret communication. Also, the outage probability becomes 0 and 1 at the extreme values of $R_{\mathrm{s}} = 0$ and $R_{\mathrm{s}} \to \infty$ respectively as per our expectation.

4 Numerical results

Figure 2 shows the probability of positive secrecy as a function of $\bar{\gamma}_B$ at selected values of $\bar{\gamma}_E$ for various schemes when $K = 4$, $W = 3$, and $L_{\mathrm{A}} = L_{\mathrm{B}} = L_{\mathrm{E}} = 2$. This figure highlights that the probability of positive secrecy increases with $\bar{\gamma}_B$ while decreases with the increase in value of $\bar{\gamma}_E$. In both cases, non-zero secrecy capacity exists even when Eve's channel has a higher average SNR relative to Bob's channel. It is also obvious that MRC at Bob and SC at Eve provides the best performance while SC at Bob and MRC at Eve results the worst performance of all four possible schemes.

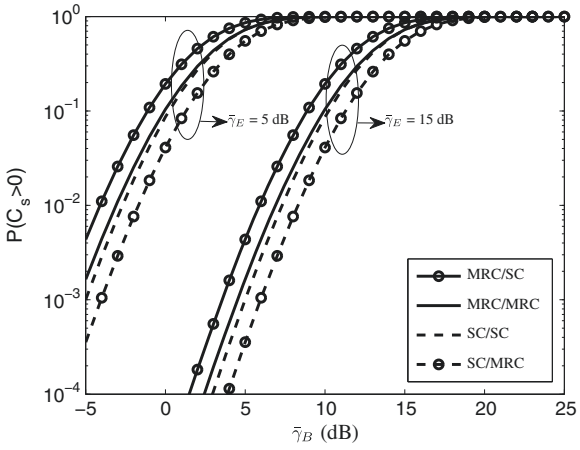

Figure 2 Probability of non-zero secrecy versus $\bar{\gamma}_B$ for selected values of $\bar{\gamma}_E$.

Figure 3 compares the secrecy outage probability versus $\bar{\gamma}_B$ for selected values of L_{A} with $K = W = L_{\mathrm{B}} = L_{\mathrm{E}} = 2$, $\bar{\gamma}_E$ = 15 dB and R_{s} = 0.1 bit/s/Hz. There is a remarkable decrease in the secrecy outage probability when we increase L_{A} from 1 to 4. This shows the improvement in performance from transmit diversity provided by TAS at Alice. For example, at $P_{\mathrm{out}} = 10^{-3}$ under MRC/MRC scheme, a gain of nearly 5.5 dB is achieved with $L_{\mathrm{A}} = 4$ compared to that of $L_{\mathrm{A}} = 1$.

In Figure 4, the asymptotic and exact secrecy outage probabilities for different schemes are shown at selected values of $\bar{\gamma}_E$ for each scheme to avoid cluttering in the figure. We consider $K = W = L_{\mathrm{A}} = L_{\mathrm{B}} = L_{\mathrm{E}} = 2$, and R_{s} = 0.1 bit/s/Hz for this case. We can observe

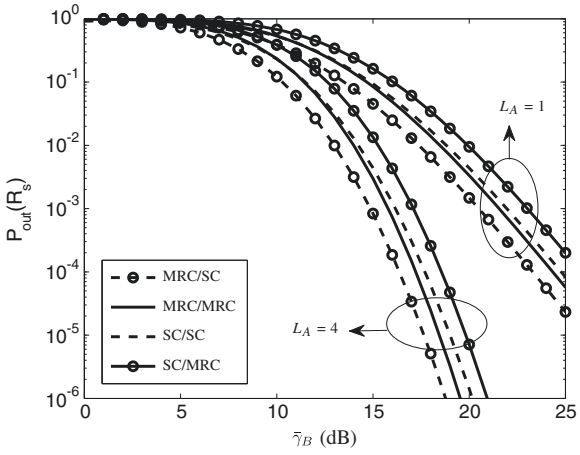

Figure 3 Secrecy outage probability versus $\bar{\gamma}_B$ for selected values of L_{A}.

