A collaborative physical layer security scheme

Dimitrios Efstathiou
Department of Informatics Engineering, Technological Educational Institute of Central Maccedonia, Serres, Greece

Article Info

Article history:

Received May 9, 2018
Revised Nov 17, 2018
Accepted Dec 11, 2018

Keywords:

OFDM
Outage probability
Physical layer security
Pilot channel estimation
Secrecy capacity

ABSTRACT

High level of security is essential in wireless 5G communications. The last few years there has been an increase in research interest in the potential of the radio channel's physical properties to provide communications security. These research efforts investigate fading, interference, and path diversity to develop security techniques for implementation in 5G New Radio (NR). In this paper, we propose a collaborative scheme to existing physical layer security schemes, taking advantage of the characteristics of the OFDM technique. An OFDM symbol includes the pilot subcarriers, typically essential for the pilot channel estimation process performed at the legitimate receiver. In this work we propose the positions of the subcarriers to change on every OFDM symbol following a probability distribution known only to the legitimate transmitter and legitimate receiver. An eavesdropper, does not have access to the information of the pilot subcarriers positions so, it performs blind channel estimation. The theoretical analysis is based on the information theoretic problem formulation and is confirmed by simulations. The performance metrics used are the secrecy capacity and the outage probability. The proposed scheme is very simple and robust, strengthening security in multimedia applications.

Corresponding Author:

Dimitrios Efstathiou,
Department of Informatics Engineering,
Technological Educational Institute of Central Macedonia,
Terma Magnesias Street, Serres 62124, Greece.
Email: defstat@teiser.gr

1. INTRODUCTION

1.1. Background

The researchers pay much attention to security issues for the 5G New Radio (NR) physical layer. This has become mandatory due to the introduction of the all-IP technology, the growing number of subscribers, the interconnection of most networks to the internet and high privacy needs of some applications. The security running on today's smart devices is vulnerable to malware and other software-based attacks, as these devices are used in sensitive processes, like banking, location-based services, or even e-health applications, making them more attractive in attacks. So there is a need for further improvement and strengthening of 5G mobile communication security standards.

Most security protocols apply cryptographic techniques for bit scrambling at the upper layers of a wireless network by exploiting a shared secret key between pairs of communicating nodes. The main benefit of physical layer security – compared to cryptographic techniques - is that it can exploit the system resources, mostly the channel characteristics, like multipath propagation, without increasing the complexity much, compared to upper-layer security. Also, it can be used in conjunction with upper layer security schemes, like authentication, encryption, admission control, etc., providing stronger security. Several papers can be found in the recent literature for physical layer security. The tutorial paper by Fang *et al.* [1] present an overview of the physical layer secure schemes, dividing them into three spatial domain-based, time domain-based, and frequency domain-based. They conclude by presenting the open research issues and directions in this area.

Liu *et al*. [2] present a review of physical layer security research efforts based on coding, precoding, signal processing, and channel estimation technologies to tackle security related challenges as fading effects, partial/imperfect channel state information (CSI), compound channels PHY-key generation, and impersonation authentication attacks. Mukherjee *et al*. [3] present some approaches for secrecy based on channel coding design, along with a description of inter-disciplinary approaches based on game theory and stochastic geometry. Tsouri and Wulich in [4] propose a multiple access method for securing orthogonal frequency division multiplexing (OFDM) over wireless time-varying channels. The method uses reverse piloting for implementing superposition modulation with joint decoding at the receiver. It makes use of channel randomness, reciprocity, and fast decorrelation in space to secure transmission with low overheads. Zurita *et al* [5] address physical layer security in multiple- input-multiple-output (MISO) communications. Beamforming and artificial noise broadcasting are chosen to increase communications security. The target is an optimization strategy that intelligently sets the transmission power and the size of the "protected zone" to probabilistically achieve secrecy at a specified target secrecy rate. Swindlehurst in [6] assumes some prior knowledge of the eavesdropper's channel and focuses on the information theoretic concept of secrecy capacity in a MIMO system, using SINR as the security metric. Zhu *et al* [7] present a technique to secure downlink transmission in a multiple-input multiple-output (MIMO) system. They consider the channel state information of the eavesdropper to be unavailable at the legitimate transmitter, so they use linear precoding of data and artificial noise to enhance secrecy.

1.2. The problem

The 3GPP standards for 5G New Radio (NR) specify cryptographic methods to protect wireless data transmission. The 5G devices will range from the upper end ones that have built-in hardware and can use state-of-the art cryptographic algorithms down to low cost devices. Some of these low cost devices cannot include the additional circuitry, power consumption, and code space needed to perform the data processing of cryptographic methodologies. Due to the limited resources of some 5G devices we have to consider tradeoffs when we study system security and identify or derive new low complexity techniques to enhance security on transmitted data.

1.3. Proposed solution

Robust and low complexity physical layer security methods can supplement or replace cryptographic techniques. Information theoretic security methods use the fading estimation of wireless channels. In this paper we propose an extension of an enhancement scheme to existing physical layer security techniques for OFDM based systems [8]. The positions of the pilot subcarriers change from one OFDM symbol to the next according to a selected probability distribution between the predefined fixed positions within the OFDM symbols. The impact of number of pilot subcarriers in an OFDM symbol and the cycle prefix duration in the secrecy capacity and the utage probability is analysed and simulation results are presented.

