Obfuscation of Index Modulated OFDM Signals

Christos Efrosynis and Antonios Argyriou
Department of Electrical and Computer Engineering, University of Thessaly, Volos, Greece

***Abstract*—The goal of Physical Layer Security (PLS), is to make use of the properties, of the physical layer, in order to enhance wireless network security, without relying on higher layer encryption techniques [1]. Side channel attacks represent one of the most powerful category of attacks on cryptographic devices [2]. Machine learning techniques have proven their quality in a numerous applications where one is definitely side channel analysis. Many wireless traffic fingerprinting techniques, rely on detecting the modulation scheme, to derive the data rate and packet size, two important features of a traffic.**

In this paper, we exploit a beneficial attribute, of Multiple-Mode Orthogonal Frequency Division Multiplexing with Index Modulation (MM-OFDM-IM) system which is the ability of embedding/hiding a lower-order modulation scheme within the highest, available one, in an optimal way. In MM-OFDM-IM, all sub-carriers are activated, in order to transmit modulated symbols, that belong to different signal constellations/modes. Moreover, all permutations, of these distinguishable modes, are being used. Finally, in order to further improve the diversity order of the system, we propose a novel index modulation technique, which is based on the MM-OFDM-IM, the Sub-block Index MM-OFDM-IM (SI-MM-OFDM-IM).

I. Introduction

Wireless communications has always faced a very specific set of challenges and targeted very specific optimization metrics. These include reliability, power efficiency, throughput. At the same time, the privacy of wireless communications has been treated as an additional objective that is orthogonal to the ones, related to wireless performance. In particular, eavesdropping is a critical security problem in wireless networks due to the inherent broadcast nature of wireless communications [3]. An eavesdropper can fingerprint encrypted traffic by analyzing it's Side Channel Information (SCI). SCI can be used to extract certain statistical traffic features, such as packet size distribution, traffic volume, and inter-packet time sequence. For example, the modulation scheme used for the frame payload reveals the packet size and the data rate. The number of possible symbols of a modulation scheme, relates to the number of bits that can be modulated into a single symbol. A more noisy channel can support fewer bits per symbol, and the transmission of a fixed size payload can take different duration under different channel conditions. By measuring the frame duration (in seconds) and detecting the modulation scheme, an eavesdropper can estimate the packet size [4]. Traffic fingerprinting can lead to user privacy breaches since it can lead to discerning its identity, activity, and interests [5].

At the same type a new type of modulation has emerged, namely index modulation (IM). IM refers to a signal modulation concept, that relies on the activation states of a fraction of the communications resources/building blocks [6]. IM modulates signals through the indices of some medium, which can be either physical such as antenna, frequency carrier and sub-carrier or virtual, such as time slot, space time matrix, and antenna activation order. A distinct feature of IM is that, part of the information is implicitly embedded into the transmitted signal.

In OFDM-IM systems [7], [8], IM is being performed in the frequency domain by using as medium the OFDM sub-carriers. The indices of the active sub-carriers, are determined according to the data bits. Only two modes are permitted, the null and the conventional $\mathcal{M}$-ary modulation. The null mode itself doesn't carry any information. The OFDM-IM signal can be detected efficiently by a low-complexity maximum-likelihood (ML) detector or a log-likelihood ratio (LLR) detector. The bit error performance of an OFDM-IM system is identical to that of the OFDM, while imposing the same or lower computational complexity. [6].

However, OFDM-IM does not make the most efficient use of resources, so that it maximizes the available throughput since there are unused sub-carriers. To avoid this one, we can upgrade the previous system into an MM-OFDM-IM [9] system in which all sub-carriers are fully used. MM-OFDM-IM exploits all n sub-carriers in each sub-block with n different signal constellations. MM-OFDM-IM uses all permutations of these constellations to apply IM. In order to achieve the modulation obfuscation, we propose a scheme based on MM-OFDM-IM, and, a novel index modulation technique, the Sub-block Index MM-OFDM-IM (SI-MM-OFDM-IM), which is an enhanced diversity MM-OFDM-IM system.

In this work we are interested to improve the privacy of wireless communications by obfuscating the used modulation by the transmitter through IM. Contrary to other works of IM, bits are mapped to QAM symbols and sub-carriers so that they mimic a fixed constellation for the duration of a wireless frame. Disjoint M-ary constellations are used repeatedly on each sub-carrier with maximum and equal sized distances. In this way, a lower-order modulation scheme is optimally and securely embedded within the symbols of the highest-order modulation scheme.

The contributions of this work are the following:

- A novel scheme for signal obfuscation based on IM that does not compromise SE.
- A novel method for one-to-one index mapping and a low complexity ML detector based on [9].
- We propose an enhanced diversity MM-OFDM-IM system, which performs an extra indexing in sub-block level.
- To enhance communication secrecy even more, we propose the use of a symmetric encryption method, by using as encryption key, the index bits of each sub-block.
- We test the BER performance of our MM-OFDM-IM, compared with those of OFDM and OFDM-IM, by us-

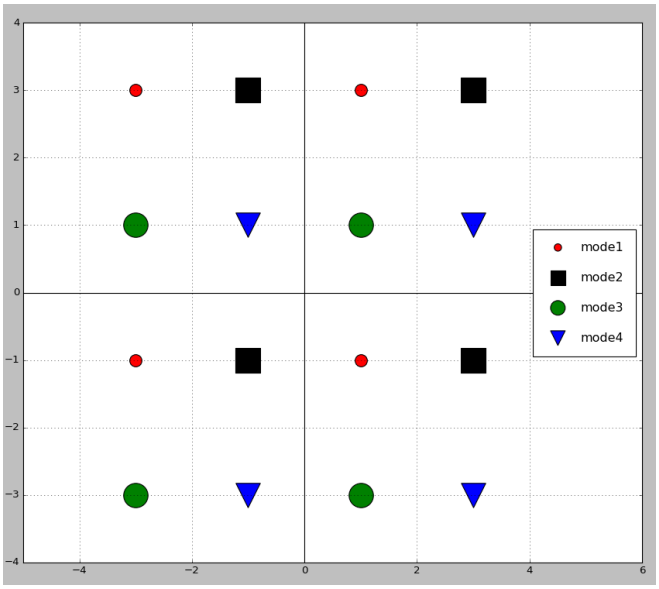

Figure 1. Hiding four 4-QAM modulation schemes into a 16-QAM by using a four mode system. There are n =4 sub-carriers in this OFDM sub-block and the modulation scheme/constellation used by each subcarrier is indicated with different color/symbol. Each one of the four modes in this example is selected by the index bits. AA: Ayta ta constellations den katalavainw pws kai an einai diaforetika apo tin eikona p.x. 3 sto [9] (ekei aplws exei BPSK) CE: Aftos xrhsimopoiei diaforetikh texnikh partitioning. Diathrei metavlhto to plhthos twn sybmolwn ana signal constellation. Se ola ta papers pou vrhka, sxetika me MM-OFDM-IM, ta constellations htan paromoia logw ths logikhs tou MIRD kai MIAD, pou anaferw oti phrame apo to [9]

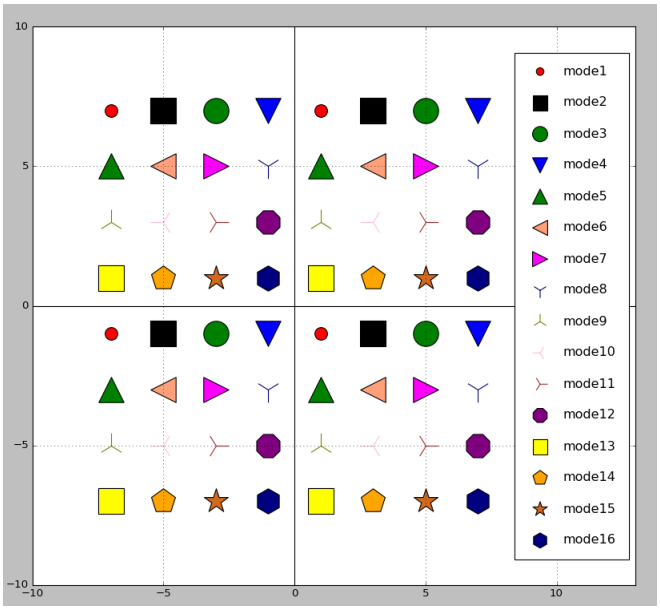

Figure 2. Hiding sixteen 4-QAM modulation schemes into a 64-QAM by using a sixteen modes system. Each one of the sixteen modes in this example is selected by the index bits.

ing Monte Carlo simulations and the robustness of the proposed modulation obfuscation technique, by using a deep learning technique, based on Convolutional Neural Networks (CNN).

