Technology Independent Security Aware OFDM (SA-OFDM)

Monette H. Khadr*, Hany Elgala*, Moussa Ayyash§, Thomas Little‡, Michael Rahaim† and Abdallah Khreishah**

*SUNY Albany, NY, USA, {mkhadr, helgala@albany.edu}
§Chicago State University, IL, USA, mayyash@csu.edu
‡Boston University, MA, USA, tdcl@bu.edu
†UMass at Boston, MA, USA, michael.rahaim@umb.edu
**NJIT, NJ, USA, abdallah@njit.edu

***Abstract*—Orthogonal frequency division multiplexing (OFDM) is currently the most prominent modulation technique, mainly due to it's spectral efficiency. To improve the security performance of OFDM based systems, multiple security approaches are proposed in literature, including physical-layer (PHY) approaches. However, these techniques are technology specific, *i.e.* mostly designed for radio frequency (RF) transmission and cannot be directly deployed in other technologies such as optical wireless communications (OWC). In this paper, security aware OFDM (SA-OFDM) is presented as a technology independent PHY security approach designed to suppress eavesdropping. The novelty of SA-OFDM is not only its versatility in deployment, but also in its perception in combining PHY encryption and the receiver's architecture to improve security performance. SA-OFDM is tested under additive white Gaussian noise (AWGN) and Rayleigh channel models, indicating negligible impact on system performance for both RF and OWC links. Results show that the eavesdropper becomes oblivious to the transmitted information, *i.e.* has a bit-error-rate (BER) of 0.5, which is equivalent to random guessing. Even if the key is seized, the eavesdropper's BER does not exceed 10^{-2}.**

***Index Terms*—PLS; HetNets; OFDM; OWC; PLE**

I. Introduction

Major factors are now driving the global wireless connectivity market including: Internet-of-Things (IoT), cloud computing, virtual reality (VR), and other wireless technological applications and devices. Concurrently, privacy is becoming more of a concern for users to ensure the confidentiality of their personal data. Due to the nature of wireless radio propagation, the physical-layer (PHY), *i.e.* the lowest layer of the protocol stack, is vulnerable to eavesdroppers [1]. However, security primitives are usually implemented in the upper layers of the protocol stack, while lower layer security functions are usually ignored and are system dependent. Thus, applications that send sensitive and private data on-the-fly such as healthcare senor nodes, which cannot perform the cryptographic methodologies' expensive mathematical calculations, suffer and are prone to data hacking. Consequently, PHY security must become an emanating requirement for wireless communication systems.

In order to conform with the increase in connectivity demands and to overcome the lack in spectrum, promising alternative or complement technologies to radio-frequencies technologies are proposed, such as optical wireless communications (OWC). Hybrid systems, also known as heterogeneous networks (HetNets), allow the coexistence of conventional radio frequency (RF) transmission, *e.g.* WiFi, with optical and are becoming a promising research area [2]. The integration of both technologies does not only improve the system's reliability and coverage area, it also offers unprecedented data rates [3]. Thus, attention needs to be forwarded towards common protocols designed for these integrated systems.

There are numerous research efforts dedicated for PHY security enhancements in RF-based systems and they can be divided into two approaches; physical-layer security (PLS) and physical-layer encryption (PLE). PLS techniques rely on the unpredictability of the wireless multipath channel to defend the transmission. However, unlike the RF channel, the optical channel is not rich scattering, hence lacks the unpredictability criterion. On the other hand, PLE schemes aim to protect the entire PHY packet by encrypting the data flow in the PHY modulation stages [4]. However, all cryptographic measures rely on the assumption that it is computationally infeasible for an eavesdropper to decipher the data without secret key knowledge, which is a statement that has not yet been mathematically proven if the eavesdropper has sufficient time and computation resources [5].