2. RESEARCH METHOD

In this section, we describe the system model, the proposed technique and the analysis of secrecy capacity and outage Probability in a Rayleigh fading channel.

2.1. System model

Figure 1 presents the OFDM baseband system model that is used in this paper. At the transmitter (Alice), the source data are mapped into 16-QAM symbols and are combined with pilot symbols and formed to parallel subcarriers. The pilots and the data are equipowered, a fact that makes difficult for a potential eavesdropper (Eve) to detect the pilot subcarriers by measuring the received power signal envelope [9]. Data and pilot subcarriers are transformed to time domain by an inverse discrete Fourier transform (IDFT). A cyclic prefix of length Ncp is added to the IDFT output samples, which are then pulse-shaped to construct the time domain signal for transmission. We assume that both the main channel and the and the eavesdropper channel experience fading, where the channel gains remain constant during each coherence interval and change independently from one coherence interval to the next in the coherence interval. The received signal by Bob and eavesdropper, are given by

$$\begin{aligned} y_b(m) &= h_b(m)x(m) + n_b(m) \\ y_e(m) &= h_e(m)x(m) + n_e(m),\ m = 1, 2, \ldots N \end{aligned} \tag{1}$$

where N is the length of the transmitted signal per OFDM symbol, and $h_b(m)$ and $h_e(m)$ are the channel gains of the main and the eavesdropper channel respectively. Additionally, $n_b(m)$ and $n_e(m)$ are independent and identically distributed Gaussian noise with zero mean and unit variance corrupting the transmitted signal ($\sigma_b^2=1$, $\sigma_e^2=1$). The fading channel power gains of the main and the eavesdropper channels are denoted by $g_b(m)=|h_b(m)|^2$ and $g_e(m)=|h_e(m)|^2$. We assume that g_b and g_e are independent and identically distributed (i.i.d) random Rayeigh variables with parameters σ_b and σ_e, respectively.

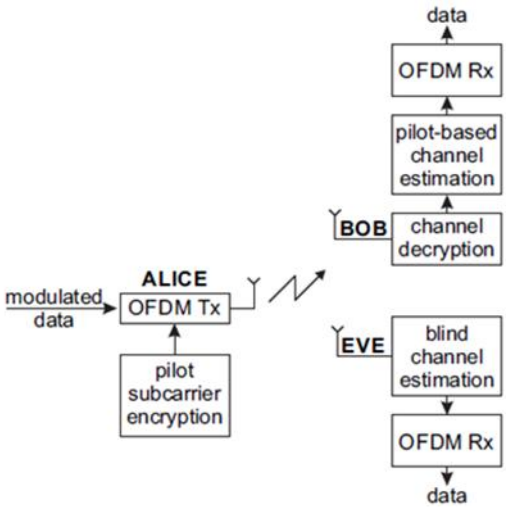


Figure 1. Block diagram for the wireless transmission between Alice and Bob in the presence of eavesdropper Eve

The channel estimation algorithms for OFDM receivers can be generally separated into two methods, pilot-based channel estimation and blind channel estimation. Pilot-based channel estimation estimates the channel information by obtaining the channel impulse response from the pilot subcarriers. The pilot subcarriers carry training symbols that are a priori known to the receiver. The blind channel estimation relies only on the received symbols to acquire channel state information (CSI) blindly. Compared with blind channel estimation, pilot-based channel estimation is a more effective method. Figure 2 presents the frequency description of an OFDM system that the pilot subcarriers are located 16 sub-carriers apart.

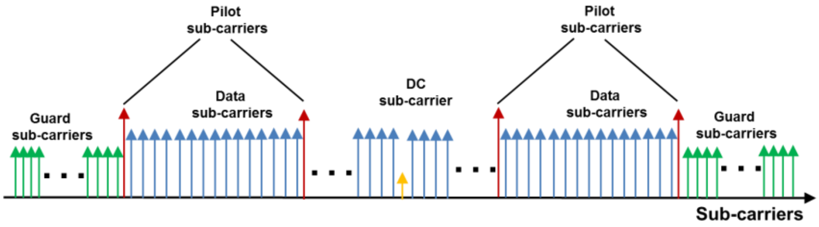


Figure 2. OFDM frequency description

Both the legitimate receiver and the eavesdropper know the position of the pilot subcarriers in the OFDM symbol, so they can perform pilot subcarrier channel estimation, demodulate, decode and decrypt the data that Alice transmits. In this work we propose the position of the pilot subcarriers to change from one OFDM symbol to the next using a discrete uniform probability distribution around the fixed pilot subcarrier positions defined in the technical specifications (IEEE 802.11, IEEE 802.16, LTE etc.). The probability distribution of the position of pilot subcarriers is generated once and shared between the legitimate transmitter and legitimate receiver during the authentication phase. The eavesdropper does not have access to this information, and thus inevitably has to perform blind channel estimation that is less effective compared to pilot subcarrier channel estimation.

We use the information theoretic problem formulation to study the security capacity and the outage probability of the proposed scheme. The secrecy capacity of fading wireless channel is explored in [10]-[13]. The proposed scheme is complementary to existing security techniques. Furthermore, it is targeted to multimedia communications, since these applications require high SNR and low bit-error probability performance as a quality of service (QoS) requirement [14],[15]. In this paper we investigate the impact of channel fading on the secrecy capacity and outage probability in the high signal-to-noise ratio (SNR) regime.

