Physical Layer Security in MIMO OSTBC Line-of-Sight Wiretap Channels with Arbitrary Transmit/Receive Antenna Correlation

Nuwan S. Ferdinand, Student Member, IEEE, Daniel Benevides da Costa, Member, IEEE, and Matti Latva-aho, Senior Member, IEEE

Abstract—In this paper, the physical layer security of multiple-input multiple-output (MIMO) wiretap channels with orthogonal space-time block codes (OSTBCs) and arbitrary antenna correlation is investigated. In our analysis, we consider general correlation matrices with arbitrary eigenvalue distributions. Also, in order to study the impact of the line-of-sight condition on the secrecy performance, the main channel is assumed to undergo Rician fading, while the eavesdropper one experiences Rayleigh fading. An easy-to-evaluate, closed-form expression for the secrecy outage probability is derived, from which an asymptotic analysis is carried out. Representative numerical results are plotted and validated through Monte Carlo simulations. Insightful discussions regarding the impact of the multiple antennas, correlation, and Rician factor on the secrecy outage performance are provided.

Index Terms—Antenna correlation, diversity gain, MIMO, orthogonal space-time block codes, physical layer security, secrecy outage performance.

I. INTRODUCTION

In light of the rapid and thriving advance of infrastructure-less networks, physical layer (PHY) security has arisen as a promising strategy to maintain secure data transmission without the need of cryptographic protocols. The idea behind this strategy is to explore the broadcast nature of the wireless medium to provide secure communications. seminal works were established by Shannon in [1], and Wyner in [2] introduced the wiretap channel, proving that perfect secrecy is possible without the use of cryptography as long as the channel between the transmitter and eavesdropper is a degraded version of the channel between the transmitter and legitimate receiver. In addition, along the last decade, multiple-input multiple-output (MIMO) techniques have received a huge interest from the wireless community due to the numerous benefits over single-antenna systems, such as a higher reliability. Motivated by these facts, recently several works have investigated the PHY security of MIMO wireless networks (please, see [3]–[7] and references therein).

In [5], assuming that the transmitter (Tx) and eavesdropper are equipped with multiple antennas, while the legitimate receiver (Rx) is a single-antenna device, the secrecy outage performance was examined. In such analysis, transmit antenna selection (TAS) and maximal-ratio combining (MRC) were employed at the Tx and eavesdropper, respectively. In [6], the PHY security of MIMO wiretap channels with TAS was studied. At the Rx and eavesdropper, two diversity combining techniques were adopted: selection combining and MRC. In [7], differently from all previous works, the impact of antenna correlation on the secrecy performance was investigated, in which TAS was employed at the Tx and MRC was considered at the Rx and eavesdropper. However, one minor drawback of [7] is that antenna correlation was assumed only at the Rx and eavesdropper. In addition, all the aforementioned works assumed that the Tx has channel state information (CSI) of the legitimate user.

The use of orthogonal space-time block codes (OSTBCs) in MIMO wiretap channels remain to be investigated in the technical literature, even for the case of uncorrelated antennas. As is well-known, OSTBCs provide full diversity gain, together with low encoding/decoding complexity [8], [9] and it does not require the CSI at the Tx. In this paper, the PHY security of MIMO OSTBC wiretap channels and arbitrary transmit/receive antenna correlation is investigated for the case where the Tx does not have the CSI of both main and eavesdropper channels. In our analysis, we consider general correlation matrices with arbitrary eigenvalue distributions. In order to study also the impact of the line-of-sight (LOS) condition on the secrecy performance, the main channel is assumed to undergo Rician fading\(^准备\), while the eavesdropper one experiences Rayleigh fading. An easy-to-evaluate, closed-form expression for the secrecy outage probability is derived, from which an asymptotic analysis is carried out. The derived expressions can also reduced to some special cases, which are new as well\(^准备\). Representative numerical results are plotted and validated through Monte Carlo simulations. The impact of the multiple antennas, antenna correlation, and Rician factor on the secrecy outage performance are investigated and insightful discussions are provided.

