Physical Communication 24 (2017) 154–160

Contents lists available at ScienceDirect

Physical Communication

journal homepage: www.elsevier.com/locate/phycom

Full length article

On signal space diversity: An adaptive interleaver for enhancing physical layer security in frequency selective fading channels☆

Marwan Yusuf [a,*], Hüseyin Arslan [a,b]

[a] School of Engineering and Natural Sciences, Istanbul Medipol University, 34810, Turkey
[b] Department of Electrical Engineering, University of South Florida, Tampa, FL, 33620, USA

ARTICLE INFO

Article history:
Received 22 December 2016
Received in revised form 25 May 2017
Accepted 2 July 2017
Available online 16 July 2017

Keywords:
Adaptive interleaving
OFDM
Rayleigh fading
Signal space diversity
Physical layer security
Eavesdropping

ABSTRACT

Signal space diversity is a powerful technique that increases reliability of detection over fading channels. In this paper, we explore the ability of this technique to provide secure communication. We enhance the security of OFDM systems in frequency selective fading channels by providing more diversity gain to the legitimate user compared to an eavesdropper. This is done by adapting the interleaving pattern to the channel of the legitimate user in rich multipath environments, where spatially separated channels are typically independent to each other. This ensures secrecy in a time division duplex system, where the eavesdropper has no information regarding the channel of the legitimate user. The scheme can also be used in the conventional frequency division duplex system, which is more challenging in terms of security aspects because of the channel state information leakage. A theoretical analysis is presented on the bit-error probability in Rayleigh fading environment. The numerical results support the conclusion that adapting the interleaving pattern to the CSI of the legitimate user provides a gain in the bit-error rate performance over the eavesdropper.

1. Introduction

The broadcast nature of wireless transmissions results in a critical drawback in terms of communication security and privacy, especially for applications in vital domains such as military, public safety or health care. Adversaries can possibly intercept the data traffic as long as they lie within the radio transmission coverage areas, a security problem known as eavesdropping. Physical-layer security is emerging as a good paradigm due to its ability to ensure communication secrecy without the explicit use of secret keys. It serves as a promising technique for highly dynamic or ad-hoc systems such as device-to-device and machine-type communication systems. Recent information-theoretic studies of the wiretap channel have demonstrated the possibility of achieving secrecy in the physical layer with the sole use of channel coding and signal processing techniques [1–5]. To that end, practical approaches have been investigated that make use of the random multipath propagation environment, multiple degrees of input/output or flexible waveform designs [6,7].

Most of the security approaches rely on the rich multipath environment, which provides enough uncorrelation between the spatially separated wireless channels of the legitimate user and the eavesdropper. To avoid the leakage of the unique channel state information (CSI) of the user to the eavesdropper, time division duplex (TDD) systems are used where the channel reciprocity assumption can be exploited. However, many of these studies make ideal assumptions on the CSI at the transmitter (Alice), the receiver (Bob), or the eavesdropper (Eve), and ignore the practical imperfections that affect the achievable secrecy performance [8]. Frequency division duplex (FDD) is a more challenging scenario for security in terms of the CSI leakage problem. In our work we propose a security technique that uses the conventional scheme of performing CSI feedback and thus can be viewed as a worst-case scenario technique in terms of security, where CSI of both the main and the wiretap channels are available at Eve [8].

Diversity, originally used to mitigate the performance degradation on fading channels and increase transmission reliability, is also used to improve the security of wireless transmission [9]. A type of diversity which has not received that much attention is signal space diversity (SSD), also referred to in the literature as modulation diversity or coordinate interleaving [10]. Most of the aforementioned diversity techniques aim to provide statistically independent copies of the transmitted sequence at the receiver for reliable detection. While they usually require extra resources or power consumption, SSD provides performance improvement over fading channels by taking advantage of the inherent orthogonality

☆ This work was supported by The Scientific and Technological Research Council of Turkey (TUBITAK) under project number 114E244.
* Corresponding author.
E-mail address: marwan.med7at@gmail.com (M. Yusuf).

http://dx.doi.org/10.1016/j.phycom.2017.07.001
1874-4907/

in the signal space [11,12]. The basic idea of SSD is that the quadrature components of each multidimensional signal constellation point are transmitted over independent fading channels. By simply interleaving these components under a certain rotation angle prior to transmission, the independence of the fading channels can easily be accomplished. The error performance of such technique and the choice of the optimal rotation angle which depends on the fading channel have been analyzed by several studies. In [11], the rotation angles are calculated at high signal-to-noise ratio (SNR) to maximize the minimum product distance of the rotated constellations over Rayleigh fading channels. In [12], the average bit error rate (BER) is approximated by considering only the nearest neighbors and the rotation angles are also chosen based on this approximation. The exact pair-wise error probability for M-ary phase shift keying signal constellations under Rayleigh fading channels is calculated in [13] where rotation angles are optimized by minimizing the upper bound on the average BER.