Based on the random coding argument introduced in [13],[16], we assume that Alice encodes a message block, represented by random variable W∈W={1, . . ., K}, into a codeword, represented by a random variable x^k = {x(1), x(2), . . ., x(k)} ∈ X^k, by using a stochastic encoder fk(·): W →X^k. The entropy G(W) is the amount of information of this transmitted message W. Bob decodes the received signal $y^k{}_b$ = {y_b(1), y_b(2), . . . , y_b(k)} ∈ Y^k by using a decoder q(·) : Yk → W. The transmission rate from Alice to Bob is given by R=G(W)/k. The measure for eavesdropper's uncertainty about W is defined as

$$R_e = \frac{1}{k} G(W|Y_e^k) \tag{2}$$

where G(W|Y_e^k) is the remaining entropy of W given that the value of Y_e^k is known. A secrecy rate R_s is achievable if there exists a (2^{kRs} , k) code for a sufficient large k such that $R_e \geq R_s - \varepsilon$ and for any given ε>0 [13]. Secrecy capacity of wireless channels is defined as the maximum information rate that the main channel can achieve in the presence of an eavesdropper. The secrecy capacity is then given by the expression:

$$C_s \square \sup remum\{R_s\} \tag{3}$$

We assume that the transmitter does not know the channel state information (CSI) of the main channel and the eavesdropper channel. The transmitter sets up a certain value for the information transmission rate Rs based on the statistical properties of the channel. We define that outage happens when the instantaneous secrecy capacity C_s is less than the target secrecy rate R_s.

2.2. Analysis of secrecy capacity and outage probability

The legitimate receiver (Bob) knows the pilot subcarriers' position per OFDM symbol and uses this information to perform pilot-based channel estimation. In contrary, the eavesdropper (Eve) does not have access to the information on pilot subcarriers' position and applies a blind channel estimation technique to demodulate Alice's transmitted data. Our analysis on secrecy capacity is based on the results of [12], [13] for the real-valued Gaussian wiretap channel. The transmitted signal power is given according to

$$\frac{1}{N} \cdot \sum_{i=1}^{N} E\left[x(i)^2\right] \leq P_s \tag{4}$$

where N is the number of samples in an OFDM symbol and P_s is the average transmit signal power. We assume that both Bob and Eve channel experience Rayleigh fading channel with channel gains h_b(m) and h_e(m) respectively. The channel gains remain constant over the coherence interval. We assume that the power of the noise in the main and the eavesdropper's channel is N_B and N_E, respectively. The instantaneous SNR for the channel between Alice and Bob is given by

$$\gamma_B = g_b \cdot (P_s/N_B) = |h_b|^2 \cdot (P_s/N_B) \tag{5}$$

Likewise, the instantaneous SNR for the channel between Alice and Eve is given by

$$\gamma_E = g_e \cdot (P_s/N_E) = |h_e|^2 \cdot (P_s/N_E) \tag{6}$$

The capacity of the channel between Alice and Bob is given by

$$C_B = \log_2\left(1 + g_b \cdot \frac{P_s}{N_B}\right) = \log_2(1+\gamma_B) \tag{7}$$

and the capacity of the channel between Alice and Eve is given by

$$C_E = \log_2\left(1 + g_e \cdot \frac{P_s}{N_E}\right) = \log_2\left(1 + \gamma_E\right) \tag{8}$$

The secrecy capacity is positive when $\gamma_B > \gamma_E$ and is zero when $\gamma_B \leq \gamma_E$ [15] and is given by

$$C_s = \begin{cases} \log_2\left(1+\gamma_B\right) - \log_2\left(1+\gamma_E\right) & \textit{if} \quad \gamma_B > \gamma_E \\ 0 & \textit{if} \quad \gamma_B \leq \gamma_E \end{cases} \tag{9}$$

From (7) we observe that when the main channel SNR is better than the eavesdropper channel SNR ($\gamma_B > \gamma_E$) the secrecy capacity of a complex AWGN is given by

$$\begin{aligned} C_s &= \log_2\left(1+\gamma_B\right) - \log_2\left(1+\gamma_E\right) = \\ &= \log_2\left(\frac{1+g_b\dfrac{P_s}{N_B}}{1+g_e\dfrac{P_s}{N_E}}\right) \square \log_2\left(\frac{1+g_b\dfrac{P_s}{N}}{1+g_e\dfrac{P_s}{N}}\right) = \leq \log_2\left(\frac{g_b}{g_e}\right) \end{aligned} \tag{10}$$

where the equality in the Equation (8) holds if P_s/N goes to infinity (very high SNR). The transmitter (Alice) has no information on h_b and h_e so it uses a constant code rate for each coherent interval, targeted for a predefined secure communication rate R_s. In our analysis we assume that the duration of the coherence interval is on the order of the length of the codeword at the output of the encoder. The outage probability is the probability that the instantaneous secrecy capacity C_s is less than a target secrecy rate $Rs > 0$.