In this paper, a PHY security technique that can be adopted by several wireless technologies is introduced. Hence, enabling common protocols to be deployed in HetNets that combine legacy RF technology with recent directional wireless technologies such as millimeter wave, terahertz communications and OWC. While other work has demonstrated PHY security for orthogonal

M. H. Khadr, H. Elgala, M. Ayyash, T. Little, M. Rahaim and A. Khreishah, "Technology Independent Security Aware OFDM (SA-OFDM)," 2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Istanbul, Turkey, 2019, pp. 1-6, doi: 10.1109/PIMRC.2019.8904102.

frequency division multiplexing (OFDM) systems, the main contribution of the paper is presenting, for the first time, a technology independent technique. The analysis focuses on OFDM due to its wide adoption, however, the proposed scheme is generic and can be applied to non-OFDM systems. Security aware OFDM (SA-OFDM) combines PHY key-based approach, *i.e.* symbol level encryption key, along with a novel keyless approach that artificially degrades the eavesdropper's channel by redesigning the time-domain samples of the OFDM symbols. Thus, even if the eavesdropper is able by exhaustive computation to intercept the PHY encryption key, a distorted signal will be received instead and the secrecy of the transmission is reserved.

The organizational structure of the paper is as follows: Section II provides a brief background containing a literature review on previously developed OFDM security techniques. Section III presents the proposed system and in Section IV the simulation results are provided. Finally, the paper concludes in Section V.

II. Background

The de facto technique utilized in most recent wireless standards, *i.e.* IEEE 802.11 protocol suite and LTE, is OFDM. OFDM is used due to its high spectral efficiency and robustness to inter-symbol interference (ISI), as well as fading. The principle of OFDM is modulating data sequences by applying *N*-point inverse fast Fourier transform (IFFT) onto a series of orthogonal sub-carriers; producing N complex IQ samples corresponding to *N* sub-carriers. Conventionally, an *N*-point complex base-band time-domain OFDM symbol can be represented as

$$\begin{aligned} x_n &= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} X_i e^{j2\pi \frac{ni}{N}} \\ &= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} \{(\Re_i + j\Im_i)(\cos(ni\theta_N) + j\sin(ni\theta_N))\} \end{aligned} \tag{1}$$

where n is the time index of the signal and X_i is the k^{th} sub-carrier modulated signal and $\theta_N = 2\pi/N$. Additionally, X_i can be expressed as $\Re_i$ and $\Im_i$ representing its real and imaginary parts respectively and $e^{j2\pi \frac{ni}{N}}$ as $\cos(ni\theta_N) + j\sin(ni\theta_N)$.

In this paper, the analysis focuses on OWC as the directional wireless technology that compliments RF. Yet, it is important to note that SA-OFDM is also viable in millimeter and terahertz communications.

A. OFDM in OWC

Unlike RF systems, OWC systems mostly use intensity modulation and direct detection (IM/DD). The baseband signal, $x(t)$, does not modulate the amplitude and phase of the optical carrier; it modulates its intensity instead.Thus, $x(t)$ must be positive and real. Hence, conventional OFDM techniques cannot be directly used. At the transmitter's side of IM/DD based

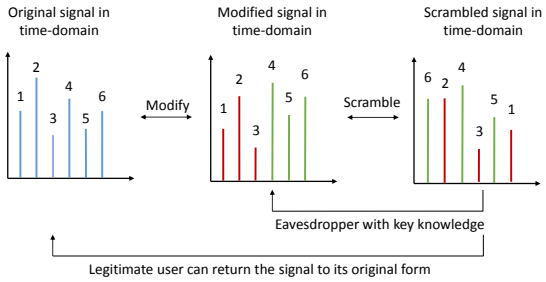


Fig. 1: PHY security enhancement based on time-domain manipulation in OFDM systems with the samples in the first group highlighted in red, while those of the second group are highlighted in green.

OFDM systems, the input vector to IFFT is designed to have Hermitian symmetry, hence, the time domain OFDM signal becomes real. Then, it becomes positive either by adding a DC bias, as in DC-biased Optical OFDM (DCO-OFDM), or by clipping at zero, as in asymmetrically clipped optical OFDM (ACO-OFDM). In this paper, DCO-OFDM is adopted due to it spectral efficiency for the optical link [6].

In OWC, the imaginary part of x_n is equal to zero, as a result of applying Hermitian symmetry as previously explained. Additionally, the received power from line-of-sight (LOS) path dominates those from the reflected paths. Hence, the multi-path response is usually ignored and the optical channel is recognized as a poor scattering environment. The two main sources of noise are the shot and thermal noise; their summation can be modelled as additive white Gaussian noise (AWGN). Thus, the AWGN channel model is widely adopted for bit-error-rate (BER) performance evaluation in OWC.