II. SYSTEM MODEL AND SECRECY CAPACITY

A. System model

Consider a MIMO wiretap channel in which a transmitter (Tx) Alice is equipped with \(N_A\) antennas and the legitimate receiver (Rx) Bob and an eavesdropper Eve are equipped with \(N_B\) and \(N_E\) antennas, respectively. We assume Bob and Eve have their own CSI to Alice. Both Tx-Rx channel and

\(\text{1}\)It is noteworthy that Rician fading reduces to Rayleigh one when the Rician factor equals zero. This is one more contribution of our paper since even assuming Rayleigh fading for the main channel, the proposed analysis was not carried out yet.

\(\text{2}\)Unfortunately, due to the space constraints, special cases of our results were not possible to be included in this paper.
eavesdropper channel experience slow fading with the same fading block length, which is assumed long enough to allow capacity-achieving codes within each block. Alice selects $L$ transmit symbols as $s_1, s_2, \ldots, s_L$ such that $E[s_i^2] = 1, \forall k$, with $E[\cdot]$ denoting expectation. Alice encodes the symbols using a $N_A \times T$ OSTBC matrix $Q$ and transmits using $T$ time slots. The received signal at Bob can be written as

$$y_B = \sqrt{P} H_{AB} Q + W_B,$$  

where $P = \frac{E}{N_0}$, $E$ denotes the transmitted power, $R = \frac{L}{T}$ is the code rate, $W_B$ represents the $N_B \times T$ noise matrix whose elements are modeled as additive white Gaussian noise (AWGN) with zero mean and variance $n_b$, $H_{AB}$ is the $N_B \times N_A$ channel matrix of the Tx-Rx link with mutually correlated Rician fading entries. In our model, $H_{AB} = H_{AB} + \tilde{H}_{AB}$, where $H_{AB}$ means the deterministic part coming from LOS, i.e., $H_{AB} = E[H_{AB}]$. The elements of $H_{AB}$ are characterized by a $N_A \times N_B$ correlation matrix $\Psi_{AB} = E[\tilde{H}_{AB} \tilde{H}_{AB}^H]$, in which $\tilde{H}_{AB}$ denotes the vectorization of $H_{AB}$, i.e., $\tilde{H}_{AB} = \text{vec}[H_{AB}]$, and $\otimes$ denotes the Hermitian transpose. Furthermore, $\Psi_{AB} = \Psi_A \otimes \Psi_B$, where $\Psi_A$ and $\Psi_B$ characterize the antenna correlation at Alice and Bob, respectively, and $\otimes$ denotes the Kronecker product.

Making use of orthogonalization property of OSTBC which reduces the MIMO channels into parallel single-input single-output (SISO) channels, we can write the $k^{th}$ combined signal at Bob as

$$y_{B,k} = \sqrt{P} v ||H_{AB}||^2_F s_k + n_{B,k},$$  

where $\parallel \cdot \parallel_F$ denotes the Frobenius norm, $n_{B,k}$ is the filtered noise with variance $v ||H_{AB}||^2_F n_b$, and $v$ is the normalizing factor of the OSTBC matrix in which one can force $v = 1$ by properly normalizing OSTBC matrix $Q$ [9].

In the eavesdropper channel, Eve hears the signal transmitted from Alice and the received signal at Eve can be written as

$$y_E(i) = \sqrt{P} H_{AE} Q + n_E,$$  

where $n_E$ is the $N_E \times T$ AWGN matrix with variance $n_e$ and $H_{AE}$ denotes the $N_E \times N_A$ channel matrix between Alice and Eve, whose entries are characterized by a $N_A \times N_E$ correlation matrix $\Psi_{AE} = E[\tilde{H}_{AE} \tilde{H}_{AE}^H]$, where $\tilde{H}_{AE} = \text{vec}[H_{AE}]$. In addition, $\Psi_{AE} = \Psi_A \otimes \Psi_E$, where $\Psi_E$ indicates the arbitrary receive antenna correlation matrix at Eve. Eve uses the orthogonalization property to obtain the $k^{th}$ combined symbol as

$$y_{E,k} = \sqrt{P} v ||H_{AE}||^2_F s_k + n_{E,k},$$  

where $n_{E,k}$ denotes the filtered noise with variance $v ||H_{AE}||^2_F n_e$.