It is shown that the proposed scheme exhibits a very flexible structure that is capable of encompassing conventional OFDM as a special case. It is also shown that the proposed scheme is capable of considerably outperforming the other OFDM-IM schemes and conventional OFDM in terms of error and SE performance while preserving a low complexity structure.

Symbol	Meaning
$NFFT$	Size of the DFT.
n	No OFDM sub-carriers per OFDM sub-block.
u	No constellation sets.
v	Length of a sub-sub-block.
$\mathcal{M}$	Highest available modulation scheme
$\mathcal{M}_i$	Obfuscated modulation scheme
q	No different signal constellations
$g1$	No sub-block index bits
$g2$	No mode bits
$g3$	No data bits

Table I
NOTATION USED IN THIS PAPER.

II. Transmitter and Channel Model

A. Transmitter Architecture

In this paper matrices are denoted with capital bold letters, i.e. $\mathbf{A}$. Bold lowercase letters denote vectors, i.e. $\mathbf{a}$. Finally the notation $\|\cdot\|$ is the Euclidean norm.

We propose a novel Sub-block Indexed MM-OFDM-IM (SI-MM-OFDM-IM) system. The SI technique is introduced into MM-OFDM-IM to improve the diversity order. MM-OFDM-IM is built on top of an OFDM system, in which, each OFDM sub-block consists of n OFDM sub-carriers (out of the $NFFT$ total) and n different signal constellations. The basic idea of the SI-MM-OFDM-IM is to divide sub-carriers and modes into u groups each (i.e. we divide the OFDM sub-block into u OFDM sub-sub-blocks). Each of the u groups of modes is called, a constellation set. In this way, we enhance the diversity order of our system by adding an extra level of indexing, which is the mapping of each constellation set into one of the u sub-sub-blocks (Fig. **??**).

So, first, m incoming bits are given as an input to the transmitter, and are divided into G blocks, each one containing

$$p = m/G \tag{1}$$

bits. Each one of these G blocks refers to a group of OFDM sub-sub-blocks. Since each group has n sub-carriers and it consists of u sub-sub-blocks, every sub-sub-block has

$$v = n/u \tag{2}$$

OFDM sub-carriers. AA: Also $n = NFFT/G$. Hence, each OFDM sub-sub-block is denoted as

$$\mathbf{X}_{(s)} = [X((s-1)u+1) \;\; X((s-1)u+2) \;\; \ldots \;\; X(su)]^T$$

with $1 \leq s \leq u$. The OFDM sub-block has the form

$$\mathbf{X}^{(b)} = [\mathbf{X}^T_{(1)}((b-1)n+1) \;\; \mathbf{X}^T_{(2)}((b-1)n+2) \;\; \ldots \;\; \mathbf{X}^T_{(u)}(bn)]^T$$

with $1 \leq b \leq G$

Because each OFDM sub-block $\mathbf{X}^{(b)}$ undergoes the same processing procedure, we focus our analysis on a single sub-block. Each constellation set corresponds to one sub-block.

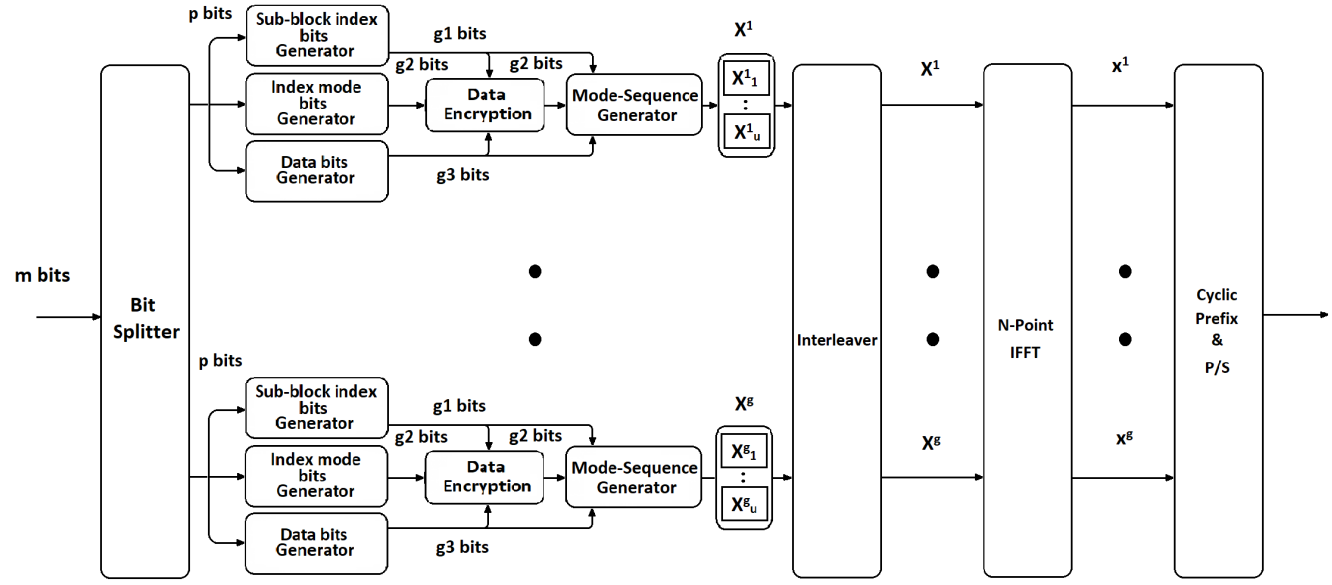

Figure 3. System model of the SI-MM-OFDM-IM transmitter, including encryption. AA: Gia oles tis eikones vale sto Dropbox to original arxeio pou tis ekanes etsi wste na to metatrepsw se pdf. Ypothetw sto libbreoffice impress?

The p bits are separated into three groups. The first group, with length

$$g_1 = \lfloor \log_2 (u!) \rfloor \tag{3}$$

bits, referred as the *sub-block index bits*. This number of bits is tied to u with this expression since $\log_2 (u!)$ is equal to the number different ways we can order of the u constellation sets, that will be used by the u sub-sub-blocks. The second group of bits, where bits are also transmitted through indexing like before, has a length of

$$g_2 = u \lfloor \log_2 (v!) \rfloor \tag{4}$$

bits, and are referred to as the *mode index bits*. Similarly with before, this number determines the order of the signal constellations $[X_1, ..., X_v]$, that will be used by the v sub-carriers in each sub-sub-block. All the valid signal constellations are different. This means that symbol $X(i)$ that will be transmitted in the i-th subcarrier is an $\mathcal{M}_i$-ary QAM signal (where $\mathcal{M}_i$ is the signal constellation for this i_{th} sub-carrier), which is assumed to be non-overlapping with any one of the other constellations $X(j)$ (where $j \neq i$, $i \in \{1, ..., v\}$ and $j \in \{1, ..., v\}$). Finally, the third group of bits, with length

$$g_3 = n \log_2(|\mathcal{M}_i|) \tag{5}$$

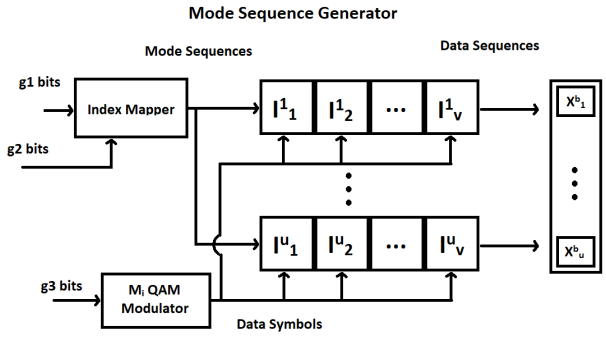

Figure 4. Mode Sequence Generator Block for the SI-MM-OFDM-IM.

bits, corresponds to the n symbols, that will be transmitted over the sub-carriers of the entire OFDM blocks based on the selected signal constellations.