In this paper, we extend the work done in [14], where an adaptive design is proposed for the interleaving pattern which takes advantage of the frequency selective channels in wideband systems such as OFDM. An observation from previous studies is that the interleaving is done either randomly or by merely shifting the quadrature components, not taking the information of the fading channel into consideration. In this work, the interleaving of the quadrature components is done in frequency domain over different subcarriers typically exhibiting uncorrelated channel coefficients. Based on the estimated CSI of Bob, the interleaving pattern is adapted to maximize the overall diversity gain delivered to Bob compared to Eve, since they experience independent fading. This relative gain in channel conditions allows us to improve the secrecy performance of the system. Another advantage of our scheme is that it does not need multiple requirements such as, additional transmitted power for AN, information of the eavesdropping channel and location, multiple Tx and Rx antennas or cooperating nodes. With limited computational complexity for detection, we are able to improve the error performance at Bob compared to Eve.

The rest of the paper is organized as follows. In Section 2, we explain briefly the SSD system model, followed by our proposed adaptation for security in Section 3. Performance analysis of the Rayleigh fading channel is given in Section 4. Finally, Section 5 presents the numerical simulation results while conclusions are drawn in Section 6.

2. System model

In phase shift keying (PSK) or quadrature amplitude modulation (QAM) constellations, the in-phase (I) and the quadrature (Q) channels are orthogonal and can be separated at the receiver. Therefore, transmitting these two components through independently fading channels introduces a diversity gain into the system. However, this diversity gain is useful only if there is a redundancy between the two quadrature components. This redundancy is achieved through the rotation of the constellation points [12]. Fig. 1 shows a block diagram of an OFDM system employing SSD. Originally, the concept of coordinate interleaving and constellation rotation is used for frequency non-selective slowly fading channel where interleaving can be performed over time. In this work, we take advantage of the OFDM system performance in frequency selective channels. Interleaving can be performed to subcarriers over each OFDM symbol, making the added delay independent of the interleaving depth.

The concept of SSD is generic to all PSK/QAM constellations, hence we confine our analysis to PSK signal constellations for simplicity. Introducing the redundancy needed for diversity can be achieved by rotating the signal constellations by a certain angle θ. The modified MPSK constellation can be written as

$$S_M = \{s_p = e^{j(2\pi p/M+\theta)} : p = 0, 1, \ldots, M-1\} \quad (1)$$

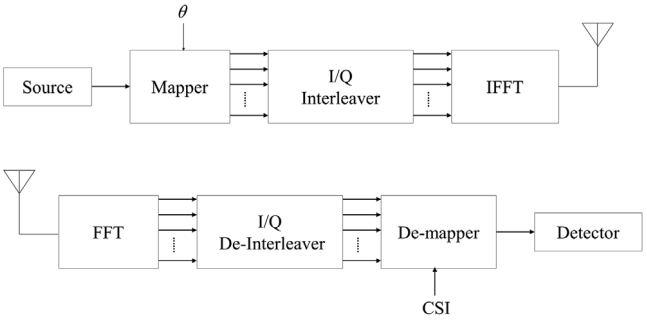


Fig. 1. OFDM system model employing SSD.

where each symbol corresponds to $\log_2 M$ bits. Each quadrature component is then interleaved independently. The interleaving in the proposed scheme is done in the frequency domain over each OFDM symbol. For N number of subcarriers, let the sequence of rotated I and Q components be denoted as $x = (x_0, x_1, \ldots, x_{N-1})$ and $y = (y_0, y_1, \ldots, y_{N-1})$, respectively. Let z_I and z_Q represent the I and Q interleavers, resulting in sequences $\bar{x} = z_I(x)$ and $\bar{y} = z_Q(y)$ which are to be transmitted over the N subcarriers.

The communication channel is assumed to be frequency selective fading channel. Let the discrete channel frequency response matrix be denoted as $\mathbf{H} = \text{diag}(H_0, H_1, \ldots, H_{N-1})$ where $H_k = |H_k|e^{j\phi_k}$ is the complex coefficient of the kth subcarrier. These coefficients are generated from the channel time impulse response where the taps are modeled as i.i.d. zero-mean complex Gaussian random variables in a Rayleigh fading channel. The N subcarrier channels are identically distributed but may not be independent of each other, since each coefficient is a linear combination of Gaussian variables. In order to simplify the mathematical analysis, it is assumed that all subcarriers experience i.i.d. fading.

Considering perfect synchronization at the receiver, the received symbols after FFT can be written as

$$r = \mathbf{H}\bar{s} + n \quad (2)$$

where $\bar{s} = \bar{x} + j\bar{y}$ is the vector of the transmitted interleaved symbols and n is a complex vector of additive white Gaussian noise with zero mean and a variance of $N_0/2$ in each dimension. Since the CSI is available at the receiver via channel estimation, the phase shift of the channel response $e^{j\phi_k}$ can be removed without any error. The received I and Q components are then de-interleaved to give $\bar{r}_I = z_I^{-1}(r_I)$ and $\bar{r}_Q = z_Q^{-1}(r_Q)$. The magnitude of CSI is also de-interleaved resulting in $|\mathbf{H}_I| = z_I^{-1}(|\mathbf{H}|)$ and $|\mathbf{H}_Q| = z_Q^{-1}(|\mathbf{H}|)$. The receiver then performs a maximum likelihood detection on the de-interleaved sequence

$$\bar{r} = |\mathbf{H}_I|x + j|\mathbf{H}_Q|y + \bar{n} \quad (3)$$

where $\bar{r} = \bar{r}_I + j\bar{r}_Q$ and $\bar{n}$ are the received signal and noise respectively after de-interleaving.