$$P_{outage}(R_s) = P(C_s < R_s) \tag{11}$$

The main channel and the eavesdropper channel are independent and their instantaneous SNR is proportional to $|h_b|^2$ and $|h_e|^2$ so γ_B and γ_E follow the exponential distribution with probability density functions

$$p(\gamma_B) = \frac{1}{E\left[\gamma_B\right]}\exp\left(-\frac{\gamma_B}{E\left[\gamma_B\right]}\right), \quad \gamma_B > 0 \tag{12}$$

and

$$p(\gamma_E) = \frac{1}{E\left[\gamma_E\right]}\exp\left(-\frac{\gamma_E}{E\left[\gamma_E\right]}\right), \quad \gamma_E > 0 \tag{13}$$

In a fading channel there is some finite probability (in reality very small probability) that the instantaneous SNR of the main channel γ_B is higher than the instantaneous SNR of the eavesdropper channel γ_E (although the average SNR of main channel could be lower than the average SNR of the eavesdropper). The outage probability for a Rayleigh fading channel is given by the expression [17]

$$P_{outage}(R_s) = 1 - \frac{E\left[g_b\right]}{E\left[g_b\right] + 2^{R_s} E\left[g_e\right]\dfrac{\sigma_b^2}{\sigma_e^2}} \exp\left(-\frac{2^{R_s}-1}{E\left[g_b\right]\dfrac{P}{\sigma_b^2}}\right) \tag{14}$$

2.3. Channel estimation techniques

In this section we describe the channel estimation methods adopted by the legitimate receiver (Bob) and the eavesdropper (Eve). Bob knows the pilot subcarriers positions within every OFDM symbol, and, thus, can perform pilot-based channel estimation. In this work we use the least squares (LS) estimator described in [18] given by

$$\hat{h}_b = \left(E_p \cdot F_P^H \cdot F_P\right)^{-1} \cdot F_P^H \cdot P_D^H \cdot y_p \tag{15}$$

where, $E_p=E\{|p_m|^2\}$, p_m, $m=1,\ldots,N_p$ are the pilot symbols with power E_p, $P_D = \text{diag}(p_1, \ldots, p_{N_p})$, vector $\mathbf{y_p}$ consists of the output samples at the positions of pilot subcarriers and F_p is the N_p x L submatrix of the DFT matrix F corresponding to the pilots. In general case the channel impulse response is *L* samples. In our work L=1. The LS estimator used for Bob is a sub-optimal pilot-based channel estimator. Furthermore, both the pilot subcarriers and data subcarriers are equipowered, a fact that makes difficult for a potential eavesdropper to detect the pilot subcarriers by measuring the received power signal envelope.

Eve cannot find the exact position of the pilot subcarriers on per OFDM symbol basis, because the pilot subcarriers have non-fixed positions. Thus, she has to apply a blind channel estimation technique [9], [19], [20]. In this work we consider the iterative blind channel estimation technique proposed by S. Banani and R. Vaughan [9]. In this scheme, when an OFDM symbol is received, a decision algorithm estimates the data, and then, the primary data estimates are used for minimum MSE (MMSE) channel estimation.

The method is based on the knowledge of the channel frequency response estimate of the previous OFDM symbol interval $\hat{H}_e\left[n-1,k\right]$ (k-th subcarrier, n-1 OFDM symbol) and on the approximation of the first-order autoregressive (AR) process used for the relation between H[n-1, k] and H[n,k].

$$H_e\left[n,k\right] = \rho(T_{OFDM}) \cdot H_e\left[n-1,k\right] + \sigma_H \sqrt{1-\left|\rho(T_{OFDM})\right|^2}\, w\left[n,k\right] \tag{16}$$

where σ^2_H is the total average power gain of the channel $\sigma_H^2 = \sum_{l=1}^{L} \sigma_{h_l}^2$ (in our work L=1), w[n,k] is a white Gaussian process with variance equal to 1 and $\rho(T_{OFDM})$ is the normalized time correlation coefficient, specified by Jakes' model ($\rho(T_{OFDM})=J_0(2\pi f_D T_{OFDM})$) with f_D the maximum Doppler frequency and $J_0(\cdot)$ the zero-th order Bessel function of the first kind. When Eve receives the *n*-th OFDM symbol, uses a decision algorithm to obtain a primary data estimate of x[n,k], which is denoted $\hat{X}_{pri}[n,k]$, for the *k*-th subcarrier based on a constrained linear minimum mean square error (MMSE) criterion. Then, these estimates are applied to optimal MMSE channel estimator to estimate Eve's channel gain **h***e* given by

$$\hat{h}_e = \frac{F_L^H \cdot \hat{X}_{pri}^H \cdot y_e}{\left(A^{-1} + \frac{1}{\sigma_e^2} \cdot F_L^H \cdot \hat{X}_{pri}^H \cdot \hat{X}_{pri} \cdot F_L\right) \cdot \left(\sigma_e^2\right)} \tag{17}$$

where, $A = diag\left(\sigma_{h_1}^2, \sigma_{h_2}^2, \ldots, \sigma_{h_L}^2\right)$,

If all the constellation points of the signal have the same average energy E_s, then (17) can be simplified to

$$\hat{h}_e = B \cdot F_L^H \cdot \hat{X}_{pri}^H \cdot y_e \tag{18}$$

where B is a diagonal matrix with elements

$$B_{ii} = \frac{\sigma_{h_i}^2}{E_s \cdot \sigma_{h_i}^2 + \sigma_e^2}, \qquad i = 1,\ldots,L \tag{19}$$

Eve can estimate the channel gain $\mathbf{h}_e$ and detect the transmitted symbols. For the initialization of the described algorithm, we assume that Eve has access to the pilot subcarrier position only for first OFDM symbol.