### B. Secrecy Capacity

Let the capacity of the main channel between Alice and Bob be $C_B = R \log(1 + \gamma_B)$ and, between Alice and Eve be $C_E = R \log(1 + \gamma_E)$, where $\gamma_B = \hat{\gamma}_B ||H_{AB}||^2_F$ and $\gamma_E = \hat{\gamma}_E ||H_{AE}||^2_F$, with $\gamma_B = P v / n_b$ and $\gamma_E = P v / n_e$. Achievable secrecy capacity of the wiretap channel can be written as

$$C_S = \left\{ \begin{array}{ll} C_B - C_E, & \gamma_B > \gamma_E, \\ 0, & \gamma_B \leq \gamma_E. \end{array} \right.$$  

### III. Secrecy Outage Performance

#### A. Preliminaries

Throughout the paper, we set $N_1 = N_A \cdot N_B$ and $N_2 = N_A \cdot N_E$. Let the correlation matrix $\Psi_{AB}$ be eigen-decomposed as $\Psi_{AB} = U \Sigma U^H$ such that $\chi_1, \chi_2, \ldots, \chi_{N_2}$ are the arbitrary non-zero eigenvalues, i.e., $\Sigma = \text{diag} [\chi_1, \chi_2, \ldots, \chi_{N_2}]$, with $\text{diag} [\cdot]$ denoting the diagonal matrix. Let $\delta_{m}^j$ be the $m^{th}$ element of $\Sigma_{m} \cdot \hat{U} \tilde{H}_{AB}$, where $\tilde{H}_{AB} = \text{vec} [H_{AB}]$. Then, similar to [10], [11], the Laplace Transform of the probability density function (PDF) of $\gamma_B$ can be obtained as

$$\psi(s) = \exp \left( - \sum_{v=1}^{N_1} \sum_{u=1}^{N_1} \delta_{v}^u [1 + \frac{s\chi_{v}^{u}}{2}] \right),$$  

By taking the Inverse Laplace Transform of (6), the PDF of $\gamma_B$ can be attained as [10]–[12]

$$f_{\gamma_B}(z) = \frac{1}{\pi} \sum_{m=0}^{\infty} \sum_{k=0}^{\infty} \left( \frac{m}{k} \right) \chi_{k}^{m-1} \left( 1 - \chi_{v}^{u} \right) \frac{1}{(1 + k)(2\beta)^{N_1+k+k}},$$  

where $\beta$ represents the convergence parameter, which can be chosen as $1 \leq \beta \leq 4$ for faster convergence [10], $\phi_0 = 1$, and $m = \frac{1}{\pi} \sum_{u=0}^{\infty} \delta_{u}^{m} \phi_{u}$ for $u > 0$, where

$$\phi_{u} = - \frac{m}{2\beta} \sum_{v=1}^{N_1} \left( \delta_{u}^{v} \right)^2 \chi_{v}^{m-1} \sum_{v=1}^{N_1} \left( 1 - \chi_{v}^{u} \right) \frac{1}{(2\beta)^{m}}.$$  

The cumulative distribution function (CDF) of $\gamma_B$ can be achieved from (7) as

$$F_{\gamma_B}(z) = 1 - \sum_{m=0}^{\infty} \sum_{k=0}^{\infty} \left( \frac{m}{k} \right) \chi_{k}^{m-1} \sum_{p=0}^{N_1+k-1} \frac{z^{p}e^{-\frac{p\pi}{\beta}}}{p!(2\beta)^{p}}.$$  