3. Proposed secure OFDM system with SSD

The proposed eavesdropping–resilient OFDM system with SSD depends on delivering more diversity gain to Bob compared to Eve. It is shown in previous studies that the gain of SSD depends on the Euclidean distance between constellation points which is a function of the rotation angle under independent fading of I and Q components [10]. For a certain rotation angle, larger difference in the fading components provides larger gain. This can be understood as when one component goes through deep fading, the other component should provide enough separation distance in the

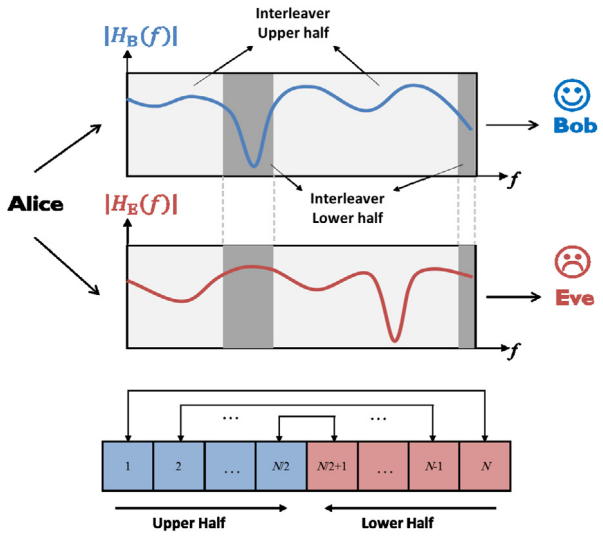


Fig. 2. Adapting interleaving pattern to the channel response to provide more diversity gain to Bob than Eve.

signal space to offer more protection against noise, so that no two constellation points collapse together along any of the quadrature components [10].

Hence, to provide more gain to Bob we adapt the interleaving pattern to his CSI such that components going through bad channel condition, i.e. deep fades, are interleaved with ones going through good channel condition. This is done by first sorting the channel coefficients H_k according to the descending order of their magnitudes. The order of the N subcarriers can be expressed as

$$|H_k(1)| \geq |H_k(2)| \geq \cdots \geq |H_k(l)| \geq \cdots \geq |H_k(N)| \tag{4}$$

where k is the variable representing the position index of each subcarrier in the frequency domain and l denotes the subcarrier order index among the N sorted subcarriers. Then the interleaving pattern is designed so that one of the quadrature components of the upper half of the sorted subcarriers,which has the largest magnitudes, should replace the lower half, which has the smallest magnitudes. This can be visualized as moving from the ends to the middle as shown in Fig. 2. This way, we make sure that each bad component is interleaved with the best component possible. The interleaved pairs would have the l indices of

$$\{(1, N),\ (2, (N-1)),\ \ldots (N/2, (N/2+1))\}. \tag{5}$$

As mentioned before, our scheme makes use of the channel spatial dependency, meaning that wireless channels associated with different end points at separate locations typically exhibit uncorrelated propagation characteristics in rich scattering environments. As a result, the eavesdropping channel $\mathbf{H}^E$ would be uncorrelated with the main channel $\mathbf{H}$. The de-interleaved signal at Eve can be written as

$$\bar{r}_E = |\mathbf{H}_I^E|x + j|\mathbf{H}_Q^E|y + \bar{n}_E \tag{6}$$

Since this is a CSI-based security scheme, the CSI needs to be known at Alice. While the CSI can be estimated at Alice in a TDD system, It needs to be fedback by Bob in the conventional FDD systems. Alternatively, Bob can feedback only the interleaving indices in (5) for feedback bandwidth efficiency. Also, the time variation of the wireless channels introduces frequently updated randomness, which further strengthens its security. In some scenarios, the CSI may be outdated due to insufficient feedback bandwidth, causing the main channel at Alice to consist of only the past channels. Since the channel is slowly fading, using the past channel for the interleaving pattern adaptation will not have a large effect on the diversity gain delivered. Hence, Bob can also use the past channel for interleaving adaptation while the current channel is used for normal detection. Since the CSI is fed back from Bob to Alice, Eve can intercept the transmission to acquire the interleaving pattern and use it for detection. However, even if she manages to use the same de-interleaver as Bob, the gain delivered is not the same due to the uncorrelation between their channels, as shown in Fig. 2. In fact, the performance of Eve will be the same as SSD with random interleaving, as shown later on.

However, if we take a closer look at the interleaved pairs in (5), we notice that not all the pairs contribute identically to the diversity gain. In fact, most of the gain comes from the first portion of pairs, and as we move forward the contribution becomes less significant. This comes from the fact that, the interleaved channel magnitude pairs at the end are close to each other in order, hence they have the minimum differences among subcarriers. We can take advantage of this by reducing the interleaver depth to include just the contributing pairs and keep the remaining subcarriers without interleaving. In addition to reducing computational complexity, this has the advantage of significantly reducing the gain delivered to Eve. Since the chosen interleaved pairs are adapted for Bob's channel, more gain reduction is delivered to Eve compared to Bob.

