IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 4, 2020, accepted November 26, 2020, date of publication December 7, 2020,
date of current version December 21, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3042969

Inter-Subset Hamming Distance Maximization for Enhancing the Physical Layer Security of Antenna Subset Modulation

OMAR ANSARI[1], MUHAMMAD AMIN[2], MOAZAM MAQSOOD[1], (Member, IEEE), ABDUL RAHMAN MUHAMMAD MAUD[1], (Member, IEEE), AND MUDDASSAR FAROOQ[3], (Member, IEEE)

[1]Electrical Engineering Department, Institute of Space Technology, Islamabad 44000, Pakistan
[2]Avionics Engineering Department, Institute of Space Technology, Islamabad 44000, Pakistan
[3]Faculty of Engineering, Air University Islamabad, Islamabad 44000, Pakistan

Corresponding author: Omar Ansari (omar.ansari93@yahoo.com)

ABSTRACT In this article, a novel antenna subset selection technique for enhancing the Physical Layer Randomness (PLR) of Antenna Subset Modulation (ASM) has been proposed. Hamming Distance Optimized Antenna Subset Selection (HD-OASS) minimizes the correlation between the antenna subsets at transmitter by maximizing the hamming distance between the successively used antenna subsets. Unlike previously proposed Randomized Antenna Subset Selection (RASS) and Side-Lobe Level Optimized Antenna Subset Selection (SLL-OASS), in which antenna subsets are randomly selected from the codebook, HD-OASS chooses the antenna subsets having optimally maximized hamming distance. It is shown that SLL-OASS has rather unfavorable effects on encryption strength due to considerable reduction of codebook size. Furthermore, HD-OASS has been shown to outperform RASS and SLL-OASS in terms of encryption strength in the unwanted directions of eavesdropper.

INDEX TERMS Antenna subset modulation, directional modulation techniques, eavesdropper, intended receiver, physical layer randomness, physical layer security.

I. INTRODUCTION

Over the past decade, Directional Modulation (DM) has emerged as strong candidate for providing Physical Layer Security (PLS) against eavesdropping. Several DM techniques which use single or multiple antenna elements include; switched phased-array [1], near-field direct antenna modulation [2], phased-array based DM [3]–[5], 4-D antenna array [6], dual-beam DM [7], [8], and frequency diverse array [9]–[12]. Unlike traditional cryptographic approach for data security [13] in which data is encrypted even for Intended Receiver (IR), all the DM techniques transmit non-encrypted data (plaintext) along the direction of IR and encrypted data (ciphertext) along the unwanted directions. Depending upon the design of transmitter architecture, DM techniques are broadly classified into two classes [14]; radiator-reconfigurable and excitation-reconfigurable techniques.

The associate editor coordinating the review of this manuscript and approving it for publication was Chow-Yen-Desmond Sim.

Antenna Subset Modulation (ASM) is one of the excitation-reconfigurable DM techniques that performs modulation at antenna level [15]. Instead of using the complete antenna array for data transmission, it uses randomly chosen subset of antenna array (through the process of array thinning) that is modulated at symbol rate. Previously, two antenna subset selection techniques have been proposed for ASM; Randomized Antenna Subset Selection (RASS) and Optimized Antenna Subset Selection (OASS). RASS exhibit high average Side-Lobe Level (SLL) due to random selection of antenna subsets. On the other hand, OASS reduces average SLL of antenna subsets using Simulated Annealing (SA) algorithm [16].

Low-Complexity Antenna Subset Modulation (LC-ASM) improves the transmitter architecture of ASM by performing modulation both at baseband and antenna level [17]. Unlike ASM, LC-ASM generates the desired phase and amplitude of digital symbol at baseband. It makes ASM compatible with amplitude modulation schemes like Quadrature Amplitude Modulation (QAM), along with phase modulation schemes

for which ASM was originally proposed. Interference mitigation techniques for multi-directional ASM are proposed in [18].