For quadrature-amplitude modulation (QAM), according to [7], the theoretical BER for moderate to large signal-to-noise ratios (SNRs), under AWGN and gray-coded assignment can be approximated as

$$\mathrm{BER}_{\mathrm{QAM}} = \frac{4}{log_2 M}\left(1 - \frac{1}{\sqrt{M}}\right) Q\left(\sqrt{\frac{3}{M-1}\mathrm{SNR}}\right) \tag{2}$$

where the Q-function is defined as

$$Q(m) \triangleq \int_m^\infty \mathcal{N}(\tau; 0; 1) d\tau \triangleq 1 - \Phi(m) \tag{3}$$

given $\Phi(m)$ is the cumulative distribution function of the normal Gaussian distribution and M is the QAM modulation order.

B. Literature Survey

There are a number of PHY security approaches that are specifically tailored for OFDM based systems in literature. However, all the attention is diverted towards RF systems and disregard OWC. Constellation rotation and weak artificial noise insertion is presented in [8] to improve time-domain synchronous (TDS)-OFDM based

systems. An eavesdropper-resilient OFDM system using a frequency domain sub-carrier interleaving algorithm is introduced in [9]. In addition, a combined chaotic scrambling and chaotic shift keying scheme for OFDM to enhance PHY security for cognitive-radio systems is demonstrated in [10]. While the aforementioned schemes improve security and mask some of the features of the OFDM symbol, each has its drawback. Some require perfect channel-state information (CSI) and rely heavily on spatial uniqueness, a stipulation that is difficult to achieve in OWC and terahertz communications. Others necessitate multiple transmitting elements, amplifying relays or require high computational complexity.

Two efforts focused on manipulating the time-domain OFDM symbols. Huo and Gong in [11] proposed a PLE technique that relied on varying the phase, *i.e.* sign, of the IQ samples of the OFDM symbols. As previously mentioned, optical time-domain OFDM symbols have to be real and positive, hence, this technique cannot be applied in OWC. Additionally, the analysis was limited to an AWGN channel model, which is a simplistic representation of the practical environment for RF transmission. In [12], the time-domain OFDM symbol is scrambled, *i.e.* the sample sequence in one symbol is rearranged. The findings in the paper were remarkable, yet, they were under the premise that the permutation order secret key can not be intercepted by an eavesdropper. In reality, the security of key sharing can not be guaranteed, hence, a technique that does not rely on this presumption is needed.

III. Proposed System

A. System Overview

The intuition of SA-OFDM is manipulating the OFDM time domain samples along with PLE to improve the security of transmission in the presence of an eavesdropper. In SA-OFDM, an extra dimension of PHY security is added by modifying the signal in a manner that is only known and can be reverted back by a legitimate receiver. Thus, even if the eavesdropper got a hold on the secret key or is able to retrieve the signal without it, the signal will still remain distorted and the error probability will be high after decoding. The concept of legitimate transmitter-receiver pre-shared key and parameters has been commonly adopted in highly acclaimed techniques such as frequency hopping, code division multiple access and key-based PLE techniques.

Firstly, the time-domain samples of the OFDM symbols, *i.e.* after IFFT, are divided in groups. The amplitude of the IQ samples are manipulated by a parameter α. Figure 1 shows an example of the realization, where the samples are divided into two groups with the first group reduced by α while the second is increased. This operation is equivalent to performing a nonlinear masking of the information symbols in the frequency domain. Then, the modified samples are scrambled based on a pre-shared key. Thus, the transmitted signal will be significantly varied over the frequency spectrum and will no longer exhibit OFDM characteristics. The OFDM symbol in (1) can also be represented as follows:

$$\begin{aligned} x^T = &(F_{\cos}^{-1}\Re^T - F_{\sin}^{-1}\Im^T) \\ &+ j(F_{\sin}^{-1}\Re^T + F_{\cos}^{-1}\Im^T) \end{aligned} \tag{4}$$