4. Performance analysis over Rayleigh fading channels

Considering a QPSK scheme for the analysis, the conditional average bit-error probability can be written as

$$P(s_p \rightarrow \hat{s}_p|\alpha) = Q\left(\sqrt{\alpha d_{min}^2}\right) \tag{7}$$

where $\alpha = |H|^2 \frac{E_b}{N_0}$ is the faded SNR per bit and d_{min}^2 represents the minimum squared Euclidean distance between two constellation points, indicating that only the nearest neighbors are considered. It can also be represented as the sum of the distances in the I and Q directions $d_{min}^2 = d_I^2 + d_Q^2$ [12], where

$$d_I^2 = 1 + \sin(2\theta),$$
$$d_Q^2 = 1 - \sin(2\theta). \tag{8}$$

In this work, the fading amplitude is modeled as Rayleigh fading with unity average power. Hence α has the PDF and CDF of

$$f_\alpha = \frac{1}{\bar{\alpha}} e^{-\alpha/\bar{\alpha}}, \tag{9}$$
$$F_\alpha = 1 - e^{-\alpha/\bar{\alpha}} \tag{10}$$

respectively, where $\bar{\alpha} = \frac{E_b}{N_0}$ is the average SNR per bit and, in (7), $Q(x)$ is the Gaussian probability function defined as

$$Q(x) = \frac{1}{\pi} \int_0^{\frac{\pi}{2}} e^{\frac{-x^2}{2\sin^2\phi}} d\phi. \tag{11}$$

4.1. Average probability of bit error for conventional system

Assuming perfect CSI, the average bit-error probability for the conventional QPSK system is calculated by averaging over the fading statistics, giving the widely known formula when considering only the nearest neighbors [15]

$$P_e = \int_0^\infty Q\left(\sqrt{\alpha(d_I^2 + d_Q^2)}\right) f_\alpha d\alpha = \frac{1}{2}\left(1 - \sqrt{\frac{\bar{\alpha}}{1+\bar{\alpha}}}\right). \tag{12}$$

It is observed from (8) and (12) that, under the same I and Q fading, the system performance is not a function of the constellation

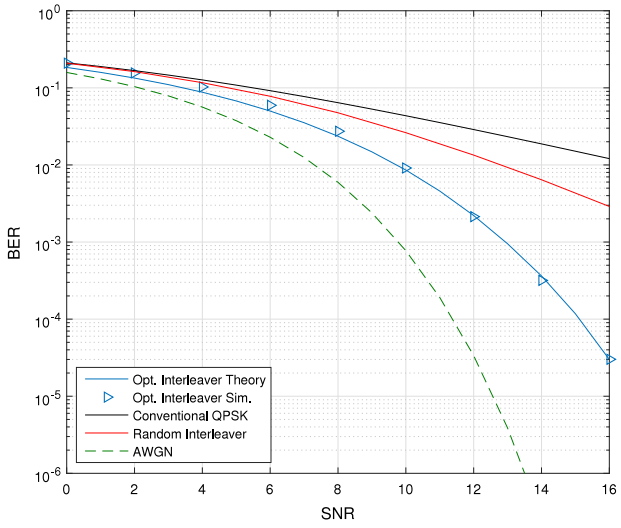


Fig. 3. Average BER of QPSK scheme for different scenarios.

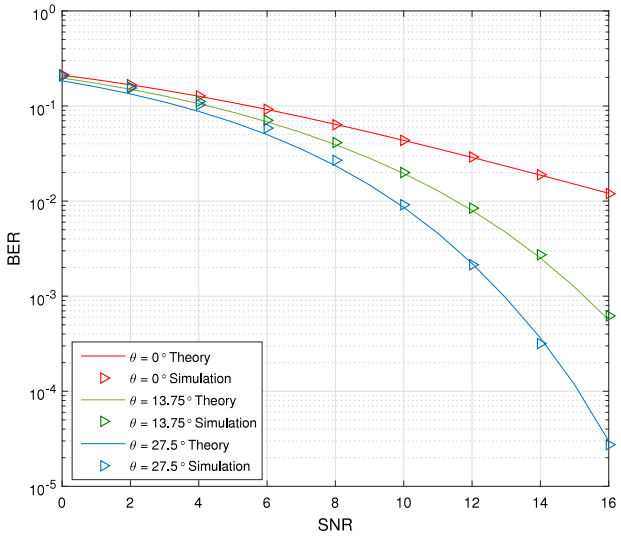


Fig. 4. Average BER of QPSK scheme with adaptive interleaver for different rotation angles along with matching simulation results.

rotation, since d_I^2 and d_Q^2 always add up to $d_{min}^2 = 2$. In subsequent analysis we consider independent I and Q fading scenarios employing coordinate interleaving.

4.2. Average probability of bit error for SSD system with random interleaver

Let α_1 and α_2 be two i.i.d. random variables with PDF given in (9). The average bit-error probability is obtained by averaging (7) over the I and Q fading components

$$P_e = \int_0^\infty \int_0^\infty Q\left(\sqrt{\alpha_1 d_I^2 + \alpha_2 d_Q^2}\right) f_{\alpha_1} f_{\alpha_2} d\alpha_1 d\alpha_2 \tag{13}$$

where $\alpha_1 = |H_I|^2 \frac{E_b}{N_0}$ and $\alpha_2 = |H_Q|^2 \frac{E_b}{N_0}$. Since we assume that all subcarriers experience independent fading, the error probability is calculated in (13) by averaging over the product of the distributions for the two interleaved fading components. This gives the result reported in [13]

$$P_e = \frac{1}{2} - \frac{d_I^2}{2(d_I^2 - d_Q^2)}\left(\sqrt{\frac{\bar{\alpha} d_I^2/2}{1 + \bar{\alpha} d_I^2/2}}\right) + \frac{d_Q^2}{2(d_I^2 - d_Q^2)}\left(\sqrt{\frac{\bar{\alpha} d_Q^2/2}{1 + \bar{\alpha} d_Q^2/2}}\right). \tag{14}$$

4.3. Average probability of bit error for SSD system with adaptive interleaver

For the proposed adaptive interleaver, the two fading components α_1 and α_2 cannot be considered exponentially distributed as in (9) anymore. Since our algorithm sorts the subcarriers according to the fading magnitude, the distribution of the fading components over each subcarrier follows an order statistic that depends on the subcarrier order index l and the total number of subcarriers N.