In the domain of PLS, Symbol Error Rate (SER) is very commonly used as a measure of wireless communication security. High and relatively stable value of SER in the unwanted directions is considered analogous to good randomization of data constellations and hence good PLS. Therefore, all the proposed techniques for ASM [15], [17]–[20] have focused on increasing SER in the unwanted directions. However, SER is not a direct measure of encryption strength. It is the probabilistic measure of erroneously received symbols. A comparatively recent paradigm in the PLS domain proposes to quantify the wireless communication security in terms of robust and well-adopted statistical randomness tests devised by National Institute of Standards and Technology (NIST) [21]. Physical Layer Randomness (PLR) [22] is one of such parameters which proposes a new model for analyzing the encryption strength of DM techniques in terms of randomness introduced along the undesired directions i.e. towards eavesdropper (Eve). It maps the concepts of PLS techniques to symmetric-key block encryption ciphers, like state-of-the-art Advanced Encryption Standard (AES) [23], to benchmark the encryption strength of DM techniques to strong block ciphers [24]. In this article, this recent paradigm has been adopted.

The contributions of our paper are summarized below:

1. The inter-subset Hamming Distance Optimized Antenna Subset Selection (HD-OASS) has been proposed as a novel antenna subset selection technique for enhancing PLR (encryption strength at physical layer) of ASM. Maximization of inter-subset hamming distance translates to minimum overlap of antenna positions among the successively used antenna subsets, which results in reduced correlation between successively transmitted symbols.
2. HD-OASS has been shown to perform better than RASS. Random selection of antenna subsets does not ensure that the correlation between the antenna positions of successively used antenna subsets is high.
3. It is shown that SLL optimization through simulated annealing degrades the performance of ASM in terms of randomness due to significant reduction of key space (usable combinations of antenna subsets). HD-OASS has been suggested as an alternate subset selection technique which should be maximized for enhancing PLR rather than SLL reduction.
4. HD-OASS has been shown to generate narrower PLR beamwidth along the direction of Bob compared to RASS and SLL-OASS.
5. The encryption strength of HD-OASS has been benchmarked against state-of-the-art symmetric key block cipher of AES. It is shown that in order to achieve PLR comparable to AES, hamming distance maximization of antenna subsets outperforms previously proposed optimization techniques.

Notations: In this article, $\mathbf{B}$ represents the codebook matrix containing all the $C_M^N = \frac{N!}{M!(N-M)!}$ possible combinations of antenna subsets. The superscript * is the notation for complex conjugate. $\mathbf{b_i}$ denotes the i^{th} row vector (or i^{th} antenna subset) from the codebook matrix $\mathbf{B}$. mod_2 is base 2 modulo operation. $\mathbf{x} \odot \mathbf{y}$ represents Hadamard or element-wise product of two vectors $\mathbf{x}$ and $\mathbf{y}$. $\sum_r$ indicates row wise summation of elements of a vector. The normalized inter-subset hamming distance between two vectors $\mathbf{b_i}$ and $\mathbf{b_j}$ is represented as d_{ij}.

II. ANTENNA SUBSET MODULATION

In this section, the system model for analyzing ASM is presented. There are two fundamental distinctions between the transmitter architecture of ASM compared to Conventional Phased Array (CPA), as shown in Fig. 1:

1. ASM synthesizes the desired phase of symbol at antenna level using phase shifters, unlike baseband symbol constellation synthesis in CPA.
2. Instead of using the complete antenna array for signal transmission in a pre-specified direction as in CPA, ASM selects a subset of array. This subset is randomly selected and modulated (changed) for every symbol duration.

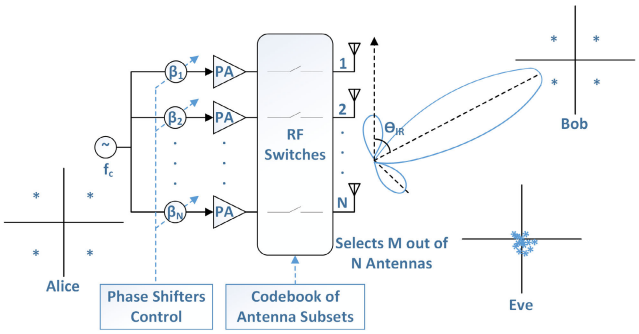

FIGURE 1. Transmitter architecture for antenna subset modulation.