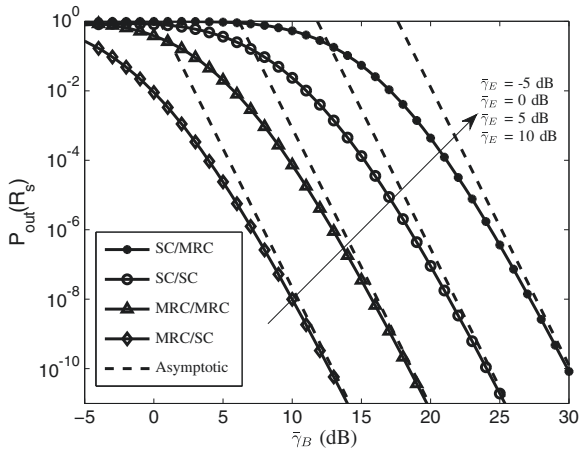

Figure 4 Asymptotic and exact secrecy outage probability versus $\bar{\gamma}_B$ for selected values of $\bar{\gamma}_E$.

that the asymptotic curve merges with exact curve in the high SNR regime. Moreover, the parallel asymptotic lines indicate the same diversity order in all four schemes. For the case of $K = L_{\mathrm{A}} = L_{\mathrm{B}} = 2$, the diversity order is found to be nearly 8 in all four schemes, which verifies the diversity order obtained in (35), (37), (39), and (41).

In Figure 5, we show the secrecy outage probability versus $\bar{\gamma}_B$ for different values of L_{B} and L_{E} with $K = W = L_{\mathrm{A}} = 2$, $\bar{\gamma}_E = 10$ dB and $R_{\mathrm{s}} = 0.1$ bit/s/Hz under MRC/MRC scheme. It is found that for fixed value of L_{B}, the increase in L_{E} will increase $P_{\mathrm{out}}(R_{\mathrm{s}})$. However, there is no improvement in the diversity order which is evident from the parallel lines for different values of L_{E}.

To compensate the performance degradation by number of antennas at Eve, we can increase the number of antennas at Bob. We can notice that a single addition of antenna at Bob sharply decreases the secrecy outage probability.

Figure 6 illustrates the secrecy outage probability versus target secrecy rate, R_s for different values of K with $W = L_{\mathrm{A}} = L_{\mathrm{B}} = L_{\mathrm{E}} = 2$, $\bar{\gamma}_B = 10$ dB and $\bar{\gamma}_E = 0$ dB. For $K = 1$, the proposed scheme corresponds to the scheme discussed in [16] and [17] but with the presence of multiple eavesdroppers. It is clear that employing opportunistic scheduling drastically improves the outage performance and higher target secrecy rate can be achieved. The performance improves with increase in K but it nearly saturates at higher values of K.

5 Conclusions

We proposed an opportunistic scheduling with TAS to enhance physical layer security. At the transmitter, a single antenna is selected to maximize the instantaneous SNR of the main channel, while at the receiver and the eavesdropper, MRC or SC is applied. The scheduler at Alice selects a single best user out of K users. The security performance metrics, i.e., probability of positive secrecy and secrecy outage probability are improved by combination of transmit diversity, receive diversity, and multiuser diversity simultaneously. The asymptotic analysis demonstrated that the outage diversity order of the proposed scheme is given by the product of the number of legitimate receivers and the number of antennas at the transmitter and receiver. We can also conclude that the secrecy outage probability is almost independent of the number of antennas and eavesdroppers in high SNR region.

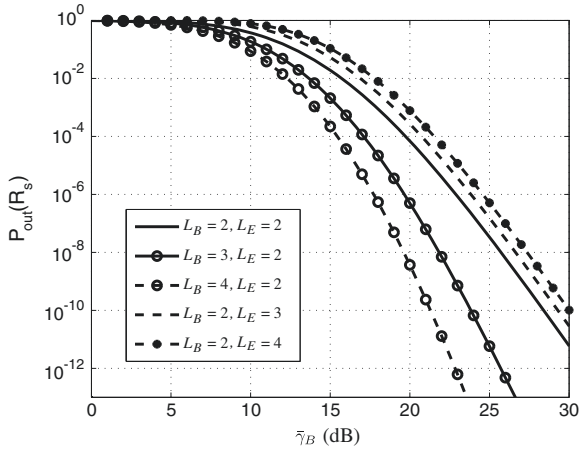

Figure 5 The secrecy outage probability versus target secrecy rate R_{s} for different values of L_{B} and L_{E}.