where $F_{\cos}^{-1}$ equals

$$\frac{1}{\sqrt{N}}\begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \cos(\theta_N) & \dots & \cos((N-1)\theta_N) \\ 1 & \cos(2\theta_N) & \dots & \cos(2(N-1)\theta_N) \\ \vdots & \vdots & & \vdots \\ 1 & \cos(i\theta_N) & \dots & \cos(i(N-1)\theta_N) \\ \vdots & \vdots & & \vdots \\ 1 & \cos((N-1)\theta_N) & \dots & \cos((N-1)^2\theta_N) \end{pmatrix} \tag{5}$$

with $[.]^T$ denoting the transpose operation and $F_{\sin}^{-1}$ is identical to $F_{\cos}^{-1}$ but the cosine functions are replaced by sines. An SA-OFDM modified signal, s, can be presented by

$$\begin{aligned} s^T = &(F_{\cos}^{-1}\Re^T - F_{\sin}^{-1}\Im^T + \alpha a^T) \\ &+ j(F_{\sin}^{-1}\Re^T + F_{\cos}^{-1}\Im^T + \alpha b^T) \end{aligned} \tag{6}$$

where a and b are two vectors of length N and their entries are equiprobable and $\in [-1, 1]$ to average the signal power increase. The parameter α is adjusted to maintain the peak-to-average power ratio (PAPR) of the OFDM symbol while preserving the security gain. Then, using an $N \times N$ scrambling matrix, M_Z, s is scrambled; mapping the i^{th} element into the j^{th} location. The scrambling function Z_n of N elements determines the scrambling sequence. For illustration, in Fig. 1, the original $s_n = [s_0, s_1, s_2, s_3, s_4, s_5]$ and the scrambled sequence is $\tilde{s}_n = [s_5, s_1, s_3, s_2, s_4, s_0]$, then: $Z_0 = 5, Z_1 = 1, Z_2 = 3, Z_3 = 2, Z_4 = 4, Z_5 = 0$. Hence, the scrambling matrix can be expressed as:

$$M_Z^T = \left(e_{Z_0}, e_{Z_1}, \dots e_{Z_{N-1}}\right) \tag{7}$$

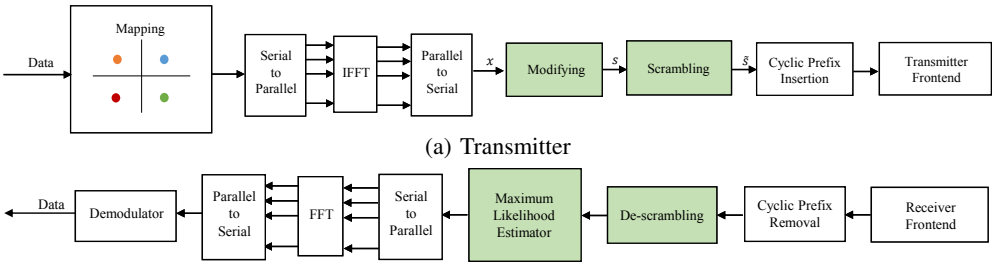
where e_{Zn} denotes an N-dimension row vector with only one element equal to one in the designated position and zero otherwise. An SA-OFDM transmitted signal, $\tilde{s}$ is

$$\tilde{s}^T = M_Z \;\; s^T \tag{8}$$

$$\begin{aligned} \tilde{s}^T = M_Z\big[&(F_{\cos}^{-1}\Re^T - F_{\sin}^{-1}\Im^T + \alpha a^T) \\ &+ j(F_{\sin}^{-1}\Re^T + F_{\cos}^{-1}\Im^T + \alpha b^T)\big] \end{aligned} \tag{9}$$

B. System Model

The block diagram of the proposed system is shown in Fig. 2, showing the stages to generate $\tilde{s}$. At the receiving end, since the legitimate user has the descrambling sequence based on the pre-shared key, the scrambling operation can be reverted. Then, using an optimal detector,