A. SYSTEM MODEL

Suppose that Alice is equipped with a uniform linear ASM-enabled array comprising of N isotropically radiating antenna elements seperated by d inter-element distance, as shown in Fig. 1. Intended Receiver (IR) i.e. Bob is located along a pre-specified direction (θ_T) known to Alice. At any discrete time k, the signal transmitted by the complete array is represented as a vector $\mathbf{x}(k)$. The modulation scheme being used is Phase Shift Keying (PSK) and $\phi(k)$ is the phase of encoded symbols. The array is phase compensated using phase-shifters to direct the main lobe in the direction of Bob. After phase compensation, the signal is amplified using Power Amplifier (PA) at each RF chain. Following it, high speed RF switches are capable of randomly selecting M ($M < N$) antenna elements depending upon the antenna subset (code) from the codebook. Eavesdropper (Eve) is situated outside the main lobe of array the direction of which is

unknown to Alice. The signal received along any direction θ at time k can be written as:

$$y(k,\theta) = \mathbf{h}^{*}(\theta)\,\mathbf{x}(k) \tag{1}$$

where $\mathbf{x}(k)$ is the transmitted signal vector and $\mathbf{h}(\theta)$ is the $N \times 1$ channel vector which can be written as:

$$\mathbf{h}(\theta) = \Big[e^{-j(\frac{N-1}{2})\frac{2\pi d}{\lambda}\cos\theta}, e^{-j(\frac{N-1}{2}-1)\frac{2\pi d}{\lambda}\cos\theta}, \ldots, e^{0}, \ldots, e^{j(\frac{N-1}{2})\frac{2\pi d}{\lambda}\cos\theta}\Big] \tag{2}$$

where λ is the wavelength of the carrier. Equation 1 is the generalized representation of transmitted signal $y(k,\theta)$. In ASM architecture, subsets of antenna array are randomly selected through high-speed RF switches for every PSK symbol transmission. The cumulative effect of switching in ASM is incorporated in the system model by Hadamard product of binary antenna subset vector $\mathbf{b}(k)$ with channel phase compensation vector $\mathbf{h}(\theta_T)$, where θ_T is the direction of intended receiver. The randomly selected code/antenna subset i.e. $\mathbf{b}(k)$ encodes the indices of M transmit antennas that are selected for k^{th} discrete symbol duration. Normalized to M active antenna elements, the resulting input vector $\mathbf{x}(k)$ can be written as:

$$\mathbf{x}(k) = \frac{\sqrt{E_s}}{M}\left[\mathbf{b}(k) \odot \mathbf{h}(\theta_T)\right] e^{j\phi(k)} \tag{3}$$

where $\sqrt{E_s}$ is the symbol energy and $e^{j\phi(k)}$ is the phase of PSK modulated symbols. Incorporating the effect of phase compensation and subset switching in ASM, the system model given by equation 1 becomes:

$$\begin{aligned} y(k,\theta) &= \mathbf{h}^{*}(\theta)\mathbf{x}(\mathbf{k}) \\ &= \frac{\sqrt{E_s}e^{j\phi(k)}}{M}\mathbf{h}^{*}(\theta)[\mathbf{b}(k) \odot \mathbf{h}(\theta_T)] \\ &= \frac{\sqrt{E_s}e^{j\phi(k)}}{M}\sum_{n=0}^{N-1}\mathbf{b_n}(k)e^{j\left(n-\frac{N-1}{2}\right)\frac{2\pi d}{\lambda}(\cos\theta-\cos\theta_T)}. \end{aligned} \tag{4}$$

Equation 4 can further be represented as:

$$y(k,\theta) = \frac{\sqrt{E_s}}{M}\sum_{n=0}^{N-1}\mathbf{b_n}(k)e^{j\beta_n(k)}e^{j\left(n-\frac{N-1}{2}\right)\frac{2\pi d}{\lambda}\cos\theta} \tag{5}$$

where,

$$\beta_n(k) = \underbrace{\phi(k)}_{\text{modulation component}} \underbrace{-\left(n-\frac{N-1}{2}\right)\frac{2\pi d}{\lambda}\cos\theta_T}_{\text{beam-steering component}}. \tag{6}$$

In equation 5, β_n is the progressive inter-element phase difference which is applied by adjusting the phase-shifters of each RF chain shown in Fig. 1. It consists of modulation component and beamsteering component. From equation 6, it is evident that modulation and beamsteering are jointly performed in ASM at antenna level.