Now each group of the p information bits is fed into the Mode-Sequence Generator (MSG) (Fig. 4) for generating the u OFDM sub-sub-blocks. After the MSG, we can get the mode

pattern for the b-th OFDM sub-block as

$$\mathbf{I}^b = \begin{bmatrix} I^b_{1,1} & \dots & I^b_{1,v} \\ \vdots & \ddots & \\ I^b_{u,1} & \dots & I^b_{u,v} \end{bmatrix} \tag{6}$$

where the (z, j)-th element refers to the selected signal constellationAA: you mean constellation? used in the j-th sub-carrier which belongs to the z-th sub-sub-block (Fig. 4).

After the mapping, an $NFFT$-point IDFT operation is performed following the concatenation of the G different OFDM groups of sub-blocks. CE: Next the Cyclic Prefix (CP), of length L is added, and the resulting signal:

$$\mathbf{x} = [x_1, ..., x_d] \tag{7}$$

(where $d = NFFT + CPL$) which is a time-domain symbol sequence, AA: einai swsto ayto? afou les meta oti vazeis to prefix. CE: Nai kanonika eprepe na einai meta to CP. is then fed into a parallel to serial converter, to generate the transmit signal.

This is followed by the digital-to-analog conversion (D/A) and power amplification before transmission.

B. Channel Model

We assume the received signal is affected by the presence of a frequency selective Rician fading channel [10] whose time domain channel impulse response (CIR) coefficient vector for the single-input single-output (SISO) fading channel is $\mathbf{h} = [h_1, ..., h_r]$ where r is the number of channel taps.

We assume that, the CP length is no smaller than the number of channel taps, r so that ISI is eliminated. After the removal of the CP from the received signal and the application of the $NFFT$-point DFT, the received signal in frequency domain (FD) can be derived as

$$\mathbf{X}_r = \mathbf{H}\text{diag}\{\mathbf{X}\} + \mathbf{W} \tag{8}$$

CE:

$$\mathbf{y} = \mathbf{h}\ \text{diag}\{\mathbf{X}\} + \mathbf{w} \tag{9}$$

$\mathbf{H} = \text{diag}\{\mathbf{h}\}$ AA: Afairesa to i to opoio anaferotan sta subcarriers. where $\text{diag}\{\mathbf{X}\}$ is a diagonal matrix with it's diagonal elements of $\mathbf{X}$ and $\mathbf{W}$ is the Additive White Gaussian Noise (AWGN) in the FD.

$$\mathbf{y} = [y_1, ..., y_d] \tag{10}$$

$$\mathbf{h} = [h_1, ..., h_d] \tag{11}$$

$$\mathbf{w} = [w_1, ..., w_d] \tag{12}$$

(where $d = NFFT + CPL$)AA: Kai pali to idio edw?

C. Performance Analysis

In this section we are going to analyze the SE of our models. By ignoring the CP, the SE is given by:

$$\text{SE}_{\text{MM-OFDM-SIM}} = \frac{Gp}{NFFT} \tag{13}$$

As defined above, the SI-MM-OFDM-IM transmits G blocks of $g1$, $g2$ and $g3$ bits by the sub-block and mode indices, and the constellation symbols on $NFFT$ sub-carriers. So the SE of this scheme is given by:

$$\text{SE}_{\text{MM-OFDM-SIM}} = \frac{G(\lfloor \log_2(u!) \rfloor + u\lfloor \log_2(v!) \rfloor + q\log_2(|\mathcal{M}_i|))}{NFFT} \tag{14}$$

Remark. *Since, we can independently adjust the $NFFT$, the n, the q and the G to achieve the desired SE, the proposed schemes has an excellent flexibility.*

III. Constellation Design for Obfuscation

Unlike other works on IM, we are concerned with modulation obfuscation. Consequently, we have to find a strategy for constructing the n signal constellations that will be used in the sub-carriers of an OFDM sub-block in such a way that they mimic a valid constellation. Assume that we want to communicate over the specific sub-block with an $\mathcal{M}$-ary modulation that consists of $|\mathcal{M}|$ possible symbols. We cluster the $|\mathcal{M}|$ symbols of the $\mathcal{M}$-ary constellation into a number of disjoint partitions that each one has the same size $|\mathcal{M}_i|$. E.g. in Fig. 1 $|\mathcal{M}|$=16 and so we have 4 disjoint partitions with $|\mathcal{M}_i|$=4 for each one of them. We consider $\mathcal{M}_i = \{M_{i,1}, .., M_{i,n}\}$ as the positions of the constellation points that belong to the same signal constellation, i.

$$\mathcal{M} = \bigcup_{i \in \{1,..,n\}}^{\forall i} \mathcal{M}_i \tag{15}$$

Fig. 1 and Fig. 2, illustrate the optimal partitioning for 16-QAM and 64-QAM modulation schemes, the points of each set are uniformly distributed. The resulting diagram, which corresponds to the entire block's modulation scheme, is similar to the distribution of the points, of a random modulation scheme (16QAM and 64QAM). This allows us to hide our modulation scheme $\mathcal{M}_i$ (where $\mathcal{M}_i$ is the modulation scheme for the i-th sub-carrier), into a higher order modulation, namely $\mathcal{M}$.

Due to the fact, that a high modulation order, is more susceptible to demodulation errors, we need to position the points in the optimal way. At a given signal-to-noise ratio (SNR), the probability of the demodulation error is inversely proportional to the minimum Euclidean distance between the symbols. According to the analysis in [9], the optimal mode selection, must satisfy the Minimum Intra-Mode Distance (MIAD) criterion:

$$\begin{aligned} e1 = \min_{i,j \in \{1,..,2^p\}} \left\| diag\{\mathbf{x}^b_i\} - diag\{\mathbf{x}^b_j\} \right\|^2 \\ s.t.\ E\{\left\| diag\{\mathbf{x}^b \right\|^2\} = n\ and \\ r_{min} = \min_{i,j \in \{1,..,2^p\}} rank(diag\{\mathbf{x}^b_i\} - diag\{\mathbf{x}^b_j\}) = 1 \end{aligned} \tag{16}$$

and the the Minimum Inter-Mode Distance (MIRD) criterion

$$e2 = \min_{i,j\in\{1,..,2^p\}} \left\|diag\{\mathbf{x}_i^b\} - diag\{\mathbf{x}_j^b\}\right\|^2$$
$$s.t.\ E\{\left\|diag\{\mathbf{x}^b\right\|^2\} = n \ and \quad (17)$$
$$r_{min} = \min_{i,j\in\{1,..,2^p\}} rank(diag\{\mathbf{x}_i^b\} - diag\{\mathbf{x}_j^b\}) = 2$$

(where $diag\{\overrightarrow{x}_i^b\}$ and $diag\{\overrightarrow{x}_j^b\}$ are two diagonal matrices, containing two different realizations of $\overrightarrow{x}^b$ $(i \neq j)$.

More specifically, in the case of criterion (16), we have $r_{min} = 1$, which arises from the error caused between symbols that belong to the same signal constellation in the high SNR region. So, maximizing the MIAD, leads to the optimal BER performance for our system, at high SNR. The criterion of (16), only considers the high SNR values, which does not necessarily ensure a good BER performance, in the medium SNR region, owing to the two diversity order protection of the index bits. According to [9], we can achieve a better BER performance at medium SNR, by using the criterion (17) and selecting n solutions out of those provided by the (16).