(a) Transmitter

(b) Receiver

Fig. 2: SA-OFDM System block diagram

i.e. maximum likelihood (ML) decoding, the variables a and b, explained in Section III, are estimated per OFDM symbol restoring back the signal to its original time-domain form. The proceeding steps are common for any OFDM receiver, the frequency domain signal, X, is obtained after the FFT operation. Then, the signal is passed to QAM demodulator and the transmitted data can be obtained, as depicted in Fig. 3(a). On the other hand, if the eavesdropper does not know the key, *i.e.* lacks the knowledge of the scrambling matrix Z_n, FFT will be directly performed on the received signal to recover the message $\hat{S}$:

$$\hat{S}^T = (F_{\cos} + jF_{\sin})\hat{s}^T = M_Z(F_{\cos} + jF_{\sin})s^T \quad (10)$$

where $F_{\cos} = F_{\cos}^{-1} = \cos(ik\theta_N)_{0\leq i,k<N}$ and $F_{\sin} = -F_{\sin}^{-1} = \sin(-ik\theta_N)_{0\leq i,k<N}$. Then,

$$\begin{aligned}\hat{S}^T =& M_Z(F_{\cos} + jF_{\sin})\big[(F_{\cos}^{-1}\Re^T - F_{\sin}^{-1}\Im^T + \alpha a^T) + \\ & j(F_{\sin}^{-1}\Re^T + F_{\cos}^{-1}\Im^T + \alpha b^T)\big]\end{aligned} \quad (11)$$

can be simplified as

$$\begin{aligned}\hat{S}^T =& M_Z\big[F_{\cos}^2\Re^T + F_{\sin}^2\Re^T + jF_{\cos}^2\Im^T + jF_{\sin}^2\Im^T + \\ & \alpha F_{\cos}a^T + \alpha F_{\cos}b + j\alpha F_{\sin}a^T - \alpha F_{\sin}b^T\big] \\ =& M_Z\big[\Re^T + j\Im^T + \alpha F_{\cos}(a+b)^T + \\ & \alpha F_{\sin}(ja-b)^T\big] \\ =& M_Z\big[X^T + \alpha F_{\cos}(a+b)^T + \alpha F_{\sin}(ja-b)^T\big]\end{aligned} \quad (12)$$

given that $F_{cos}F_{sin} = 0$ and $F_{cos}^2 + F_{sin}^2 = I$ where I is an $N \times N$ identity matrix. As observed in (11), the modification and scrambling operations cause constellation rotation when viewed in frequency domain. As a result, the eavesdropper's constellation is significantly distorted even at a signal-to-noise ratio (SNR) of 60dB as shown in Fig.3(b). Even if the eavesdropper was able to obtain the scrambling key, the constellation will be distorted by the components $\alpha F_{\cos}(a+b)^T + \alpha F_{\sin}(ja-b)^T$, causing the constellations given in Fig.3(c). The derivations listed above are analogous for OWC transmission, with the difference of the lack of the imaginary component and hence the constellations in OWC will only vary on the real axis and are portrayed in Fig.3(d). While the legitimate receiver, based on the system design, has the

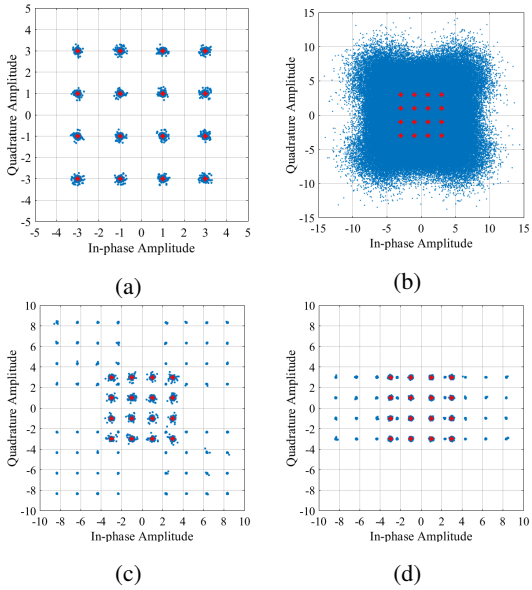


Fig. 3: Constellations of (a) the legitimate user and (b) eavesdropper with scrambling, while (c) eavesdropper without scrambling for RF and (d) eavesdropper without scrambling in OWC at 16-QAM with SNR = 60 dB and under Rayleigh channel for RF and AWGN for OWC.

ability to accurately estimate the parameters a and b, the eavesdropper requires 2^{2N} operations per OFDM symbol to guess them. For most wireless standards, the least number of OFDM subcarriers is 64, *i.e.* $N = 64$, which means that the eavesdropper requires 3.4×10^{38} operations per OFDM symbol for every possible value of α in order to restore the signal back to its original form in the time-domain. The reader may refer to our previous work published in [13] for further details on the receiver's ML estimator derivation.