3. RESULTS AND DISCUSSION

In this section, we present the system parameters used for the simulations and the corresponding results.We consider a fading channel where the channel gains remain constant during each coherence interval and change independently from one coherence interval to the next. We consider that the mean power of the channel is equal to 1 ($\sigma_{h_i}^2 = 1$). An OFDM system with N subcarriers is simulated, and the length of the cyclic prefix is set to N_{cp}. Thus, the OFDM symbol duration is equal to $T_{OFDM} = (N+N_{cp})T_s$, with T_s the duration of an input data symbol. The system was evaluated for N=256 subcarriers where N_p=8, 16, 32 are pilot subcarriers and rest subcarriers are allocated to transmit data. The pilot subcarriers and the data subcarriers use 16-QAM modulation scheme. The simulation takes in consideration that the legitimate receiver and the eavesdropper move with speed 50 km/h or 200 km/h or 500 km/h to the same direction. We assume that the legitimate receiver (Bob) estimates the channel gain using expression (15). The eavesdropper (Eve), estimates the channel using the blind method expression (18). Both receivers (Bob and Eve) estimate the input data for every OFDM symbol using the known minimum mean square error (MMSE) estimator

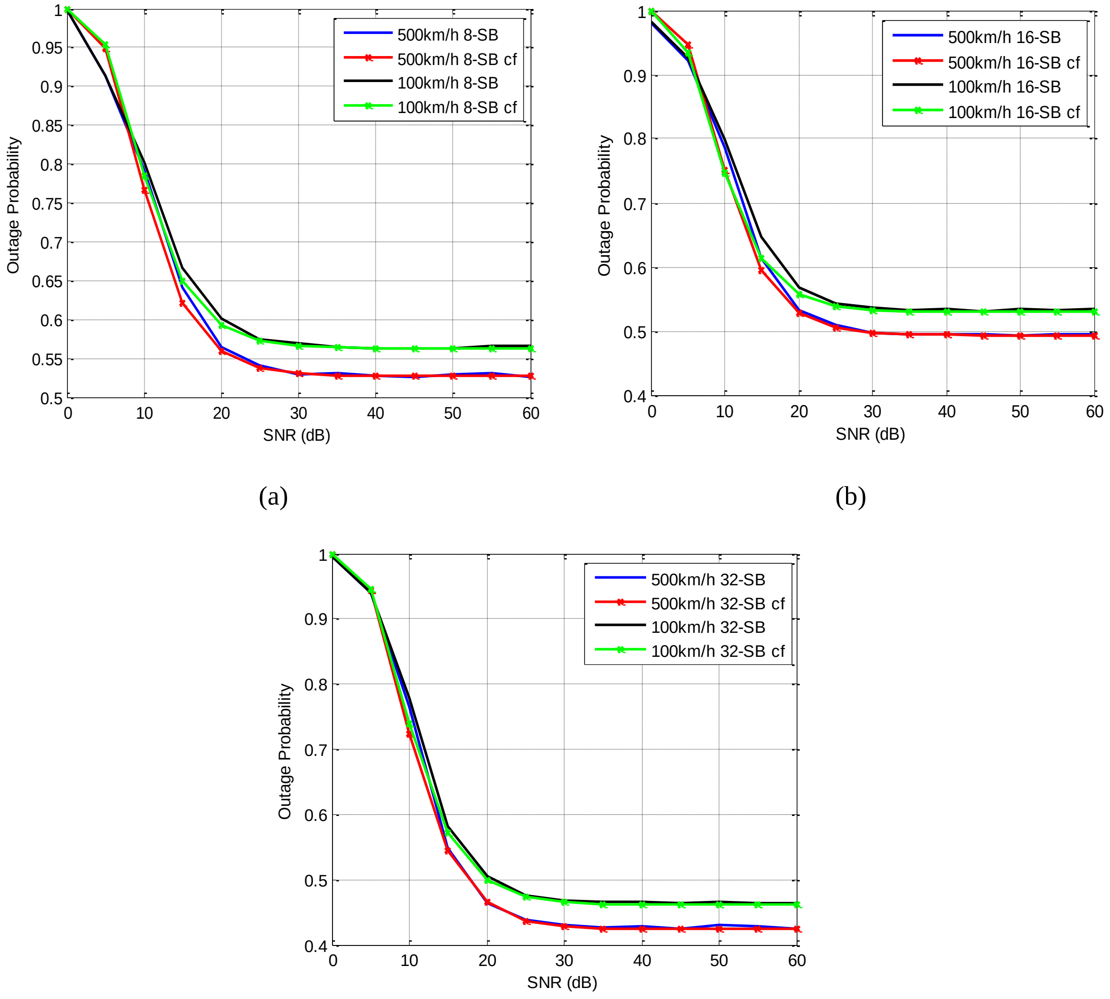
$$\hat{x}_b[m] = \left(\frac{\hat{H}_b[m]^*}{\frac{\sigma_{y_b}^2}{\sigma_x^2} + |H_b[m]|^2} \right) \cdot y_b[m], \; m = 1, \ldots., N$$

$$\hat{x}_e[m] = \left(\frac{\hat{H}_e[m]^*}{\frac{\sigma_{y_e}^2}{\sigma_x^2} + |H_e[m]|^2} \right) \cdot y_e[m], \; m = 1, \ldots., N \qquad (20)$$

Finally, a Viterbi decoder decodes the data at the output of the demodulator.