In particular, the criterion (17), takes into account two error events, the error caused by incorrectly demodulating two symbols belonging to two different signal constellations or mistaking the permutation of any two signal constellations, and so r_{min}=2. The probability of the first error case, can minimized based on (16). So, in order to maximize the MIRD, we have to minimize the probability of the second error case, given the results of the (16) criterion and we can do that by filtering the solutions of (16), leaving those, maximizing the MIRD.

For this design, we decided to use the QAM modulation scheme, which does not allow us, to maximize MIAD and MIRD at the same time due to its structure. According to our analysis, we conclude that, it is preferable for us to maximize the MIAD, owing to the larger number of modulation bits. To satisfy the MIAD criterion, *we propose a novel partitioning of the constellation points* which is based on the circle packing problem. Packing of circles in a square, is equivalent to distributing points in a square. The latter are then the circle centers. "Distance" is here the greatest distance of these (constellation) points. The maximum circle diameter, specifies, how far, two adjacent grid points, that belong to the same signal constellation, can be. Ideally, every element of $\mathcal{M}_i$, should be surrounded by as many elements of other sets, as possible in order to maximize MIAD. We divide the $|\mathcal{M}|$ constellation points into n, non-overlapping groups (18), i.e.,

$$\bigcap^{\forall i} \min(\mathcal{M}_i) = \varnothing \quad (18)$$

AA: Ti einai ayth h eksiswsh? CE: Apeikonizei mathimatika th non-overlapping idiothta twn constellation signals. Also, for different values of $\mathcal{M}$, we want, the number of groups to be proportional to $\mathcal{M}$, due to the two diversity order protection of the index bits. So in each group, we have to keep the number of points constant, and equal to four.

As we can see from Fig. 1 and Fig. 2, which illustrate an optimal partitioning for 16-QAM and 64-QAM modulation schemes, the points of each set are uniformly distributed. The resulting diagram, which corresponds to the entire block's modulation scheme, is similar to the distribution of the points, of a random modulation scheme (16QAM and 64QAM). This allows us to hide our modulation scheme $\mathcal{M}_i$ (where $\mathcal{M}_i$ is the modulation scheme for the i-th sub-carrier), into a higher order modulation, namely $\mathcal{M}$.

Algorithm 1: Heap's-like Algorithm - Index Mapping

Data:
idxVector: The final Index Sequence for the given Index Number.
idxNumber: The given Index Number.
n: The length of the sub-block.
k: In each $round$ we use the k last elements.
round: The current round.
Result: This method maps the first g1 bits of each sub-block into index sequences.

$idxVector = rowVector(1:n)$
$groupThreshold = factorial(n)$
for *round in rounds* **do**
  $groupThreshold = groupThreshold/k$
  $group = \lfloor idxNumber/groupThreshold \rfloor$
  $swap(idxVector[i], idxVector[i+group])$
  $idxNumber = idxNumber \mod groupThreshold$
end

A. Implementation

To take full advantage of IM, we must be able to use all $\log_2(n!)$ index bits, and the only way to do this is by generating all possible permutations of the available signal constellations, which leads to a factorial $(n!)$ number of combinations. If we want to implement this with an ordinary look-up table, the mapping procedure becomes impractical for a large permutation set, due to excessive storage demand. To avoid this, we propose the usage of an one-to-one mapping method, which is implemented by a Heap's-like Algorithm (Algorithms 1, 2) [11].

The Heap's-like Algorithm, uses dynamic programming, and has been designed in order to minimize the time and the storage demand. Let us assume that we have a sequence which consists of n elements. The algorithm is being executed into rounds. At each round, it generates a new permutation. In the k-th round, we deal with the $n-k+1$ last elements by interchanging a single pair of these elements. The other $k-1$ elements are not disturbed. The above process is repeated until k becomes equal to n. The final permutation gives us the desired sequence. In fact, in each round, we limit the search space by a factor of $n-k+1$.

IV. Receiver Architecture

At the receiver, after removing the CP and performing an $NFFT$-point FFT operation, an ML detector is used, in order to detect the data symbols, the mode sequence and the sub-sub-

Algorithm 2: Heap's-like Algorithm - Index Demapping

Data:
idxNumber: The number representing the desired combination.
n: The length of the sub-block.
groupThreshold: Partitioning of the combinations set, based on this threshold.
positions: A helper row-vector, to keep track of the elements.
round: The current round.
swapIndex: The index of the element that is gonna be swapped.
Result:
$idxNumber = 0$
$positions = rowVector(1:n)$
$groupThreshold = factorial(n)$
for *round in rounds[:-1]* **do**
  $groupThreshold = groupThreshold/(n-i+1)$;
  $swapIndex = positions.index(indexArray(i))$
  $idxNumber \mathrel{+}=$
  $(swapIndex - i) * groupThreshold$
  $positions(swapIndex) = positions(i)$
  $positions(i) = indexArray(i)$
end

block sequence. The set which includes all possible sub-block realizations for the i-th constellation set is defined as

$$\mathcal{S}^i = \{\mathbf{s}_1, ..., \mathbf{s}_{2^{(g2+g3)}}\} \tag{19}$$

Since the detection of each sub-sub-block is similar and independent, we can process the received signal in one sub-sub-block, in the manner of each sub-sub-block. For the received data of each constellation set we want to find the most likely mode sequence $\mathbf{I}^i$ defined as

$$\mathbf{I}^i = \begin{bmatrix} I^i_{1,1} & \dots & I^i_{1,v} \\ \vdots & \ddots & \\ I^i_{u,1} & \dots & I^i_{u,v} \end{bmatrix} \tag{20}$$

and the most likely data symbols $\mathbf{S}^i$ defined as

$$\mathbf{S}^i = \begin{bmatrix} S^i_{1,1} & \dots & S^i_{1,v} \\ \vdots & \ddots & \\ S^i_{u,1} & \dots & S^i_{u,v} \end{bmatrix}. \tag{21}$$

The (z,j)-th element of the matrices $\mathbf{I}^i_{z,j}$ and the $\mathbf{S}^i_{z,j}$ refers to the z-th sub-sub-block and the j-th sub-carrier of the most likely mode sequence and the most likely data symbol respectively. So, for the b-th sub-block and the i-th constellation set, the estimated index pattern, and the estimated data symbols, can be obtained by minimizing this metric:

$$(\mathbf{I}^i, \mathbf{S}^i) = \arg\min_{\mathbf{s}\in\mathcal{S}^i} \|\mathbf{y} - \mathbf{h}\ \mathrm{diag}\{\mathbf{s}\}\|^2 \tag{22}$$

Recall $i \in \{1, .., u\}$), that is it indexes all the sub-subblocks of a subblock.

So, based on (22), at this point, we have the most likely mode sequences $\mathbf{I}^i$, for the i-th constellation set and the most likely data symbols $\mathbf{S}^i$, for i-th constellation set for all sub-blocks in each group, and for all constellation sets ($i \in \{1, .., u\}$). AA: Ayto to komati ws edw einai shmantiko opote des to ligo kai grapsto pio prosektika.

Now we define the sub-block set

$$\mathcal{S} = \{\mathbf{s}_{i,k} := \mathrm{row}_k \mathbf{S}^i | \forall i, k \in \{1, .., u\}\} \tag{23}$$

and the combination range set

$$\mathcal{R} = \{\mathbf{r}_k := \mathrm{comb}(u, k) | \forall k \in \{1, .., u\}\} \tag{24}$$

Finally, in order to take the final estimation of the sub-sub-block pattern indicated by the vector $\mathbf{c}$

$$\mathbf{c} = [c_1, ..., c_u] \tag{25}$$

, the signal constellation pattern $\mathbf{I}$

$$\mathbf{I} = [I_1, ..., I_n] \tag{26}$$

, and the data symbols $\mathbf{S}$

$$\mathbf{S} = [S_1, ..., S_n] \tag{27}$$

, we have to minimize this metric:

$$(\mathbf{c}, \mathbf{I}, \mathbf{S}) = \arg\min_{\mathbf{r}\in\mathcal{R}, \mathbf{s}\in\mathcal{S}} \sum_{t=1}^{u} \|\mathbf{y} - \mathbf{s}_{r_t,t}\|^2 \tag{28}$$

We can see that (22) and the (28), have a computational complexity of order $\mathcal{O}(2^{g_2} \sqrt[u]{|\mathcal{M}|}^q + uq)$ (Table II). Hence, for a large number of q, g_2 and $|\mathcal{M}|$, this detector is impractical. In order to reduce the complexity, we have to reduce the search space, for all possible mode permutations. The method to achieve this is by using a Viterbi-like algorithm, which is based on this Viterbi-like idea [9], [12]. AA: exoume omos kati kainourgio kai endiaferon se exesh me aytous?