C. Secrecy Capacity and PAPR

To quantify the security gain of the system, we used the most adopted metric for PHY security, secrecy capacity [5]. Secrecy capacity, C_s, can be defined as the difference between the channel capacities of the legitimate user C_u and the eavesdropper C_e as:

$$C_s = C_u - C_e = \log(1 + \frac{P}{N_u}) - \log(1 + \frac{P}{N_e}) \quad (13)$$

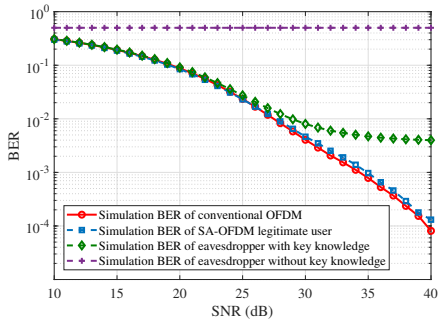


Fig. 4: BER performance of the 16-QAM RF link under a flat fading Rayleigh channel with a maximum doppler shift of 3 Hz, a delay spread of 20 ns and a channel bandwidth of 20 MHz.

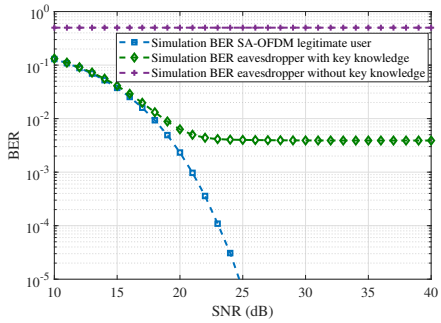


Fig. 5: BER performance of the 16-QAM RF link under AWGN channel at $\alpha = 0.05$.

where N_u and N_e are the user's and eavesdropper noise power respectively and P is the signal power. The eavesdropper's channel is degraded by the signal manipulation process described in the preceding subsections, which can be seen as artificial noise insertion, thus it becomes of lower quality when compared to that of the legitimate user. For an OFDM system, it can be redefined as:

$$C_s = \sum_{n=0}^{N-1} \Big(log(1 + \frac{P_n}{N_{nu}}) - \log(1 + \frac{P_n}{N_{ne}}) \Big) \quad (14)$$

where $\frac{P_n}{N_{nu}}$ and $\frac{P_n}{N_{ne}}$ are the user and eavesdropper SNR on the n^{th} sub-carrier, respectively. By definition, a positive C_s denotes that the system is able to avoid the data being intercepted by the eavesdropper.

Additionally, since peak-to-average power ratio (PAPR) is considered one of the major drawbacks of OFDM, the analysis includes PAPR calculations to examine the practicality of SA-OFDM. It can be defined as a measure of the peak signal power in comparison to the average power. It can be calculated using the formula,

$$\text{PAPR} = \frac{max|x_n|^2}{E[x_n]^2} \quad (15)$$

where $E[.]$ denotes the expectation operation.

IV. Results

SA-OFDM is firstly tested for the RF transmission under flat fading Rayleigh channel model and an AWGN channel model, the results can be observed in Fig.4 and Fig.5, respectively. The secrecy BER, which is the BER of the eavesdropper under the proposed technique, is evaluated given the premises of the eavesdropper having knowledge of the secret key and without. Under both channel models, the eavesdropper's BER without key-knowledge has a constant value of 0.5, *i.e.* equivalent to random guessing. However, even if the key is intercepted, assuming the signal is normalized to have a maximum of 1 and at $\alpha = 0.05$, the eavesdropper's BER saturates within the range of 10^{-2}. On the other hand, the legitimate user's BER remains unaffected and is consistent with the simulated BER of conventional OFDM, as depicted in Fig. 4. The PHY security gain is also depicted in Fig. 6, showing the secrecy capacity of SA-OFDM with and without the eavesdropper's knowledge of the utilized key. SA-OFDM excels without key knowledge, however, even with key knowledge the secrecy capacity always yields a positive value which is intuitively proportional with SNR. On the other hand, the performance of the proposed technique is also evaluated for the OWC link. To quantify the effect of the parameter α on the eavesdropper's BER performance, Fig. 7 shows the BER performance *vs.* SNR for the OWC link at 16-QAM DCO-OFDM at different values of α. As shown,