The figures presented below are created by running multiple simulations, in order to minimize the statistical errors and to assure the validity of the results. The metrics under test are the secrecy capacity and the outage probability.

Figure 3 shows the outage probability for an OFDM system with N=256 subcarriers with three configurations. The first configuration has 8 pilot subcarriers (Figure 3(a)), the second configuration has 16 pilot subcarriers (Figure 3(b)) and the third configuration has 32 pilot subcarriers (Figure 3(c)). The positions of the subcarriers carrying the pilot symbols change randomly on every OFDM symbol. The presented curves correspond to a mobile device velocity of 100 km/h and 500 km/h. The cyclic prefix duration is 1/8 of the OFDM symbol duration ($T_{CP}=T_{OFDM}/8$). The coherence interval is equal to the codeword length of 3 symbols. The solid lines present the simulation results and the lines with the markers present the curves based on the closed form expression (14). The simulation results are very similar to the curve provided by the closed form expression for SNR > 20 dB. Therefore, expression (14) can be used to estimate the outage probability in the high SNR region (25dB-60dB) that is appropriate for multimedia applications.



(a) (b)

(c)

Figure 3. Outage probability versus SNR for Bob and Eve

We observe that as the mobile device moves with higher velocity the outage probability decreases in high SNR region. This can be explained by the fact that Bob's receiver uses a pilot based channel estimator (Bob knows the pilot subcarrier positions on every OFDM symbol) and outperforms Eve's receiver that uses a blind channel estimator (Eve does not have access to pilot sub-carrier position) in fast fading radio channels. We observe as well, that the configuration of 32 pilot subcarriers provides a better agreement between simulation results and closed form expression for low SNR values.

Figure 4 shows a comparison of the the outage probability among the three configurations. Firstly, we notice that as the velocity of the mobile device increases the outage probability decreases. From Figure 4 we observe that as the number of pilot subcarriers increases the outage probability decreases, because Bob knows the pilot subcarrier positions on every OFDM symbol and its receiver outperforms Eve's receiver in a fast fading channel. So, we can perform a trade off between outage probability performance versus data throughput performance by changing the number of data subcarriers (N_D) and the number of pilot subcarriers ($N-N_D$) on the fly. We get the best outage probability performance when we use 32 pilot subcarriers (32-SB in Figure 4).

As an extension of the previous observation, we set the number of pilot subcarriers to 32 and we run simulations for various cycle prefix time duration ($T_{CP}=T_{OFDM}/8$, $T_{CP}=T_{OFDM}/16$, $T_{CP}=T_{OFDM}/32$) where T_{OFDM} is the OFDM symbol. The solid lines present the simulation results for mobile device velocity of 500 km/h and the lines with the markers present the simulation results for mobile device velocity of 100 km/h. From Figure 5 we observe that the outage probality is not affected by the cycle prefix time duration.

Figure 6 shows the secrecy capacity rate for an OFDM system with N=256 subcarriers with 8 pilot subcarriers, 16 pilot subcarriers and 32 pilot subcarriers positioned according to the proposed technique. The simulation results in Figure 6 correspond to a mobile device velocity of 100km/h and 500 km/h. The cyclic prefix duration is 1/8 of the OFDM symbol duration (T_{CP}=T_{OFDM}/8) . The coherence interval is equal to the codeword length of 3 symbols. As we expected the secrecy capacity increases as the SNR increases and Bob's receiver outperforms Eve's receiver. In the SNR vicinity of 30dB-60dB (BER < 10^{-6} at the output of the decoder that is appropriate for multimedia applications) the proposed scheme provides an extra secrecy capacity rate of about 0.25-0.34 bits/s/Hz to existing security schemes. We observe that the configuration of 32 pilot subcarriers outperforms the other two configurations (8 pilot symbols and 16 pilot symbols) in a matter of security capacity.