The operation of the Viterbi algorithm can be visualized by means of a trellis diagram (Fig. **??**). In a trellis graph, each node corresponds to a distinct state at a given time, and each arrow represents a transition to some new state at the next instant of time. We divide the process into stages. Each stage has a k-combination set of the index pattern which have a size of k and there are n stages in total. For example, for an index pattern with length 4, we have a trellis diagram with four stages (Fig. **??**).

After initialization, the algorithm will search for the shortest path from the initial to final state. With the help of the Viterbi algorithm, we compare the cumulative metrics of all paths merged on a node, and keep the minimum value in order to use it on the next stage. More specifically, searching for the optimal input sequence, is equivalent to finding the path in the lattice, whose final cumulative metric is minimal. The above process is repeated until the final state is reached, and the updated label of the final state provides the most likely index pattern. So, in the k-th stage we have $\binom{n}{k}$ states. In the last stage, we have the maximum number of incoming egdes. So

Table II
DECODER COMPUTATIONAL COST.

Detector	Model I	Model II
Optimal ML Detector	$\mathcal{O}(2^{g_1} * \lvert\mathcal{M}\rvert^n)$	$\mathcal{O}(2^{g_2} * \sqrt[u]{\lvert\mathcal{M}\rvert^q} + u*q)$
Viterbi-like Algorithm	$\mathcal{O}(n * 2^{(n-1)})$	$\mathcal{O}(u * 2^{(u-1)})$

we can consider n, as a safe limit of incoming edges for each state. As a result, the time complexity of this algorithm is:

$$n \times \sum_{k=1}^{n} \binom{n}{k} \tag{29}$$

There are several ways to calculate this. By using the Pascal's triangle we have:

$$n \times \sum_{k=1}^{n} \binom{n}{k} = n \times 2^{(n-1)} \tag{30}$$

So the computational complexity of the Viterbi-like Algorithm is of order $\mathcal{O}(n \times 2^{(n-1)})$ (Table II).

By analyzing (22), we see that we have to perform a Viterbi algorithm for each constellation set. So, for the i-th constellation set, we have a $v \times v$ matrix $\mathbf{T}$, whose $((z, j)$-th entry refers to the most likely symbol when the z-th sub-carrier employs $S^i_{j,z})$:

$$\mathbf{T}_{z,j} = \underset{\mathbf{s} \in \mathcal{S}^i}{\arg\min} \left\| \mathbf{y_z} - \mathbf{h_z}\ \mathbf{s}_z \right\|^2 \tag{31}$$

The process above, gives us the most likely mode sequences $\mathbf{I}^{i,b}$ (20), and the most likely data symbols $\mathbf{S}^{i,b}$ (21). Let us consider a $u \times u$ matrix $\mathbf{G}$, whose $((z, j)$-th entry refers to the most likely mode pattern when the z-th sub-sub-block employs $S_j)$, y^z refers to the received data y, which correspond to the z-th sub-sub-block and the h^z refers to the estimated channel coefficients h, which correspond to the z-th sub-sub-block:

$$\mathbf{G}_{z,j} = \underset{\mathbf{s} \in \mathcal{S}}{\arg\min} \left\| \mathbf{y^z} - \mathbf{h^z}\ \text{diag}\{\mathbf{s_{j,z}}\} \right\|^2 \tag{32}$$

Finally, we get the final estimation for the sub-block pattern $\mathbf{c}$, the signal constellation pattern $\mathbf{I}^b$, and the data symbols $\mathbf{S}^b$. The Viterbi-like algorithm has a computational complexity of order $\mathcal{O}(u \times 2^{(u-1)})$ (Table II).

V. PHYSICAL LAYER ENCRYPTION

Modulation obfuscation, discussed in the previous section, has acted, to make our transmission more secure, but it still has some limitations. It may inadvertently disclose the constellation design being used, which enables the eavesdropper to perform synchronization and channel estimation like a legitimate user, and extract the unencrypted fields in the physical layer.

In order to enhance our security and avoid this issue, we propose a physical layer stream encryption, which is based on the Caesar cipher algorithm [13], [14]. The main idea of this encryption method is to use the index bits, as the key for the encryption function. This fact, gives us the ability to further enhance the security of our system, due to the fact that the index bits are not necessarily the same for each sub-sub-block, and more specifically, they randomly change.

The proposed encryption process is performed after the bits separation of g in g_1 (3), g_2 (4) and g_3 (5) and before the MSG (Fig. 3). Our encryption function takes as an input, a number which falls within the range $\{1..|\mathcal{M}_i|\}$, and at the output gives a number which falls within the range $\{1..|\mathcal{M}_i|\}$. As a result, adding this level, does not affect the other levels in any way. As we said before, since each OFDM sub-block undergoes the same processing procedure, we focus our analysis on a single sub-sub-block. Let V_i^b, e^b, t^b and $V_i^{b'}$ be the decimal values of the unencrypted data belonging to the i-th group of to the b-th sub-block, the decimal value of the sub-block index bits which corresponds to the b-th sub-sub-block, the decimal value of the mode index bits which corresponds to the b-th sub-sub-block, and the decimal value of the encrypted data, belonging to the i-th group of the b-th sub-sub-block. So the value of the encrypted data, is given by:

$$V_i^{b'} = (V_i^b + e^b + t^b) \mod |\mathcal{M}_i| \tag{33}$$

In order for the receiver to be able to decrypt the data, he must use the same encryption key as the transmitter does. The decryption process, takes place, immediately, after the demodulation of the encrypted data. Respectively for the receiver we will consider that the A_i^b, e^b, t^b and $A_i^{b'}$ be the decimal value of the unencrypted data, belonging to the i-th group of to the b-th sub-sub-block, the decimal value of the sub-block index bits which corresponds to the b-th sub-sub-block, the decimal value of the mode index bits which corresponds to the b-th sub-sub-block, and the decimal value of the encrypted data, belonging to the i-th group of the b-th sub-sub-block. So the unencrypted data for the transmitted signal can be obtained from:

$$A_i^b = (A_i^{b'} - e^b - t^b) \mod |\mathcal{M}_i| \tag{34}$$

Remark. *The robustness of our encryption system depends on the randomness and the length of our encryption keys. As we discussed earlier, the nature of the index bits ensures the randomness of our encryption key. So we have to choose the parameters of our system in such a way as to get the maximum possible value of the index bits.*

VI. SIMULATION RESULTS

A. BER Perfromance

In this section we analyze and compare the uncoded BER performance of the proposed schemes, MM-OFDM-IM and SI-MM-OFDM-IM, with that of OFDM-IM and OFDM, assuming Rician fading channel and perfect channel estimation. The number of subcarriers is set to $N = 64$ and the length of the CP in no smaller than the number of channel taps. For brevity, we will refer to the OFDM-IM scheme with k out of n sub-carriers are active and transmitting $\mathcal{M}$-ary QAM symbols as OFDM-IM $(k, n, |\mathcal{M}|)$, MM-OFDM-IM $(n, |\mathcal{M}_i|)$ as the MM-OFDM-IM scheme with n subcarriers

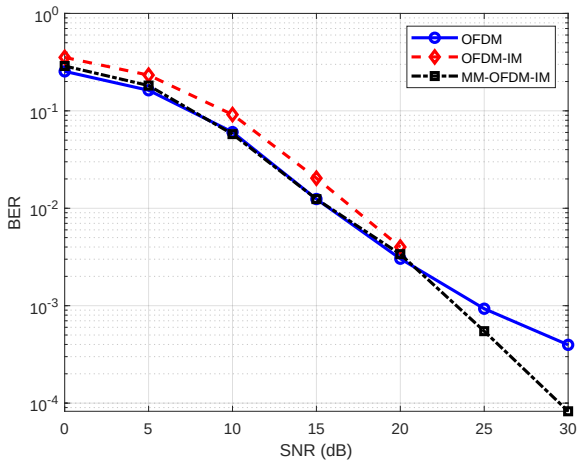

Figure 5. BER performance comparison between OFDM (4), OFDM-IM (4, 6, 16) and MM-OFDM-IM (4, 4).