For a sequence of i.i.d. random variables $\{\alpha_1, \alpha_2, \ldots, \alpha_N\}$ of length N, PDF f_α and CDF F_α, the PDF of the kth order statistic, that is, the k smallest of the sequence, is given by [16]

$$f_k = \frac{N!}{(k-1)!(N-k)!} F_\alpha^{k-1} [1 - F_\alpha]^{N-k} f_\alpha. \tag{15}$$

Hence, for a subcarrier with the interleaved pair of order indices (k_1, k_2), the distribution of the fading components α_1 and α_2 follows the order statistics f_{k_1} and f_{k_2} from (15) respectively, and the bit-error probability can be calculated as

$$P_s(k_1, k_2) = \int_0^\infty \int_0^\infty Q\left(\sqrt{\alpha_1 d_I^2 + \alpha_2 d_Q^2}\right) f_{k_1} f_{k_2} d\alpha_1 d\alpha_2 \tag{16}$$

$$= \sum_{u_1=0}^{k_1-1} \sum_{u_2=0}^{k_2-1} A \binom{k_1-1}{u_1} \binom{k_2-1}{u_2} (-1)^{u_1+u_2} \left[1 - \frac{\beta}{\beta-\gamma}\sqrt{\frac{\beta}{1+\beta}} + \frac{\gamma}{\beta-\gamma}\sqrt{\frac{\gamma}{1+\gamma}}\right], \tag{17}$$

where

$$A = \frac{N!}{2(k_1-1)!(N-k_1)!(u_1+N-k_1+1)} \times \frac{N!}{(k_2-1)!(N-k2)!(u_2+N-k_2+1)},$$

$$\beta = \frac{d_I^2 \bar{\alpha}}{2(u_1+N-k_1+1)},$$

$$\gamma = \frac{d_Q^2 \bar{\alpha}}{2(u_2+N-k_2+1)}.$$

The exact derivation of (17) can be found in the appendix. According to (5), for a total number of N subcarriers, the orders take the values $k_1 \in \{1, 2, \ldots, N\}$ while $k_2 = N + 1 - k_1$. As a result, (16) can be written as a function of only k_1 and the total average bit-error probability is calculated by averaging over the N subcarriers

$$P_e = \frac{1}{N} \sum_{k_1=1}^{N} P_s(k_1). \tag{18}$$

Fig. 3 shows the error performance of the conventional QPSK system over Rayleigh fading channel, as in (12), and the SSD system with both random interleaver (14) and adaptive optimal interleaver (17). The rotation angle is set to the optimal value of 27.5° as reported in [13]. The AWGN performance is also added for comparison. It is clear how adapting the interleaving pattern

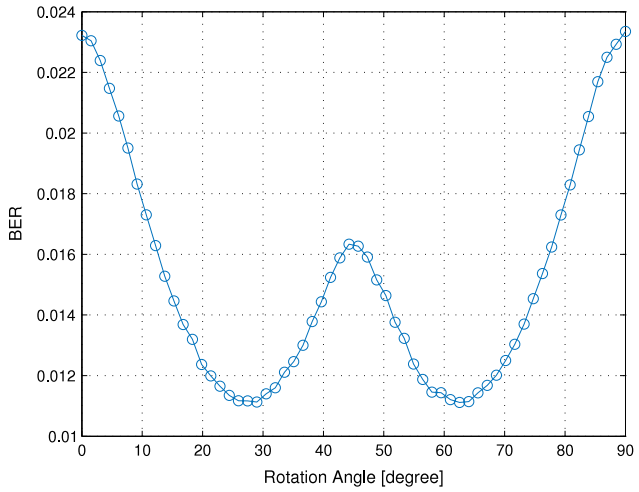


Fig. 5. Average BER of QPSK signal constellation at different values of the rotation angle θ over Rayleigh channel at $E_b/N_0 = 15$ dB.

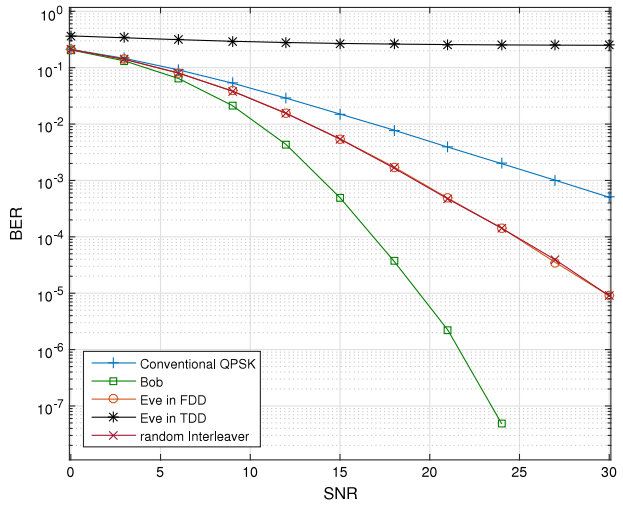


Fig. 6. Average BER of QPSK signal constellation at different SNR over Rayleigh channel at $\theta = 27.5°$.

improves the error performance over the conventional systems. Simulation results which match the theoretical formula are also included where the number of OFDM subcarriers is set to 16. Fig. 4 shows the matching simulations results and theoretical formula of the adaptive interleaver design for different rotation angles.