Now, let the arbitrary non-zero eigenvalues of the correlation matrix $\Psi_{AE}$ be $\phi_1, \phi_2, \ldots, \phi_t$ with multiplicities $\eta_1, \eta_2, \ldots, \eta_t$ such that $\sum_{i=1}^{t} \eta_i = N_2$. Thus, the PDF of $\gamma_E$ can be obtained as in [13]

$$f_{\gamma_E}(z) = \sum_{i=1}^{t} \sum_{j=1}^{\eta_i} \frac{\gamma_{i,j}^{\eta_{i,j}}}{(\eta_{i,j} - j)! \Gamma(\eta_{i,j})} z^{j-1} e^{-\frac{z}{\gamma_{i,j}}},$$  

where

$$\gamma_{i,j} = \frac{1}{(\eta_{i,j} - j)!} \left( \phi_i \right)^{\eta_{i,j} - j} \prod_{k=1, k \neq i}^{t} \left( \frac{1}{1 + \phi_k} \right)^{\eta_k}.$$  

$^3$Values of $\beta$ are important for the convergence of the series and further details can be found in [10].
B. Secrecy Outage Probability

The secrecy outage probability is defined as the probability that $C_S$ drops below a predefined secrecy rate $R_S$. It can be mathematically expressed as $P_S(R_S) = \Pr(C_S < R_S)$, which by its turn can be rewritten as

$$P_S(R_S) = \Theta_1 + \Theta_2,$$  
(12)

where $\Theta_1 = \Pr(C_S < R_S | \gamma_B > \gamma_E)$, $\Theta_2 = \Pr(\gamma_B < \gamma_E)$ and $\Theta_2 = \Pr(\gamma_B < \gamma_E)$. By using probability theory concepts, $\Theta_1$ and $\Theta_2$ can be re-expressed as

$$\Theta_1 = \int_0^\infty \int_{\gamma_E}^{\infty} f_{\gamma_E}(\gamma_E)f_{\gamma_B}(\gamma_B)d\gamma_Bd\gamma_E,$$  
(13)

$$\Theta_2 = \int_0^\infty \int_0^{\gamma_E} f_{\gamma_E}(\gamma_E)f_{\gamma_B}(\gamma_B)d\gamma_Bd\gamma_E.$$  
(14)

Now, by substituting (13) and (14) into (12), it follows that

$$P_S(R_S) = \int_0^\infty \int_0^{\gamma_E} f_{\gamma_E}(\gamma_E)f_{\gamma_B}(\gamma_B)d\gamma_Bd\gamma_E = \int_0^\infty f_{\gamma_E}(z)F_{\gamma_B}(2\frac{R_S}{\gamma_E} (1 + z)^{-1})dz,$$  
(15)

which, from (10) and (9), it yields

$$P_S(R_S) = 1 - \sum_{i=1}^t \sum_{j=1}^m \frac{(N_1 - 1)!}{(j - 1)!((N_1 - 1)\gamma_E \phi_i)^j} \sum_{m=0}^\infty \sum_{k=0}^m \frac{(m)_k}{(k)_k} \left( -1 \right)^k \times \sum_{p=0}^{N_1 - k - 1} e^{-\frac{p\beta}{2\gamma_E \phi_i}} \left( \frac{p}{q} \right) \left( \frac{2}{2\beta} \right)^p (1 - \phi_i)^q^{-p - q} \times 2^{\frac{R_S}{\gamma_E}} \Gamma(q + j) \left( \frac{2}{2\beta} \right)^{q-j} \left( \frac{1}{\gamma_E \phi_i} \right)^{(q-j)},$$  
(16)

where $\Gamma(\cdot)$ denotes the Gamma function. It should be emphasized that (16) is evaluated almost instantaneously, in which very few terms are required for the series convergence. Also, it is noteworthy that secrecy outage probability given in (16) can be further simplified to several cases (e.g., distinct eigenvalue distribution, uniform correlation and uncorrelated cases) using the properties given in [13, Section II-E]. Unfortunately, due to the space limitation, these special cases were not possible to be included.