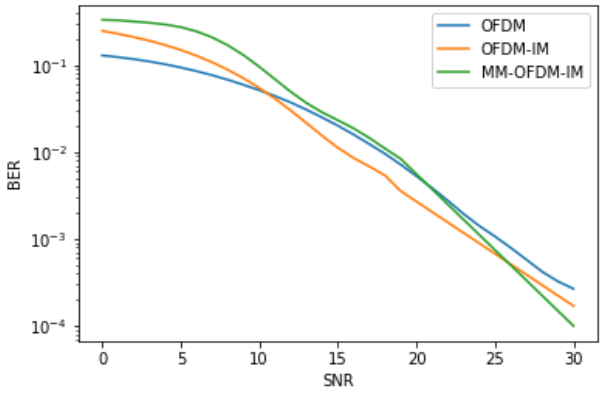

Figure 6. BER performance comparison between OFDM (16), OFDM-IM (4, 6, 64) and MM-OFDM-IM (16, 4)

employing n different $\mathcal{M}_i$-ary QAM symbols, and SI-MM-OFDM-IM $(n, |\mathcal{M}_i|, u)$ as the SI-MM-OFDM-IM scheme with n subcarriers employing n different $\mathcal{M}_i$-ary QAM symbols with u different constellation sets. For our simulations, we consider two cases. In the first case we use a 16-QAM scheme ($|\mathcal{M}| = 16$) and in the second one, a 64-QAM scheme ($|\mathcal{M}| = 64$).

For our first simulation the constellation diagram is depicted in Fig. 1 whereby the i-th sub-carrier is modulated by the i-th mode. In Fig. 5, we compare the BER performance of the proposed scheme MM-OFDM-IM (4, 4), with OFDM (4), and OFDM-IM (4, 6, 16), with SE being 3 bps/Hz, 2 bps/Hz and 3.17 bps/Hz respectively (Table III). As shown in Fig. 5, the proposed MM-OFDM-IM can achieve an SNR gain of 5 db when compared to OFDM-IM, and an SNR gain of 8 db over OFDM. MM-OFDM-IM and OFDM outperform the OFDM-IM in low SNR region, due to, the modulation order employed by each sub-carrier in MM-OFDM-IM and OFDM, is lower than that in OFDM-IM. MM-OFDM-IM and OFDM-IM outperform the OFDM in high SNR region, because the IM bits, have a stronger protection, than the ordinary modulation bits in the high SNR region, so that the IM bits are more likely to undergo error-free transmission at high SNR. MM-OFDM-IM performs the best among all schemes in the whole region owing to the larger proportion of the index bits, which alleviates the impact of the ordinary modulation bits on the BER more, verifying the advantages of using multiple signal constellations for IM.

Table III
SPECTRAL EFFICIENCY COMPARISON FOR THE FIRST SIMULATION

Scheme	SE
OFDM (4)	3.17 bps/Hz
OFDM-IM (4, 6, 16)	2 bps/Hz
MM-OFDM-IM (4, 4)	3 bps/Hz

For our second set of simulations the constellation diagram is depicted in Fig. 2 whereby the i-th sub-carrier is modulated by the i-th mode. In Fig. 6, we compare the BER performance of the proposed scheme MM-OFDM-IM (16, 4) with OFDM (16), OFDM-IM (4, 6, 64), with SE being 4.75 bps/Hz, 4 bps/Hz and 4.5 bps/Hz respectively (Table IV). As shown in Fig. 6, the proposed MM-OFDM-IM can achieve 2.5 db SNR gain on OFDM-IM and 5 db on OFDM. MM-OFDM-IM and OFDM-IM perform worse than OFDM at low SNR, due to the high errors probability of detecting mode permutations (index bits). As before, MM-OFDM-IM and OFDM-IM outperform OFDM for a sufficent SNR range owing to the two diversity order protection index bits. MM-OFDM-IM outperforms the OFDM and OFDM-IM in high SNR region because the modulation order employed by each sub-carrier in MM-OFDM-IM is lower than that in OFDM-IM and MM-OFDM-IM has a larger proportion of the two diversity protection index bits.

Table IV
SPECTRAL EFFICIENCY COMPARISON FOR THE SECOND SIMULATION

Scheme	SE
OFDM (16)	4 bps/Hz
OFDM-IM (4, 6, 64)	4.5 bps/Hz
MM-OFDM-IM (16, 4)	4.75 bps/Hz

Fig. 7, illustrates the comparison of the BER performance, between the proposed schemes, MM-OFDM-IM (4, 4) and MM-OFDM-IM (16, 4), with SE being 3 bps/Hz and 4.75 bps/Hz respectively. As we saw in Fig. 7, the MM-OFDM-IM (4, 4) has similar behavior in performance of BER, with a 2 db SNR gain on MM-OFDM-IM (16, 4) in the medium-to-high SNR region. This is because, the MM-OFDM-IM (16,4) has larger proportion of the index bits, which have a higher error probability of detecting the mode permutations (index bits) in the low-to-medium SNR region, and the MIRDs, of these two shemes are equal. On the other hand the MIAD of the MM-OFDM-IM(16, 4) is bigger that the MIAD of the MM-OFDM-IM(4, 4), which we expect to gives us a better performance at higher SNR values.

In this simulation, we will analyze and compare the BER performance of the enhanced diversity order schemes,

Table V
MIAD AND MIRD FOR THE THIRD SIMULATION

Scheme	MIAD	MIRD	SE
MM-OFDM-IM (4, 4)	4	2	3 bps/Hz
MM-OFDM-IM (16, 4)	8	2	4.75 bps/Hz

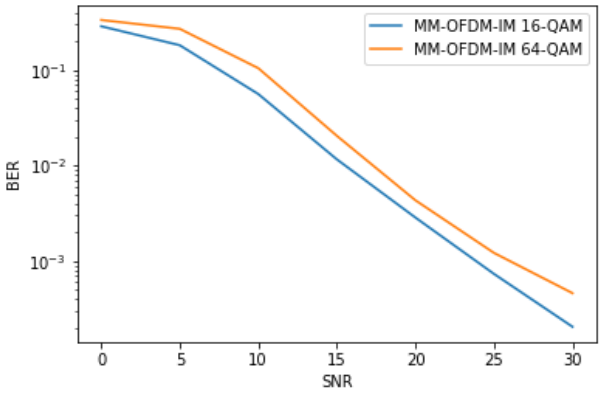

Figure 7. BER performance comparison between the MM-OFDM-IM (4, 4) and the MM-OFDM-IM (16, 4).

SI-MM-OFDM-IM $(2, 4, 2)$, SI-MM-OFDM-IM $(8, 4, 2)$, SI-MM-OFDM-IM $(4, 4, 4)$ and SI-MM-OFDM-IM $(2, 4, 8)$ with the BER performance of the MM-OFDM-IM $(4, 4)$ and MM-OFDM-IM $(16, 4)$, with SE being 3.69 bps/Hz, 3.94 bps/Hz, 3.25 bps/Hz, 3.44 bps/Hz, 3 bps/Hz and 4.75 bps/Hz respectively (Table VI). As we see in Fig. 8, the SI-MM-OFDM-IM has the same BER performance with the MM-OFDM-IM in low SNR region. SI-MM-OFDM-IM outperforms the MM-OFDM-IM, with a significant SNR gain, due to the four diversity order protection sub-block index bits in the high SNR region, so that the IM bits are more likely to undergo error-free transmission at high SNR region. With the above analysis we verify the advantages of using the SI-MM-OFDM-IM.