5. Numerical results

The security of the proposed OFDM system employing SSD is evaluated through the BER of Bob and Eve over fading channels. We take QPSK as the candidate constellation in MPSK signal constellations and present the simulation results over Rayleigh fading multipath channels with uniform power delay profile. In order to make fair comparisons, we assume that the main channel and the wiretap channel follow an identical statistical model, and that the noise levels at all nodes are the same.

First we show the simulation results for the optimum rotation angle for QPSK signal constellations. Fig. 5 shows the BER performance at $E_b/N_0 = 15$ dB with different rotation angles and random interleaving. The optimum rotation angle matches the one calculated in [13] for natural bit mapping. Fig. 6 shows the performance gain achieved by the SSD over the conventional modulation system for the optimum rotation angle calculated and $N = 64$ subcarriers. This gain is achieved using a certain random interleaver at both Alice and Bob.

In FDD case, under the assumption that Eve can acquire the interleaving pattern used by Alice and Bob, the maximum gain that can be delivered to Eve is the same as the random interleaver case, which is shown clearly in Fig. 6. We also include the TDD case where the interleaving pattern at Eve does not match with Bob, since CSI is not known to Eve. It shows that the performance of Eve is totally degraded and secrecy is ensured. In addition, the figure shows that the gain delivered to Bob is larger than the normal SSD gain since we adapt the interleaving pattern to the main channel response.

As we mentioned before, the interleaver depth can be reduced without losing much of the performance gain for Bob. Fig. 7 shows the performance for different values of interleaver depth as percentage of the N subcarriers at SNR = 20 dB. Keeping in mind that it is in log scale, we see that the gain reduction for Eve is very large compared to Bob. Based on the acceptable performance of Bob, the interleaver depth can be chosen to minimize the gain delivered to Eve. Fig. 8 shows the performance gain for Bob and Eve for interleaver depth of 50%. It is clear that the diversity gain delivered to Eve over the conventional system is becoming insignificant compared to Bob.

6. Conclusion

The randomness of the wireless multipath channel is used to provide more diversity gain to the legitimate user compared to an eavesdropper. Using signal space diversity, we are able to enhance the error performance by adapting the interleaving pattern to the unique channel response of the legitimate user. This scheme is robust to the channel state information leakage problem usually faced in wireless communication, hence conventional FDD systems can be adopted. Based on the theoretical analysis and numerical results, the design of an adaptive interleaver is presented with a trade off between computational complexity and error performance.

Appendix

Substituting (11) and (15) into (16) gives

$$\begin{aligned} P_s(k_1,k_2) =& \frac{N!}{(k_1-1)!(N-k_1)!}\frac{N!}{(k_2-1)!(N-k2)!} \\ &\times \int_0^{\infty}\int_0^{\infty}\int_0^{\frac{\pi}{2}} \frac{1}{\pi} e^{-\left(\frac{\alpha_1 d_I^2+\alpha_2 d_Q^2}{2\sin^2\phi}\right)} d\phi \\ &\times \left[1-e^{-\alpha_1/\bar{\alpha}}\right]^{k_1-1}\left[e^{-\alpha_1/\bar{\alpha}}\right]^{N-k_1}\frac{1}{\bar{\alpha}}e^{-\alpha_1/\bar{\alpha}}d\alpha_1 \\ &\times \left[1-e^{-\alpha_2/\bar{\alpha}}\right]^{k_2-1}\left[e^{-\alpha_2/\bar{\alpha}}\right]^{N-k_2}\frac{1}{\bar{\alpha}}e^{-\alpha_2/\bar{\alpha}}d\alpha_2 \end{aligned} \tag{19}$$

where f_α and F_α in (15) are taken from (9) and (10) respectively. Using the binomial expansion results in

$$\begin{aligned} P_s(k_1,k_2) =& B\int_0^{\frac{\pi}{2}}\int_0^{\infty}\int_0^{\infty} e^{-\alpha_1\left(\frac{N-k_1+1}{\bar{\alpha}}+\frac{d_I^2}{2\sin^2\phi}\right)} \\ &\times e^{-\alpha_2\left(\frac{N-k_2+1}{\bar{\alpha}}+\frac{d_Q^2}{2\sin^2\phi}\right)}\sum_{u_1=0}^{k_1-1}\binom{k_1-1}{u_1}\left(-e^{-\alpha_1/\bar{\alpha}}\right)^{u_1} \\ &\times \sum_{u_2=0}^{k_2-1}\binom{k_2-1}{u_2}\left(-e^{-\alpha_2/\bar{\alpha}}\right)^{u_2} d\alpha_1 d\alpha_2 d\phi \end{aligned} \tag{20}$$