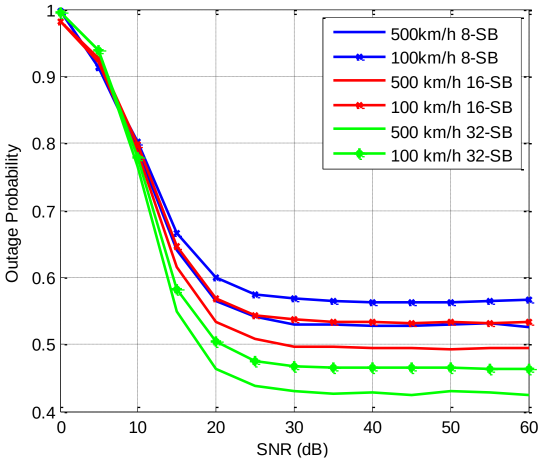


Figure 4. Comparison of outage probability among the three configurations

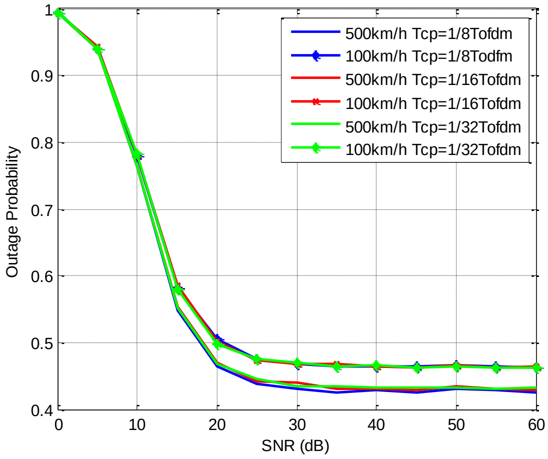


Figure 5. Outage probability versus SNR and T_{CP} time duration

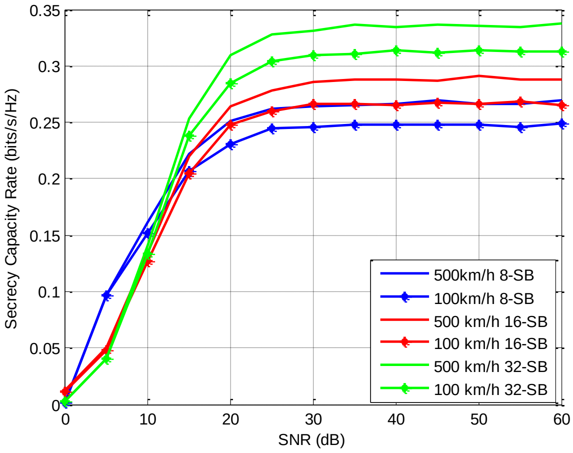


Figure 6. Secrecy capacity versus SNR for Bob and Eve

We observe as well that as the mobile device moves with higher velocity the average secrecy rate (bits/s/Hz) increases slightly in high SNR region, which comes in agreement with the observation that we made for outage probability in Figure 3.

As an extension of the previous observation, we set the number of pilot subcarriers to 32 and we run simulations for various cycle prefix time duration (T_{CP}=T_{OFDM}/8, T_{CP}=T_{OFDM}/16, T_{CP}=T_{OFDM}/32) where T_{OFDM} is the OFDM symbol. The solid lines present the simulation results for mobile device velocity of 500 km/h and the lines with the markers present the simulation results for mobile device velocity of 100 km/h. From Figure 7 we observe that the secrecy capacity is not affected by the cycle prefix time duration.

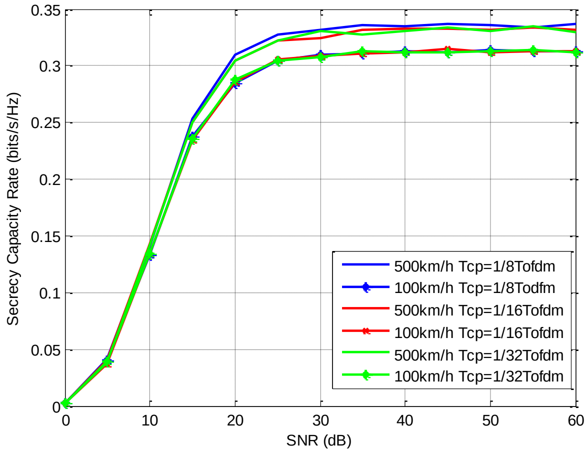


Figure 7. Outage Probability versus SNR and Cyclix Prefix time duration

The proposed scheme in this work provides a simple enhancement to secure communications for 5G New Radio (NR). This collaborative security scheme would not work to applications that can operate in low SNR values as voice transmission. The major advantage of the proposed scheme is that it is very simple, with minimal cost in complexity, thus processing time, a most important issue in communications security systems. Furthermore, the results are very promising when compared to other techniques.

Our research aim moving ahead is to perform a mathematical analysis of the secrecy capacity upper bound and outage probability lower bound with respect to the number of pilot subcarriers per OFDM symbol. We will derive closed form expressions for these two bounds and also a mathematical analysis of the computational complexity that the eavesdropper needs in order to be able to detect the positions of the pilot subcarriers.

4. CONCLUSION

This paper proposed a security scheme collaborative to existing physical layer security schemes, taking advantage of the characteristics of the OFDM technique. The positions of the subcarriers carrying the pilot symbols change randomly from one OFDM symbol to the next following discrete uniform probability distribution between the nominal positions of pilot subcarriers defined in the technical specifications. In the results section we showed the secrecy capacity and the outage probability in a fast fading channel. We showed that we can perform a trade off between outage probability performance and the data throughput by changing the number of data subcarriers and the number of pilot subcarriers accordingly. Finally, it was shown that the proposed scheme provides a good security enhancement for multimedia communication, for high SNR values where BER is low (BER<10^{-6}), with very low complexity.

ACKNOWLEDGEMENTS

The author wishes to acknowledge the financial support provided by the Research Committee of the Technological Educational Institute of Central Macedonia under the grant SAT/GS/15/1/17-01-2018.