Finally, Fig 9 presents the comparison between the the SI-MM-OFDM-IM (8, 4, 2), the SI-MM-OFDM-IM (4, 4, 4) and the SI-MM-OFDM-IM (2, 4, 8). By analyzing this figure, we can see that the increase of u, can increase the BER performance of our system, owing to the the stronger protection of the sub-block index bits.

Table VI
SPECTRAL EFFICIENCY COMPARISON FOR THE SECOND MODEL

Scheme	SE
SI-MM-OFDM-IM (2, 4, 2)	3.69 bps/Hz
SI-MM-OFDM-IM (8, 4, 2)	3.94 bps/Hz
SI-MM-OFDM-IM (4, 4, 4)	3.25 bps/Hz
SI-MM-OFDM-IM (2, 4, 8)	3.44 bps/Hz
MM-OFDM-IM (4, 4)	3 bps/Hz
MM-OFDM-IM (16, 4)	4.75 bps/Hz

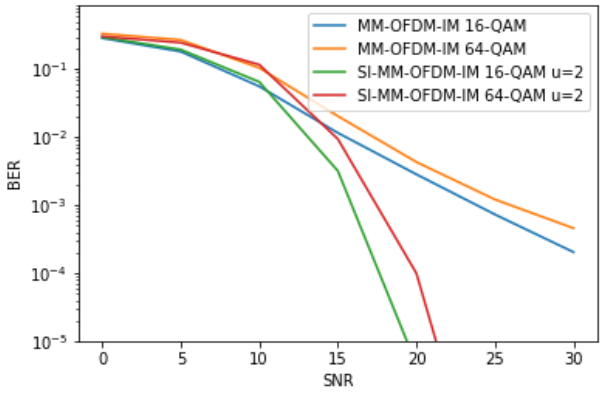

Figure 8. BER performance comparison between the SI-MM-OFDM-IM (2, 4, 2) and the SI-MM-OFDM-IM (8, 4, 2) with the MM-OFDM-IM (4, 4) and the MM-OFDM-IM (16, 4).

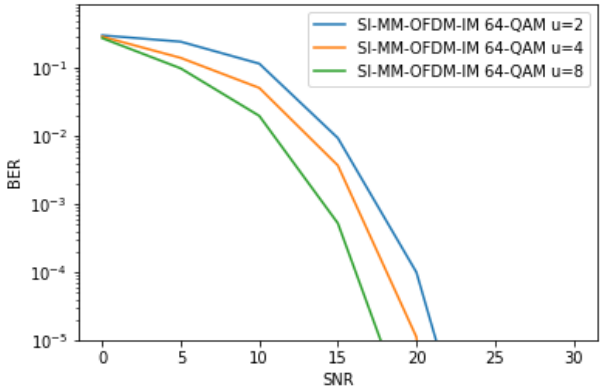

Figure 9. BER performance comparison between the SI-MM-OFDM-IM (8, 4, 2), the SI-MM-OFDM-IM (4, 4, 4) and the SI-MM-OFDM-IM (2, 4, 8).

B. Modulation Classification

We test the robustness of the proposed modulation obfuscation method, against of one of the aforementioned attacks, by using a deep learning technique, designed for noise channels, based on CNN [15]. Since both models use the same constellation design, we can use in our experiment only the one of these two models, the MM-OFDM-IM.

The modulation recognition can modeled as an N-class decision problem, where the input is a sampled signal and the output is a binary vector with size N, that determines the chosen modulation scheme.

We evaluate the system performance by using Python and tensorflow framework. We generate a dataset, that consists of three different modulations, 4-QAM, 16-QAM and 64-QAM $(N = 3)$. So the points of our sample are evenly distributed among all modulations and in the SNR range, from -5 db to 10 db. We will have a CNN for each value of SNR. We assume that the training SNR and the testing SNR have similar values.

Our dataset consists of three million (3000000) samples.

The training set is composed of 70% of entire dataset selected at random. We use the rest of our dataset for validation purposes.

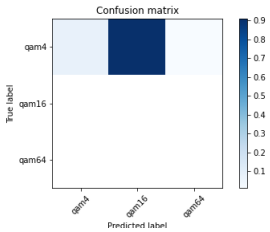

Figure 10. Confusion Matrix for the 16-QAM modulation scheme (M=16). This figure depicts the average values of the accuracy for our model over the entire SNR range.

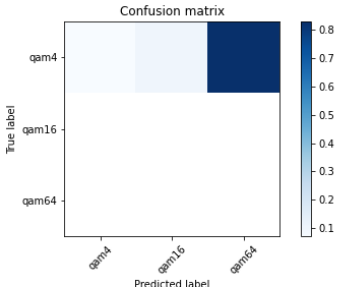

Figure 11. Confusion Matrix for the 64-QAM modulation scheme (M=64). This figure depicts the average values of the accuracy for our model over the entire SNR range.

Our CNN [16] consists of nine (9) layers (Fig. **??**, **??**), two 2D Convolutions, one Batch Normalization, one 2D Max Pooling, one Dropout, one Flatten and two Dense Layers. By using the Batch Optimizer, we make our CNN model faster and more stable. Also, by using a Dropout layer, our model preserved to be over-fitted. Our CNN uses two different Dense Layers. The first Dense Layer is formed by a ReLU activation function. The second one, uses a softmax activation function. In this CNN the number of filters from one stage to another are being reduced. Our experience with many different configurations indicated that the architectures that get narrower in each following Convolutional Layer perform better in terms of classification and reduce training time.

Since we use the same constellation design in both models, we can it's robustness by using only one of these two models. Therefore, for this simulation, we will use the MM-OFDM-IM.

As we see from Fig. **??**, our model does not over-fit due to the convergence of training loss to validation loss.

As can be seen from the confusion matrices (Fig. 10, 11), Eavesdropper cannot retrieve the modulation scheme, $\mathcal{M}_i$ (4-QAM), used for each mode. Our CNN predicts that the probability of the transmitter using a 4-QAM modulation scheme is much smaller than the other two schemes, with the most likely being the 16-QAM and the 64-QAM respectively. Due to the fact that, the points of each mode are uniformly distributed and each sub-block uses all available modes, the resulting constellation diagram for each OFDM block is similar to the

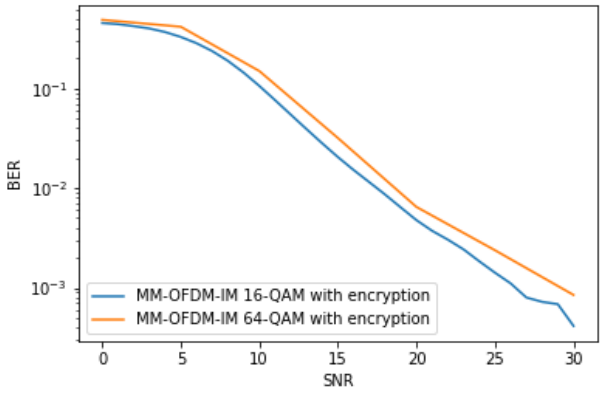

Figure 12. Bit Error Rate performance comparison between MM-OFDM-IM (4, 4) and MM-OFDM-IM (16, 4) including physical layer encryption in both.

distribution of the points of an $\mathcal{M}$-ary (16-QAM, 64-QAM) modulation scheme. This results in a succesful modulation obfuscation for our model.

C. PHY Layer Encryption - BER Performance

In the final simulation, we will test the BER performance of the MM-OFDM-IM and the SI-MM-OFDM-IM models, including encryption.

Figure 12 depicts the comparison of the MM-OFDM-IM (4,4) and the MM-OFDM-IM (16,4) including encryption in both. As shown in Fig. 12, the MM-OFDM-IM (4,4) has narrowly better performance than the MM-OFDM-IM (16,4) due to the fact that, the MM-OFDM-IM (16,4) has larger proportion of the index bits, which have a higher error probability of detecting the mode permutations (index bits) in the low-to-medium SNR region. Also, as we saw in Fig. 7, these two schemes have a similar behavior in performance.