IV. ASYMPTOTIC SECRECY OUTAGE ANALYSIS

In this Section, we study the effects of the multiple antennas, antenna correlation, and LOS condition on the secrecy outage performance. A very good agreement between the analytical and simulated results is observed, which validates the proposed analysis. In addition, the asymptotic curves are depicted and shown to be very tight with the analytical ones at high SNR regions. For the plots, we consider two types of correlation matrix structures: (a) exponential correlation matrix, where $(i,j)^{th}$ entry can be modeled as $\rho^{j-i}$, $0 < \rho < 1$, and (b) uncorrelated case, where we set $\rho = 0$ so that all the eigenvalues equal to 1. Correlation coefficients at Alice, Bob, and Eve are represented by $\rho_A, \rho_B$, and $\rho_E$ respectively. Furthermore, we use the full rate Alamouti code [8] for $N_A = 2$ and the OSTBC matrix given in [9, eq. 27] for $N_A = 3$. Thus, we have $R = 1$ in all the curves. When following the legends of the figures, please note that different parameters for the analytical curves are ordered as the direction of arrows, e.g., $n^{th}$ set of parameters are for the $n^{th}$ analytical curve in the direction of the arrow.

4We assume that all eigenvalues of the correlation matrices are non-zero. However, if some of these eigenvalues are zero, then the desired diversity order cannot be realized. This occurs when some of the antennas are fully correlated, i.e., when all the elements of the correlation matrix are 1. However, in practice, note that transmission systems are designed such that the transmit antennas are not fully correlated.

Then, by taking the first non-zero order expansion of $F_{\gamma_B}(z)$, (17) simplifies to

$$F_{\gamma_B}(z) = \frac{\xi}{N_1!(2\beta)^{N_1}} \left( \frac{z}{2\beta} \right)^{N_1} + o \left( \left( \frac{z}{2\beta} \right)^{N_1+1} \right),$$  
(18)

where $o(\cdot)$ denotes the higher order terms and $\xi = \sum_{m=0}^\infty s_m$. By using (18) in (12), a high SNR expression for the secrecy outage can be written as

$$P_S(R_S) = \psi \frac{\xi - N_1}{N_1},$$  
(19)

where

$$\psi = \frac{\xi}{(N_1 - 1)!((2\beta)^N_1)} \sum_{i=0}^t \sum_{j=1}^m \frac{Y_{i,j}}{(j - 1)!((N_1 - 1)^{2\beta} \phi_i \gamma_E)^p} \times (2\frac{R_S}{\gamma_E} - 1)^{p - 2\beta} \Gamma(p + 1).$$  
(20)

From above, observe that the achievable diversity order equals to $G_D = N_1 = N_A \cdot N_B$ even in the presence of correlation. Next, we simplify the asymptotic results in the following special cases: (i) distinct eigenvalue distribution, and (ii) uncorrelated case. For the case (i), using [13, Section II-E] for distinct eigenvalues, (20) can be reduced to

$$\psi^c = \sum_{i=1}^{N_2} \sum_{p=0}^{N_1} \left( \frac{N_1}{(N_1 - 1)!((2\beta)^N_1 \phi_i \gamma_E)^p} \right)^2 \frac{\bar{w}(2\frac{R_S}{\gamma_E} - 1)^{N_1} - 2\frac{R_S}{\gamma_E} \Gamma(p + 1)}{(N_1 - 1)!((2\beta)^N_1 \phi_i \gamma_E)^p},$$  
(21)

where $\bar{w}$ is given as in [13, Eq. 20]. For the uncorrelated case, (20) can be simplified as

$$\psi^u = \sum_{p=0}^{N_1} \frac{N_1}{(N_1 - 1)!((2\beta)^N_1 \phi_i \gamma_E)^p} \frac{\bar{w}(2\frac{R_S}{\gamma_E} - 1)^{N_1} - 2\frac{R_S}{\gamma_E} \Gamma(p + N_2)^{N_1}}{(N_1 - 1)!((2\beta)^N_1 \phi_i \gamma_E)^p}$$  
(22)