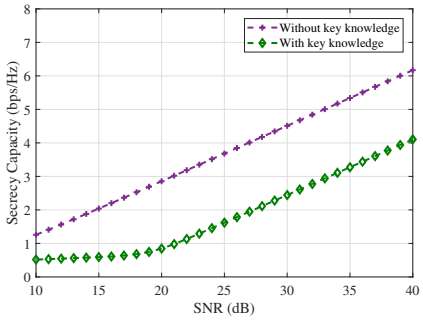


Fig. 6: Secrecy capacity, C_s, for the RF link at $\alpha = 0.05$ and 16-QAM OFDM transmission, the efficacy of SA-SM can be shown as C_s always maintains a positive value even with key knowledge.

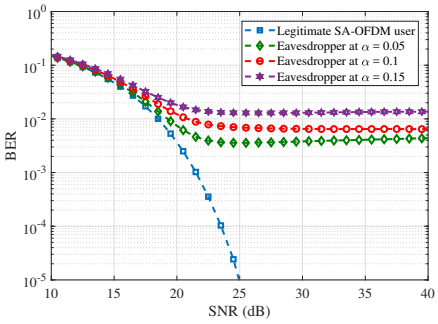


Fig. 7: The BER performance of the OWC link under various SNR levels showing the effect of α on the eavesdropper's BER at 16-QAM using DCO-OFDM assuming the eavesdropper has key knowledge.

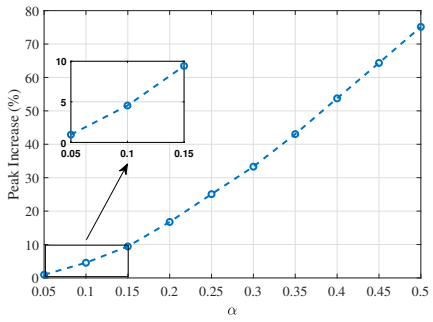


Fig. 8: The effect of α on the peak power showing that as α increases so does the peak power, hence, there is a trade-off between the eavesdropper's BER and the system's PAPR but can be avoided by using $\alpha = 0.05$.

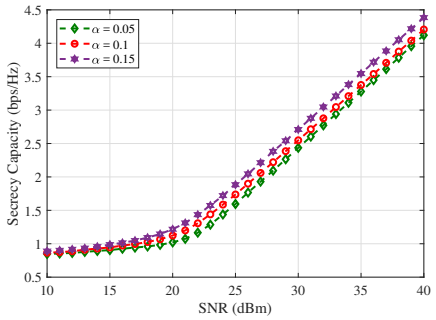


Fig. 9: Secrecy capacity for various α using the same simulation parameters for the OWC link, the efficacy of SA-OFDM can be shown as C_s is always positive.

even with key knowledge, the BER of the eavesdropper is less than 10^{-2} and is proportional to α, consistent with the results obtained in the RF link. In Fig. 7, the eavesdropper's BER at $\alpha = 0.15$ is 1.3×10^{-2}, while that at $\alpha = 0.05$ is 0.4×10^{-2} at SNR= 24 dBm, where the BER remains constant. However, increasing α effects the amplitude of the OFDM's peaks and in return effects the PAPR. The sequences a and b follow a uniform distribution with equal probability of either increasing the peak by α or reducing it, *i.e* probability of 0.5 to either increase or decrease the peak by the value α. Hence, the effect of α on increasing the peak power is averaged over 10^4 OFDM symbols and depicted in Fig. 8. At $\alpha = 0.05$, the peak power is increased only by less than 1% and at $\alpha = 0.15$ by 10%. It is important to note that the analysis focused on peak power, rather than calculating the PAPR, as the peak power is the restricting factor. Furthermore, to quantify the security gain of SA-OFDM, given the eavesdropper has key knowledge, the system's secrecy capacity is calculated for the OWC link and is presented in Fig. 9. Intuitively, the secrecy capacity C_s improves with α. Yet, even at $\alpha = 0.05$ the secrecy capacity persistently has a positive value, which naturally increases as the SNR value increases.