Effect of ASM along Bob:

Consider that Bob is spatially situated along θ_T direction with respect to Bob and the direction of Bob is known to Alice. The main beam is pointed in the direction of Bob by array phase compensation i.e. $\theta = \theta_T$. Therefore, in the direction of Bob, Equation 4 simplifies as:

$$\begin{aligned} y(k,\theta_T) &= \frac{\sqrt{E_s}e^{j\phi(k)}}{M}\sum_{n=0}^{N-1}\mathbf{b_n}(k)e^{j\left(n-\frac{N-1}{2}\right)\frac{2\pi d}{\lambda}(\cos\theta_T-\cos\theta_T)} \\ &= \frac{\sqrt{E_s}e^{j\phi(k)}}{M}\sum_{n=0}^{N-1}\mathbf{b_n}(k)e^{j\left(n-\frac{N-1}{2}\right)\frac{2\pi d}{\lambda}(0)} \\ &= \frac{\sqrt{E_s}e^{j\phi(k)}}{M}\sum_{n=0}^{N-1}\mathbf{b_n}(k) \\ &= \frac{\sqrt{E_s}e^{j\phi(k)}}{M}(M) \\ y(k,\theta_T) &= \sqrt{E_s}e^{j\phi(k)}. \end{aligned} \tag{7}$$

From equation 7, it is clear that Bob receives the original non-distorted phase of symbol i.e. $\phi(k)$. This is because Alice has phase-compensated the array only in the direction of Bob. Hence, Bob receives non-encrypted data (plaintext) at physical layer in ASM.

Effect of ASM along Eve:

Consider that Eve is located along $\theta \neq \theta_T$ and its direction is unknown to Alice. For any θ, the system model of ASM is given by equation 5 as:

$$\begin{aligned} y(k,\theta) &= \frac{\sqrt{E_s}e^{j\phi(k)}}{M}\sum_{n=0}^{N-1}\mathbf{b_n}(k)e^{j\left(n-\frac{N-1}{2}\right)\frac{2\pi d}{\lambda}(\cos\theta-\cos\theta_T)} \\ &= \frac{\sqrt{E_s}}{M}\sum_{n=0}^{N-1}\mathbf{b_n}(k)e^{j\beta_n(k)}e^{j\left(n-\frac{N-1}{2}\right)\frac{2\pi d}{\lambda}\cos\theta}. \end{aligned} \tag{8}$$

Equation 8 would result in a complex value which would depend on the value of θ as well as $\mathbf{b}(k)$. The direction of Bob i.e. θ_T is also unknown to Eve. Furthermore, the antenna indices are being randomly modulated after every symbol transmission. For Eve to de-modulate the phase of original transmitted symbol, it would require the exact estimate of not only the direction of Bob but also the information of antenna subsets which are changing for every symbol. Therefore, in the direction of Eve scrambled and encrypted constellation of data (ciphertext) is transmitted.

III. INTER-SUBSET HAMMING DISTANCE MAXIMIZATION

In this section, the algorithm of HD-OASS is discussed. Suppose that a_{in} represent n^{th} antenna position of i^{th} antenna subset. Then, any antenna subset $\mathbf{b_i}$ can be written as:

$$\mathbf{b_i} = [a_{i1} \quad a_{i2} \quad a_{i3} \quad \ldots \quad a_{iN}]. \tag{9}$$

Similarly, the antenna subset for the j^{th} symbol duration would be:

$$\mathbf{b_j} = [a_{j1} \quad a_{j2} \quad a_{j3} \quad \ldots \quad a_{jN}]. \tag{10}$$