REFERENCES

[1] W. Fang, *et al.*, “Information Security of PHY Layer in Wireless Networks,” *Hindawi Journal of Sensors*, vol. 2016, 2016.
[2] Y. Liu, *et al.*, “Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges,” *IEEE Communications Surveys & Tutorials*, vol/issue: 19(1), pp. 347-376, 2017.
[3] A. Mukherjee, *et al.*, “Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey,” *IEEE Communications Surveys & Tutorials*, vol/issue: 16(3), pp. 1550-1573, 2014.
[4] G. R. Tsouri and D. Wulich, “Securing OFDM over Wireless Time-Varying Channels Using Subcarrier Overloading with Joint Signal Constellations,” *EURASIP Journal on Wireless Communications and Networking - Special issue on wireless physical layer security*, vol/issue: 2009(1), pp. 18, 2009.
[5] N. Romero-Zurita, *et al.*, “PHY Layer Security Based on Protected Zone and Artificial Noise,” *IEEE Signal Processing Letters*, vol/issue: 20(5), pp. 487-490, 2013.

[6] A. L. Swindlehurst, “Fixed SINR solutions for the MIMO wiretap channel,” *Proc. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2009, Taipei, Taiwan*, pp. 2437-2440, 2009.

[7] J. Zhu, *et al.*, “Linear precoding of data and artificial noise in secure massive MIMO systems,” *IEEE Trans. Wireless Commun.*, vol/issue: 15(3), pp. 2245-2261, 2016.

[8] D. Efstathiou, *et al.*, “Enhancement of Transmission Security for OFDM Based Systems,” *Proceedings of ISCC’2017, Herakleio, Crete, Greece*, pp. 548-551, 2017.

[9] S. A. Banani and R. G. Vaughan, “OFDM With Iterative Blind Channel Estimation,” *IEEE Trans. Veh. Technol.*, vol/issue: 59(9), pp. 4298-4308, 2010.

[10] P. K. Gopala, *et al.*, “On the Secrecy Capacity of Fading Channels,” *IEEE Trans. Inf. Theory*, vol/issue: 54(10), pp. 4687-4698, 2008.

[11] Y. Liang, *et al.*, “Secure communication over fading channels,” *IEEE Trans. Inf. Theory*, vol/issue: 54(6), pp. 2470–2492, 2008.

[12] J. Barros and M. R. D. Rodrigues, “Secrecy Capacity of Wireless Channels,” *IEEE Int. Symp. Information Theory, Seattle, WA*, pp. 356–360, 2006.

[13] J. Zhu, *et al.*, “Outage Secrecy Capacity Over Correlated Fading Channels at High SNR,” *Proceedings of Information Processing Scociety of Japan, ICMU*, pp. 92-97, 2012.

[14] B. Come, *et al.*, “Impact of front-end non-idealities on bit error rate performance of WLAN-OFDM transceivers,” *Proc. IEEE Radio and Wireless Conference (RAWCON) 2000, Denver, CO, USA*, 2000.

[15] A. Sayeed and A. Perrig, “Secure wireless communications: Secret keys through multipath,” *Proc. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2008, Wisconsin, USA*, pp. 3013 – 3016, 2008.

[16] H. Jeon, *et al.*, “Bounds on Secrecy Capacity Over Correlated Ergodic Fad- ing Channels at High SNR,” *IEEE Trans. Inf. Theory*, vol/issue: 57(4), pp. 1975–1983, 2011.

[17] M. Bloch and J. Barros, “Physical Layer Security, From Information Theory to Security Engineering,” Cambridge University Press, pp. 177-211, 2011.

[18] T. Cui and C. Tellambura, “Semiblind Channel Estimation and Data Detection for OFDM Systems With Optimal Pilot Design,” *IEEE Trans. Commun*., vol/issue: 55(5), pp. 1053–1062, 2007.

[19] H. H. Zeng and L. Tong, “Blind Channel Estimation Using the Second-Order Statistics: Asymptotic Performance and Limitations,” *IEEE Trans. Signal Process.*, vol/issue: 48(5), pp. 2060–2071, 1997.

[20] O. Edfors, *et al.*, “OFDM channel estimation by singular value decomposition,” *IEEE Trans. Commun.*, vol/issue: 46(7), pp. 931939, 1998.

BIOGRAPHY OF AUTHOR

Dimitrios Efstathiou is an Assistant Professor in the Department of Informatics Engineering, Technological Educational Institute of Central Macedonia, Serres, Greece. He received a Diploma of Electrical Engineering from the Department of Electrical Engineering, University of Patras, Greece. He received a M.Sc. in Digital Electronics and a Ph.D. in the Mobile Telecommunication Systems from the Department of Electrical Engineering of King' College, University of London, United Kingdom. He has more than twenty-five years of professional and academic experience in the field of digital telecommunication systems. He was awarded four USA patents. He worked for Nokia Mobile Phones in Camberley, Surrey, United Kingdom. In 1996 he joined Analog Devices Inc. at Greensboro, North Carolina, USA. He contributed as a systems designer and project manager to the design of various digital integrated circuits. His current research interests include wireless body area networks (WBANs), Physical Layer Security, Cognitive Radio, Clock generation and distribution, Direct Digital Synthesizers (DDS), analogue and digital Phase Lock Loops (PLLs).