V. Conclusion

SA-OFDM is the first PHY security technique proposed for deployment in both conventional RF and OWC systems. The proposed technique restricted the eavesdropper's BER performance to random guessing, *i.e* BER = 0.5. Even if the key is intercepted, the BER is reserved below 10^{-2}. The performance of the proposed system is evaluated in terms of secrecy BER and secrecy capacity for both the RF and optical link. The effect of the proposed system on the OFDM's PAPR is also evaluated, showing a penalty of only 1% increase in peak power can enforce the BER of the eavesdropper to be 0.5 without key knowledge and 0.4×10^{-2} with key knowledge.

Acknowledgment

The authors are grateful for partial support by the NSF grant ECCS-1331018, the Engineering Research Centers Program of the National Science Foundation under NSF Cooperative Agreement No. EEC-0812056.

References

[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proceedings of the IEEE*, 104(9):1727–1765, Sept. 2016.

[2] M. Ayyash, H. Elgala, A. Khreishah, V. Jungnickel, T. Little, S. Shao, M. Rahaim, D. Schulz, J. Hilt, and R. Freund. Co-existence of WiFi and LiFi toward 5G: concepts, opportunities, and challenges. *IEEE Communications Magazine*, 54(2):64–71, February 2016.

[3] S. Shao, A. Khreishah, M. Ayyash, M. B. Rahaim, H. Elgala, V. Jungnickel, D. Schulz, T. D. C. Little, J. Hilt, and R. Freund. Design and Analysis of a Visible-Light-Communication Enhanced WiFi System. *IEEE/OSA Journal of Optical Communications and Networking*, 7(10):960–973, Oct. 2015.

[4] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong. Design of an OFDM Physical Layer Encryption Scheme. *IEEE Transactions on Vehicular Technology*, 66(3):2114–2127, March 2017.

[5] J. M. Hamamreh, H. M. Furqan, and H. Arslan. Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey. *IEEE Communications Surveys Tutorials*, pages 1–57, 2018.

[6] H. Elgala, R. Mesleh, and H. Haas. Indoor Optical Wireless Communication: Potential and State-of-the-Art. *IEEE Communications Magazine*, 49(9):56–62, Sep. 2011.

[7] J. G. Proakis and M. Salehi. *Digital Communications*. McGraw-Hill, New York, 5th edition, 2007.

[8] R. Ma, L. Dai, Z. Wang, and J. Wang. Secure Communication in TDS-OFDM System Using Constellation Rotation and Noise Insertion. *IEEE Transactions on Consumer Electronics*, 56(3):1328–1332, Aug. 2010.

[9] H. Li, X. Wang, and J. Chouinard. Eavesdropping-Resilient OFDM System Using Sorted Subcarrier Interleaving. *IEEE Transactions on Wireless Communications*, 14(2):1155–1165, Feb. 2015.

[10] A. Al-Talabani, A. Nallanathan, and H. X. Nguyen. Enhancing Physical Layer Security of Cognitive Radio Transceiver via Chaotic OFDM. In *2015 IEEE International Conference on Communications (ICC)*, pages 4805–4810, June 2015.

[11] F. Huo and G. Gong. A New Efficient Physical Layer OFDM Encryption Scheme. In *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, pages 1024–1032, April 2014.

[12] H. Li, X. Wang, and W. Hou. Secure Transmission in OFDM Systems by Using Time Domain Scrambling. In *2013 IEEE 77th Vehicular Technology Conference (VTC Spring)*, pages 1–5, June 2013.

[13] M. H. Khadr, H. Elgala, M. Ayyash, T. Little, A. Khreishah, and M. Rahaim. Security Aware Spatial Modulation (SA-SM). In *2018 IEEE 39th Sarnoff Symposium*, pages 13–18, Sept. 2018.