For any two binary vectors $\mathbf{b_i}$ and $\mathbf{b_j}$, the normalized inter-subset hamming distance is be defined as:

$$d_{ij} = \frac{1}{N} \sum_r mod_2(\mathbf{b_i} + \mathbf{b_j}) \tag{11}$$

where $\sum_r$ denotes row wise summation of elements of a vector and mod_2 is base 2 modulo operation. The equation can further be modified as:

$$d_{ij} = \frac{1}{N} \sum_r mod_2([a_{i1} \quad a_{i2} \quad a_{i3} \quad \dots \quad a_{iN}] + [a_{j1} \quad a_{j2} \quad a_{j3} \quad \dots \quad a_{jN}]) \tag{12}$$

$$d_{ij} = \frac{1}{N} \sum_r mod_2 \left[a_{i1} + a_{j1} \quad a_{i2} + a_{j2} \quad \dots \quad a_{iN} + a_{jN}\right] \tag{13}$$

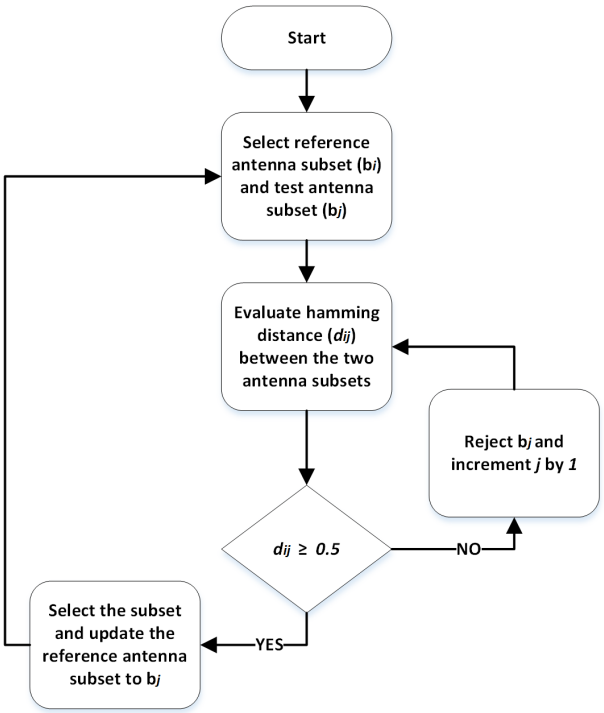

FIGURE 2. Block Diagram of HD Optimization.

A. COST FUNCTION

The cost function for inter-subset hamming distance optimization algorithm can be represented as:

$$\begin{aligned} f &= max[d_{ij}] \\ &= max\left[\frac{1}{N} \sum_r mod_2(\mathbf{b_i} + \mathbf{b_j})\right] \\ &= max\left[\frac{1}{N} \sum_r mod_2\left[a_{i1} + a_{j1} \quad \dots \quad a_{iN} + a_{jN}\right]\right] \end{aligned} \tag{14}$$

under the constraint:

$$d_{ij} \geq 0.5. \tag{15}$$

Algorithm 1 Hamming Distance Maximization

```
procedure Antenna_Subset_Selection (N,M)
    Initialize (b_i, b_j)
    for c = 1 to iter_count do
        for i = 1 to codebook_size do
            if d_ij = (1/N) Σ_r mod_2(b_i + b_j) ≥ 0.5
                b_{i+1} = b_j
            else
                b_{i+1} = φ
            end if
            j = j + 1
        end for
    end for
end procedure
```

The normalized hamming distance constraint value of greater than or equal to 0.5 means that for any successive symbol transmissions, the antenna positions remain uncorrelated by atleast 50%. Antenna subsets having low inter-subset hamming distance are discarded by the algorithm.