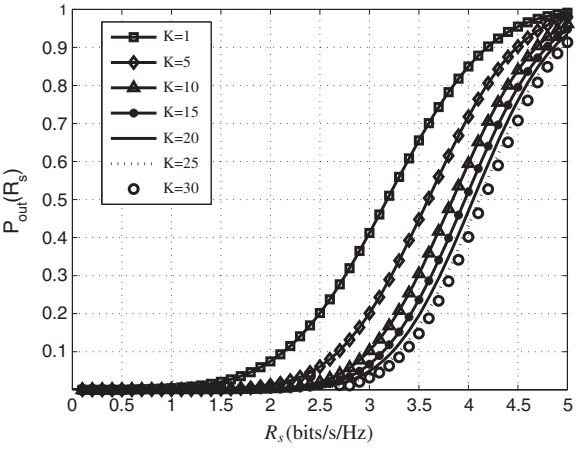

Figure 6 The secrecy outage probability versus target secrecy rate R_{s} for $W = L_{\mathrm{A}} = L_{\mathrm{B}} = L_{\mathrm{E}} = 2$.

Appendix 1

Proof of (35)

As $\bar{\gamma}_B \to \infty$, the CDF of Bob's channel with MRC can be approximated as

$$\begin{aligned} F_{\mathrm{B}}^{\mathrm{MRC}(a)}(\gamma_B) &\approx [F_{\mathrm{B}}(\gamma_B)]^{KL_{\mathrm{A}}} \\ &= \left[1 - \frac{\Gamma(L_{\mathrm{B}}, \frac{\gamma_B}{\bar{\gamma}_B})}{\Gamma(L_{\mathrm{B}})}\right]^{KL_{\mathrm{A}}} \\ &= \left[1 - \frac{(L_{\mathrm{B}}-1)! - \left(\frac{\gamma_B}{\bar{\gamma}_B}\right)^{L_{\mathrm{B}}} \frac{1}{L_{\mathrm{B}}}\left(1 + \mathcal{O}\left(\frac{\gamma_B}{\bar{\gamma}_B}\right)\right)}{(L_{\mathrm{B}}-1)!}\right]^{KL_{\mathrm{A}}} \\ &= \frac{\gamma_B^{KL_{\mathrm{A}}L_{\mathrm{B}}}}{\bar{\gamma}_B^{KL_{\mathrm{A}}L_{\mathrm{B}}}(L_{\mathrm{B}}!)_{\mathrm{A}}^{KL}}, \end{aligned} \tag{44}$$

where $\mathcal{O}$ denotes higher-order terms such that $f(x) = \mathcal{O}(g(x))$ implies that there exists a non-negative constant τ so that $\lim_{x\to\infty} \frac{f(x)}{g(x)} \leq \tau$. We select only the first order terms in (44) and finally substitute (15) and (44) in (30) to obtain (35).

Appendix 2

Proof of (37)

As $\bar{\gamma}_B \to \infty$, the CDF of Bob's channel with SC can be approximated as

$$\begin{aligned} F_{\mathrm{B}}^{\mathrm{SC(a)}}(\gamma_B) &\approx [1 - e^{-\frac{\gamma_B}{\bar{\gamma}_B}}]^{KL_{\mathrm{A}}L_{\mathrm{B}}} \\ &= \left[1 - 1 + \frac{\gamma_B}{\bar{\gamma}_B} + \mathcal{O}\left(\frac{\gamma_B}{\bar{\gamma}_B}\right)\right]^{KL_{\mathrm{A}}L_{\mathrm{B}}} \\ &= \frac{\gamma_B^{KL_{\mathrm{A}}L_{\mathrm{B}}}}{\bar{\gamma}_B^{KL_{\mathrm{A}}L_{\mathrm{B}}}}. \end{aligned} \tag{45}$$

Neglecting higher terms in (45) and substituting (15) and (45) in (30), we can obtain (37).

Competing interests

The authors declare that they have no competing interests.

Acknowledgements

This research was supported by a grant (12-TI-C01) from Advanced Water Management Research Program funded by Ministry of Land, Infrastructure and Transport of the Korean government.