V. NUMERICAL RESULTS AND DISCUSSIONS

In this Section, we study the effects of the multiple antennas, antenna correlation, and LOS condition on the secrecy outage performance. A very good agreement between the analytical and simulated results is observed, which validates the proposed analysis. In addition, the asymptotic curves are depicted and shown to be very tight with the analytical ones at high SNR regions. For the plots, we consider two types of correlation matrix structures: (a) exponential correlation matrix, where $(i,j)^{th}$ entry can be modeled as $\rho^{j-i}$, $0 < \rho < 1$, and (b) uncorrelated case, where we set $\rho = 0$ so that all the eigenvalues equal to 1. Correlation coefficients at Alice, Bob, and Eve are represented by $\rho_A, \rho_B$, and $\rho_E$ respectively. Furthermore, we use the full rate Alamouti code [8] for $N_A = 2$ and the OSTBC matrix given in [9, eq. 27] for $N_A = 3$. Thus, we have $R = 1$ in all the curves. When following the legends of the figures, please note that different parameters for the analytical curves are ordered as the direction of arrows, e.g., $n^{th}$ set of parameters are for the $n^{th}$ analytical curve in the direction of the arrow.
Fig. 1. Secrecy outage performance versus the Bob’s average SNR. All the curves are plotted for $\gamma_E = -5$ dB and $R_S = 1$.

Fig. 2. Secrecy outage performance versus LOS to non-LOS power ratio of Bob’s channel. We used $\gamma_B = 10$ dB, $N_A = N_B = N_E = 2$, and $R_S = 1$.

was investigated. A general, closed-form expression for the secrecy outage probability was derived, from which an asymptotic analysis was carried out. It was observed that the diversity gain is not affected by the antenna correlation as well as by the LOS condition. It was also shown that the presence of LOS increases the secrecy performance, but antenna correlation is highly undesirable under this condition.

VI. CONCLUSIONS

The PHY security of MIMO OSTBC line-of-sight wiretap channels with arbitrary transmit/receive antenna correlation was studied. Analyzing now the two leftmost curves, it can be observed that the antenna correlation does not alter the system diversity order. Specifically, in the two bottom-most curves, we can notice that secrecy outage varies from $3 \times 10^{-3}$ to $6 \times 10^{-5}$ for the correlated and uncorrelated case when $K = 2$; however this difference is only $5 \times 10^{-2}$ to $2 \times 10^{-2}$ for $K = 0$ case. Hence, it can be concluded that the LOS condition increases the secrecy performance, but antenna correlation is highly undesirable when LOS is available.

Fig. 1 shows the secrecy outage probability versus Bob’s average SNR. From the three rightmost curves, observe that the increase of antenna correlation increases the secrecy outage probability. Specifically, at $10^{-7}$ one can notice a 2 dB difference between the uncorrelated case and $[\rho_A, \rho_B, \rho_E] = [0.5, 0.6, 0.6]$ case. Furthermore, observe that the diversity gain remains equal to 4, even when antenna correlation increases, showing that the antenna correlation does not alter the system diversity order. Analyzing now the two leftmost curves, it can be seen that the increase of either $N_A$ or $N_B$ enhances the system diversity, resulting in a higher secrecy performance. However, note that the increase of $N_B$ outperforms the increase of $N_A$ for the same configuration. This occurs due to the fact that the increase of $N_A$ also improves the signal strength at Eve, causing the degradation of the performance when compared to an increase of $N_B$ (for this latter only Bob will be benefited).

Fig. 2 depicts the secrecy outage probability versus LOS to non-LOS power ratio (denoted by the parameter $K$) of Bob’s channel. Curves are plotted for two different Eve’s average SNR values. As expected, an improvement in secrecy performance occurs when Eve’s average SNR is low. Note that the decrease of secrecy outage probability is linear with the increase of $K$. Also, it is observed that lower the $\gamma_E$, the higher the secrecy outage gap with the increase of correlation and $K$. Moreover, it can be seen that the secrecy outage gap between correlated and uncorrelated cases increases with $K$ and this gap is minimum at non-LOS scenario (i.e., $K = 0$).

REFERENCES