Fig. 13 and Fig. 14, present the comparison of the MM-OFDM-IM (4,4) and the MM-OFDM-IM (16,4) with and without encryption. We see that the MM-OFDM-IM with encryption performs worse than the one without the encryption. This slight difference comes from the fact that, the decryption function uses the index bits as the encryption key. As mentioned in Section III, in order for us to have an erroneous index detection, in the best case scenario, we have to detect the permutation of any two signal constellations incorrectly, which means that the other constellation symbols are correct. After the decryption operation, using the wrong encryption key, the whole sub-block will be shifted in such a way as to increase the average BER and decrease the probability of a symbol being received correctly.

Fig. 15 depicts the comparison of the SI-MM-OFDM-IM (2, 4, 2) and the SI-MM-OFDM-IM (8, 4, 2) with and without encryption. As we can see the SI-MM-OFDM-IM (2, 4, 2) and the SI-MM-OFDM-IM (8, 4, 2) with the encryption perform worse than the one without the encryption. The reason is the same as in MM-OFDM-IM. The encryption key increase the

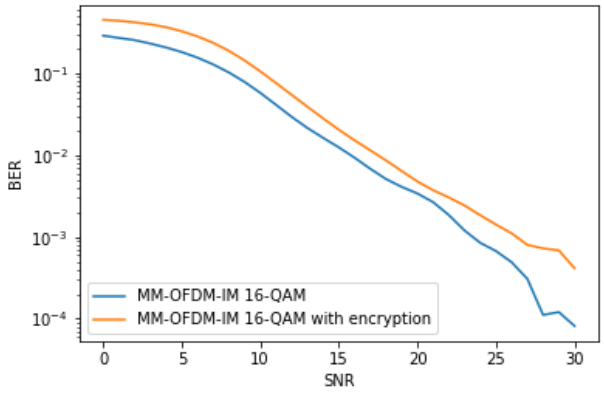

Figure 13. Bit Error Rate performance comparison between MM-OFDM-IM (4, 4) without physical layer encryption and MM-OFDM-IM (4, 4) with physical layer encryption.

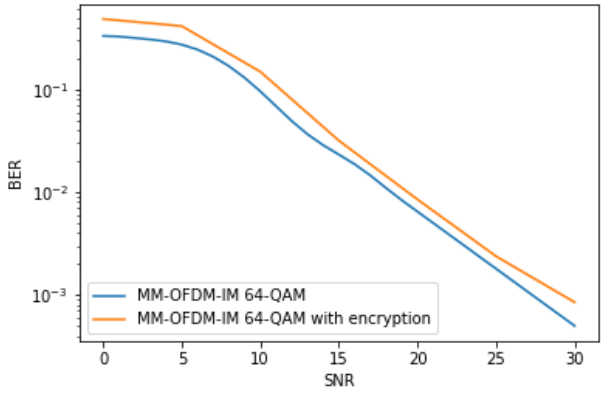

Figure 14. Bit Error Rate performance comparison between MM-OFDM-IM (16, 4) without physical layer encryption and MM-OFDM-IM (16, 4) with physical layer encryption.

average BER and decrease the probability of a symbol being received correctly.

VII. Conclusion

SCI leaked from encrypted wireless communications can be exploited to violate user privacy by using various traffic analysis techniques. Preventing the leakage of transmission attributes, such as, modulation scheme, is challenging. In this paper, a novel MM-OFDM-IM design has been proposed, which utilizes, all available sub-carriers to transmit data. Modulation obfuscation and encryption techniques are being used. Also, it has been shown that, the proposed scheme achieves a significantly better BER performance than the others OFDM-IM schemes and improves the spectral efficiency. This design should also be investigated in real world conditions, such as mobility.

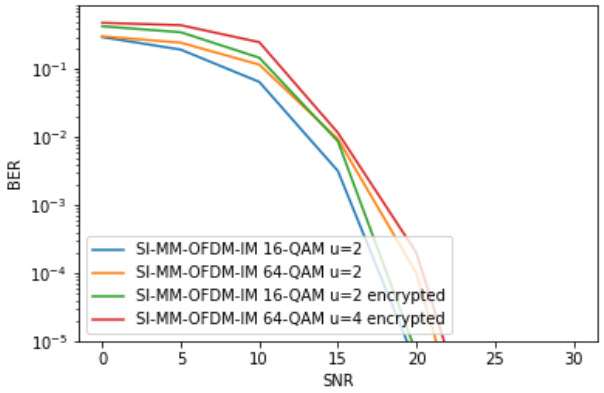

Figure 15. Bit Error Rate performance comparison of the SI-MM-OFDM-IM (2, 4, 2) and the SI-MM-OFDM-IM (8, 4, 2) without physical layer encryption with the SI-MM-OFDM-IM (2, 4, 2) and the SI-MM-OFDM-IM (8, 4, 2), including physical layer encryption.

References

[1] Melki, Reem and Noura, Hassan N. and Mansour, Mohammad M. and Chehab, Ali, "A survey on ofdm physical layer security," *Physical Communication*, vol. 32, p. 1–30, 2019.

[2] Shuo Chen, Rui Wang, XiaoFeng Wang, Kehuan Zhang, "Side-channel leaks in web applications: a reality today, a challenge tomorrow," *2010 IEEE Symposium on Security and Privacy*, may 2010.

[3] "Zhenzhen Gao, Shaozhuang Bai, Xuewen Liao, Meiqin Liu", "Anti-eavesdropping scheme based on random mapping for gsm-mbm systems," *IEEE Access*, vol. 8, pp. 48 416 – 48 427, mar 2020.

[4] Rahbari, Hanif and Krunz, Marwan, "Secrecy beyond encryption: obfuscating transmission signatures in wireless communications," *IEEE Communications Magazine*, vol. 53, no. 12, p. 54–60, 2015.

[5] Dyer, Kevin P. and Coull, Scott E. and Ristenpart, Thomas and Shrimpton, Thomas, "Peek-a-boo, i still see you: Why efficient traffic analysis countermeasures fail," *2012 IEEE Symposium on Security and Privacy*, 2012.

[6] Cheng, Xiang and Zhang, Meng and Wen, Miaowen and Yang, Liuqing, "Index modulation for 5g: Striving to do more with less," *IEEE Wireless Communications*, vol. 25, no. 2, p. 126–132, 2018.

[7] Tianqi Mao, Zhaocheng Wang, Qi Wang, Sheng Chen, and Lajos Hanzo, "Dual-mode index modulation aided ofdm," *IEEE*, 2017.

[8] E. P. Ertuğrul Başar, Ümit Aygölü, "A new technique for ofdm: Ofdm-index modulation," *IEEE*, apr 2013.

[9] Wen, Basar, Li, Zheng, Zhang, "Multiple-mode orthogonal frequency division multiplexing with index modulation," *IEEE Transactions on Communications*, pp. 3892–3906, 2017.

[10] Nicolay Kostov, "Mobile radio channels modeling in matlab," *Multimedia Communications*, p. 12–16, 2003.

[11] "Heap's algorithm," Mar 2020. [Online]. Available: https://en.wikipedia.org/wiki/Heap's_algorithm

[12] "Viterbi algorithm." [Online]. Available: https://en.wikipedia.org/wiki/Viterbi_algorithm

[13] H. Rahbari, M. Krunz, "Full frame encryption and modulation obfuscation using channel-independent preamble identifier." *IEEE Transactions on Information Forensics and Security.*, vol. 11, p. 2732–2747, 2006.

[14] "Caesar cipher." [Online]. Available: https://en.wikipedia.org/wiki/Caesar_cipher

[15] O'Shea, Timothy J. and Corgan, Johnathan and Clancy, T. Charles, "Convolutional radio modulation recognition networks," *Engineering Applications of Neural Networks Communications in Computer and Information Science*, p. 213–226, 2016.

[16] "Nitish Srivastava, G E Hinton, Alex Krizhevsky, Ilya Sutskever, Ruslan R Salakhutdinov", "Dropout: A simple way to prevent neural networks fromoverfitting," *The Journal of Machine Learning Research*, jan 2014.