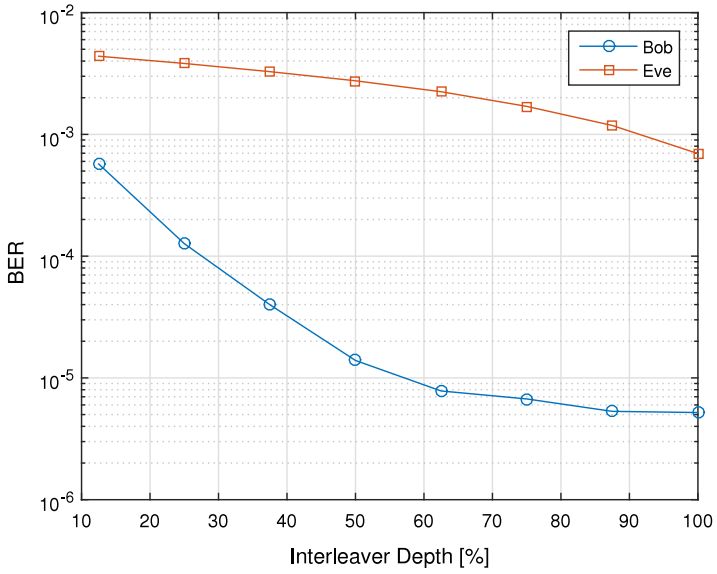


Fig. 7. Average BER of QPSK signal constellation at different percentage values of the interleaver depth over Rayleigh channel at SNR = 20 dB.

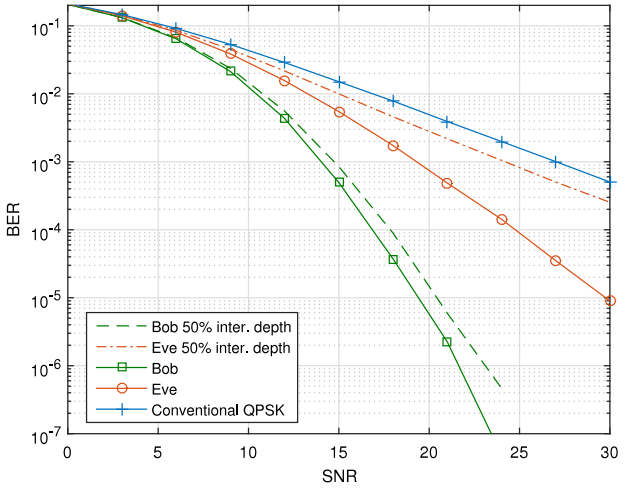


Fig. 8. Performance reduction in average BER at different SNR with 50% interleaver depth.

where

$$B = \frac{1}{\pi\bar{\alpha}^2}\frac{N!}{(k_1-1)!(N-k_1)!}\frac{N!}{(k_2-1)!(N-k2)!}.$$

Rearranging (20) gives

$$P_s(k_1,k_2) = B\sum_{u_1=0}^{k_1-1}\sum_{u_2=0}^{k_2-1}\binom{k_1-1}{u_1}\binom{k_2-1}{u_2}(-1)^{u_1+u_2} \times \int_0^{\frac{\pi}{2}}\int_0^{\infty}\int_0^{\infty} e^{-\alpha_1\left(\frac{u_1+N-k_1+1}{\bar{\alpha}}+\frac{d_I^2}{2\sin^2\phi}\right)} \times e^{-\alpha_2\left(\frac{u_2+N-k_2+1}{\bar{\alpha}}+\frac{d_Q^2}{2\sin^2\phi}\right)} d\alpha_1 d\alpha_2 d\phi \quad (21)$$

which is integrated over α_1 and α_2 to get

$$P_s(k_1,k_2) = \sum_{u_1=0}^{k_1-1}\sum_{u_2=0}^{k_2-1}\frac{2A}{\pi}\binom{k_1-1}{u_1}\binom{k_2-1}{u_2}(-1)^{u_1+u_2} \times \int_0^{\frac{\pi}{2}}\frac{\sin^4\phi}{(\sin^2\phi+\beta)(\sin^2\phi+\gamma)}d\phi \quad (22)$$

where A, β and γ are the same as in (17). The integral in (22) can be solved using partial fraction expansion as

$$I = \int_0^{\frac{\pi}{2}}\left[1-\frac{\beta}{\beta-\gamma}\frac{\beta}{\sin^2\phi+\beta}+\frac{\gamma}{\beta-\gamma}\frac{\gamma}{\sin^2\phi+\gamma}\right]d\phi = \frac{\pi}{2}\left[1-\frac{\beta}{\beta-\gamma}\sqrt{\frac{\beta}{1+\beta}}+\frac{\gamma}{\beta-\gamma}\sqrt{\frac{\gamma}{1+\gamma}}\right]. \quad (23)$$

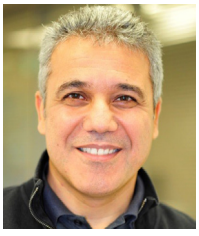
Substituting (23) into (22) gives the final result in (17).