Received: 8 July 2013 Accepted: 27 January 2014
Published: 4 March 2014

References

1. AD Wyner, The wire-tap channel. Bell Syst. Techn. J. **54**, 1355–1387 (1975)
2. I Csiszár, J Körner, Broadcast channels with confidential messages. IEEE Trans. Inf. Theory. **24**(3), 339–348 (1978)
3. S Leung-Yan-Cheong, M Hellman, The Gaussian wire-tap channel. IEEE Trans. Inf. Theory. **24**(4), 451–456 (1978)
4. M Bloch, J Barros, MRD Rodrigues, SW McLaughlin, Wireless information-theoretic security. IEEE Trans. Inf. Theory. **54**(6), 2515–2534 (2008)
5. Z Awan, A Zaidi, L Vandendorpe, Secure communication over parallel relay channel. IEEE Trans. on Info. Forensics Secur. **7**(2), 359–371 (2012)
6. Y Zou, X Wang, W Shen, Optimal relay selection for physical-layer security in cooperative wireless networks. IEEE J. Sel. Areas Commun. **31**(10), 2099–2111 (2013)
7. Z Awan, A Zaidi, L Vandendorpe, Multiaccess channel with partially cooperating encoders and security constraints. IEEE Trans. on Inf. Forensics Secur. **8**(7), 1243–1254 (2013)
8. A Zaidi, ZH Awan, S Shamai, L Vandendorpe, Secure degrees of freedom of MIMO X-channels with output feedback and delayed CSI. IEEE Trans. Inf. Forensics Secur. **8**(11), 1760–17774 (2013)
9. NS Ferdinand, DB da Costa, M Latva-aho, Effects of outdated CSI on the secrecy performance of MISO wiretap channels with transmit antenna selection. IEEE Commun. Lett, in press. **17**(5), 864-867 (2013)
10. AP Shrestha, KS Kwak, On maximal ratio diversity with weighting errors for physical layer security. IEEE Commun. Lett, in press. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=06746738
11. Y Zou, X Wang, W Shen, Physical-layer security enhancement with multiuser scheduling in cognitive radio. IEEE Trans. Commun, in press. http://arxiv.org/pdf/1311.0404.pdf
12. F He, H Man, W Wang, Maximal ratio diversity combining enhanced security. IEEE Commun. Lett. **15**(5), 509–511 (2011)
13. MZI Sarkar, T Ratnarajah, Enhancing security in correlated channel with maximal ratio combining diversity. IEEE Trans. on Signal Process. **60**(12), 6745–6751 (2012)
14. VU Prabhu, MRD Rodrigues, On wireless channels with m-antenna eavesdroppers: characterization of the outage probability and ϵ-outage secrecy capacity. IEEE Trans. Inf. Forensics Secur. **6**(3), 853–860 (2011)
15. A Mukherjee, AL Swindlehurst, Robust beamforming for security in MIMO wiretap channels with imperfect CSI. IEEE Trans. Signal Process. **59**(1), 351–361 (2011)
16. H Alves, RD Souza, M Debbah, Enhanced physical layer security through transmit antenna selection, in *IEEE GlobeCOM Workshops (GC Wkshps)*, Texas, 5–9 December 2011 (Houston, Tx, 2011), pp. 879-883
17. H Alves, RD Souza, M Debbah, M Bennis, Performance of transmit antenna selection physical layer security schemes. IEEE Signal Process. Lett. **19**(6), 372–375 (2012)
18. N Yang, PL Yeoh, M Elkashlan, R Schober, IB Collings, Transmit antenna selection for security enhancement in MIMO wiretap channels. IEEE Trans. on Commun. **61**(1), 144–154 (2013)
19. N Yang, HA Suraweera, IB Collings, C Yuen, Physical layer security of TAS/MRC with antenna correlation. IEEE Trans. Inf. Forensics Secur. **8**(1), 254–259 (2013)
20. D Sun, H Benaboud, M Noufissa, J Li, Exploring opportunistic scheduling in ad-hoc network with physical layer security, in *2012 National Days of Network Security and Systems (JNS2)*, Marrakech, 20–21 April 2012, pp. 62-67
21. AP Shrestha, KS Kwak, Secure opportunistic scheduling with transmit antenna selection, in *IEEE 24th International Symposium on Personal Indoor and Mobile Radio Communications PIMRC'13*, London, 8–11 September 2013 (London, 2013), pp. 461-465
22. H Cho, JG Andrews, Resource-redistributive opportunistic scheduling for wireless systems. IEEE Trans. Wireless Commun. **8**(7), 3510–3522 (2009)
23. A Goldsmith, *Wireless Communications* (Cambridge University, New York, 2005)
24. IS Gradshteyn, IM Ryzhik, *Table of Integrals, Series, and Products* (Academic, New York, 2007)
25. HA David, HN Nagaraja, *Order Statistics*. (Wiley, Hoboken, 2005)
26. CJ Chen, LC Wang, A unified capacity analysis for wireless systems with joint multiuser scheduling and antenna diversity in Nakagami fading channels. IEEE Trans. on Commun. **54**(3), 469–478 (2006)

doi:10.1186/1687-1499-2014-33
Cite this article as: Shrestha and Kwak: **Performance of opportunistic scheduling for physical layer security with transmit antenna selection.** *EURASIP Journal on Wireless Communications and Networking* 2014 **2014**:33.