B. OPTIMIZATION ALGORITHM

The algorithm for antenna subset selection using inter-subset hamming distance maximization is as following:

1: For an array of N antenna elements in which $M (M < N)$ are randomly turned on, there are C_M^N possible combinations of antenna subsets. All the C_M^N combinations of antenna subsets of ASM are stored in a cookbook.
2: A reference antenna subset $\mathbf{b_i}$ and a test antenna subset $\mathbf{b_j}$ are randomly selected from the codebook.
3: Run the optimization equal to the number of pre-specified *iter_count* starting from $c = 1$. Each round of optimization iteratively discards antenna subsets which have $d_{ij} \leqslant 0.5$.
4: For every iteration, the inter-subset hamming distance of complete codebook is calculated with respect to reference antenna subset.
5: Calculate the hamming distance between $\mathbf{b_i}$ and $\mathbf{b_j}$. For binary codebook (as for ASM), the normalized inter-subset hamming distance is calculated by $d_{ij} = \frac{1}{N} \sum_r mod_2(\mathbf{k_i}, \mathbf{k_j})$. After calculation, the condition is checked whether the hamming distance between the two codes is greater than or equal to *0.5*. The value of $d_{ij} \geq 0.5$ means that we are discarding all the antenna subsets which have hamming distance less than *0.5*.
6: If $d_{ij} \geq 0.5$, then the test antenna subset $\mathbf{b_j}$ is selected as the next antenna subset i.e. $\mathbf{b_{i+1}} = \mathbf{b_j}$ after $\mathbf{b_i}$. Furthermore, the subset $\mathbf{b_j}$ is updated as the reference subset for next calculation.
8: If $d_{ij} \ngeq 0.5$, then the algorithm rejects the antenna subset $\mathbf{b_j}$.
10: The test antenna subset is incremented by one in the codebook.

Antenna Subsets \ Antenna no.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	Hamming Distance (Normalized)
1	■	■	■	■		■	■		■		■	■	■	■			■			■	■	■		■	---
2		■			■	■	■	■	■	■	■	■	■	■	■	■		■	■				■		0.67
3	■	■	■	■			■				■	■	■	■	■	■				■		■	■	■	0.5
4	■		■	■	■	■	■		■	■	■				■		■	■			■	■	■	■	0.5
5	■	■	■	■	■			■	■			■	■			■	■	■	■	■	■	■			0.583

FIGURE 3. Hamming Distance for HD OASS.

Antenna Subsets \ Antenna no.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	Hamming Distance (Normalized)
1	■	■		■	■	■			■	■		■	■	■		■		■	■		■	■		■	---
2	■				■		■		■	■			■	■	■		■	■	■	■	■	■	■	■	0.417
3	■			■	■		■	■			■	■	■		■	■	■	■		■		■	■	■	0.417
4	■	■	■	■		■		■		■	■		■		■	■	■	■			■	■		■	0.417
5		■	■	■	■	■		■		■	■	■	■			■	■	■				■	■	■	0.25

FIGURE 4. Hamming Distance for RASS.

Antenna Subsets \ Antenna no.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	Hamming Distance (Normalized)
1	■		■	■	■		■	■	■	■	■	■	■	■	■	■			■				■		---
2			■		■		■	■	■		■	■	■	■	■	■	■	■	■		■		■		0.25
3		■		■	■	■	■	■	■		■						■	■	■	■	■	■	■	■	0.5
4	■	■			■	■	■	■		■	■	■	■		■		■		■	■			■	■	0.417
5	■	■	■		■	■	■	■		■		■	■	■			■	■	■			■	■		0.33

FIGURE 5. Hamming Distance for SLL OASS.

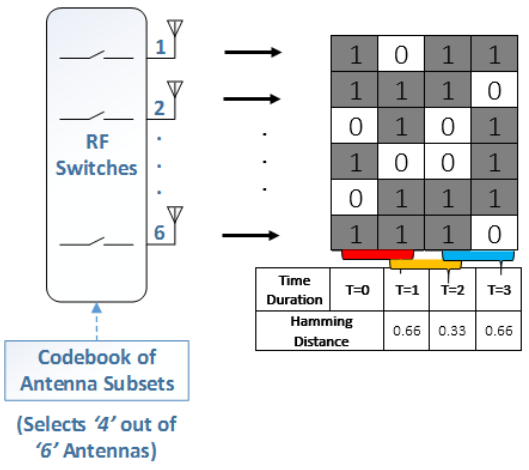

FIGURE 6. An example demonstrating the evaluation of inter-subset hamming distance.