References

[1] A.D. Wyner, The wire-tap channel, The Bell Syst. Tech. J. 54 (8) (1975) 1355–1387.
[2] S. Leung-Yan-Cheong, M. Hellman, The Gaussian wire-tap channel, IEEE Trans. Inf. Theory 24 (4) (1978) 451–456.
[3] M. Bloch, J. Barros, M.R. Rodrigues, S.W. McLaughlin, Wireless information-theoretic security, IEEE Trans. Inform. Theory 54 (6) (2008) 2515–2534.
[4] K. Ren, H. Su, Q. Wang, Secret key generation exploiting channel characteristics in wireless communications, IEEE wirel. commun. 18 (4) (2011) 6–12.
[5] F. Renna, N. Laurenti, H.V. Poor, Physical-layer secrecy for OFDM transmissions over fading channels, IEEE Trans. Inf. Forensic Secur. 7 (4) (2012) 1354–1367.
[6] H. Lei, I.S. Ansari, G. Pan, B. Alomair, M.-S. Alouini, Secrecy capacity analysis over $\alpha-\mu$ fading channels, IEEE Commun. Lett.
[7] H. Lei, C. Gao, I.S. Ansari, Y. Guo, Y. Zou, G. Pan, K.A. Qaraqe, Secrecy outage performance of transmit antenna selection for MIMO underlay cognitive radio systems over Nakagami-*m* channels, IEEE Trans. Veh. Technol. 66 (3) (2017) 2237–2250.
[8] T.-Y. Liu, P.-H. Lin, S.-C. Lin, Y.-W.P. Hong, E.A. Jorswieck, To avoid or not to avoid CSI leakage in physical layer secret communication systems, IEEE Commun. Mag. 53 (12) (2015) 19–25.
[9] Y. Zou, J. Zhu, X. Wang, V.C. Leung, Improving physical-layer security in wireless communications using diversity techniques, IEEE Netw. 29 (1) (2015) 42–48.
[10] J. Boutros, E. Viterbo, Signal space diversity: a power-and bandwidth-efficient diversity technique for the Rayleigh fading channel, IEEE Trans. Inform. Theory 44 (4) (1998) 1453–1467.
[11] G. Taricco, E. Viterbo, Performance of component interleaved signal sets for fading channels, Electron. Lett. 32 (13) (1996) 1170–1172.

[12] S.B. Slimane, An improved PSK scheme for fading channels, IEEE Trans. Veh. Technol. 47 (2) (1998) 703–710.
[13] N.F. Kiyani, J.H. Weber, A.G. Zajic, G.L. Stuber, Performance analysis of a system using coordinate interleaving and constellation rotation in Rayleigh fading channels, in: Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th, IEEE, 2008, pp. 1–5.
[14] M. Yusuf, H. Arslan, Enhancing physical-layer security in wireless communications using signal space diversity, in: 2016 IEEE International Conference for Military Communications, MILCOM, IEEE, 2016.
[15] M.K. Simon, M.-S. Alouini, Digital Communication over Fading Channels, vol. 95, John Wiley & Sons, 2005.
[16] H.A. David, H.N. Nagaraja, Order Statistics, Wiley Online Library, 1981.

Marwan Yusuf acquired his B.Sc. from Ain Shams University, Egypt in 2010 and M.Sc. from Istanbul Medipol University, Turkey in 2016 in Electrical, Electronics and Communications Engineering. His research interests include wireless communications and signal processing for 5G, Physical layer security and Internet-of-Things.



Hüseyin Arslan (IEEE Fellow) has received his BS degree from Middle East Technical University (METU), Ankara, Turkey in 1992; MS and Ph.D degrees in 1994 and 1998 from Southern Methodist University (SMU), Dallas, TX, USA. From January 1998 to August 2002, he was with the research group of Ericsson inc., NC, USA, where he was involved with several projects related to 2G and 3G wireless communication systems. Since August 2002, he has been with the Electrical Engineering Dept. of University of South Florida, Tampa, FL, USA, where he is a Professor. In December 2013, he joined Istanbul Medipol University to found the Engineering College, where he has worked as the Dean of the School of Engineering and Natural Sciences. He has also served as the Director of the Graduate School of Engineering and Natural Sciences in the same university. In addition, he worked as a part-time consultant for various companies and institutions including Anritsu Company, Savronik Inc., and The Scientific and Technological Research Council of Turkey.

Arslan's research interests are related to advanced signal processing techniques at the physical and medium access layers, with cross-layer designed for networking adaptivity and Quality of Service (QoS) control. He is interested in many forms of wireless technologies including cellular radio, wireless PAN/LAN/MANs, fixed wireless access, aeronautical networks, underwater networks, in vivo networks and wireless sensors networks. His current research interests are on 5G and beyond, physical layer security, interference management (avoidance, awareness, and-cancellation), cognitive radio, small cells, powerline communications, smart grid, UWB, multi-carrier wireless technologies, dynamic spectrum access, co-existence issues on heterogeneous networks, aeronautical (High Altitude Platforms) communications, *in vivo* channel modeling and system design, and underwater acoustic communications. He has served as technical program committee chair, technical program committee member, session and symposium organizer, and workshop chair in several IEEE conferences. He is currently a member of the editorial board for the IEEE Surveys and Tutorials and the Sensors Journal. He has also served as a member of the editorial board for the IEEE Transactions on Communications, the IEEE Transactions on Cognitive Communications and Networking (TCCN), the Elsevier Physical Communication Journal, the Hindawi Journal of Electrical and Computer Engineering, and Wiley Wireless Communication and Mobile Computing Journal.