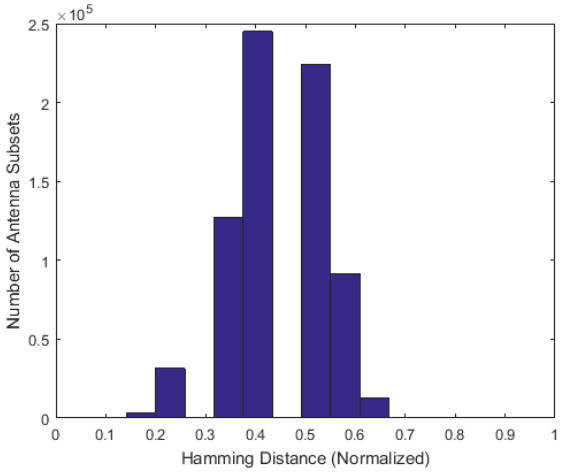

FIGURE 7. Histogram of hamming distance of antenna subsets for RASS.

IV. PHYSICAL LAYER RANDOMNESS (PLR)

PLR is crypthography-inspired metric that has been proposed for analyzing randomness introduced by a PLS technique [22]. PLR also enables direct comparison of encryption strength of physical layer techniques to that of upper layer block ciphering techniques like AES, a strong encryption algorithm.

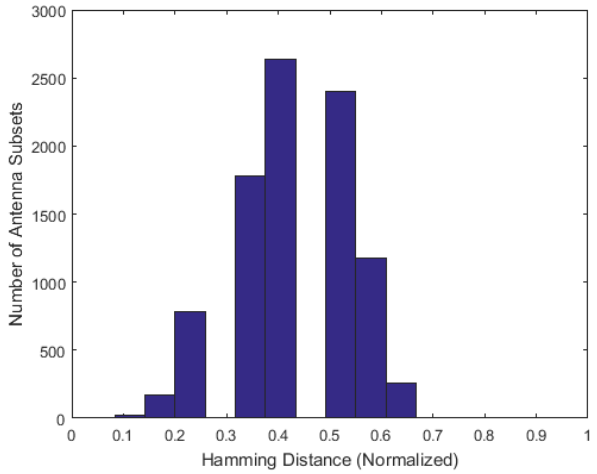

FIGURE 8. Histogram of hamming distance of antenna subsets for SLL optimized ASM.

TABLE 1. Classification of p-values into ranks.

S. No.	Rank	Rank Definition	Description
1	$\zeta = 5$	$p - value \geq 0.5$	Extremely Strongly Passed
2	$\zeta = 4$	$0.4 \leq p - value < 0.5$	Strongly Passed
3	$\zeta = 3$	$0.3 \leq p - value < 0.4$	Moderately Passed
4	$\zeta = 2$	$0.2 \leq p - value < 0.3$	Satisfactorily Passed
5	$\zeta = 1$	$0.01 \leq p - value < 0.2$	Barely Passed
6	$\zeta = F$	$p - value < 0.01$	Failed

PLR consists of 15 standard randomness tests devised by NIST, namely; frequency monobits test, block frequency test, runs test, longest runs of ones in a block test, binary matrix rank test, discrete fourier transform test, non-overlapping template matching test, overlapping template matching test, universal statistical test, linear complexity test, serial test, approximate entropy test, cumulative sums test, random excursion test, and random excursion variant test. The results of each test is recorded as a p-value and accordingly denoted by; P_F, P_B, P_R, P_L, P_K, P_D, P_N, $P_O, P_U, P_C, P_T, P_A, P_S, P_E$ and P_V. A rank ζ is designated to each p-value depending upon its magnitude, as shown in Table 1. The cumulative sum of ranks of all the tests is defined as PLR:

$$PLR = \sum_{z=1}^{N_T} \zeta_z, \tag{16}$$

where N_T represents the total number of tests that has been performed for the analysis of randomness of ciphertext. It is equal to *15* in our case, as we are performing all the NIST tests.

V. SIMULATION RESULTS

In this section, simulation results for hamming distance codebook optimization and its effect on PLR are discussed. A comparison of PLR of HD-OASS with RASS and SLL-OASS is also presented to show the effectiveness of hamming distance maximization.

Consider a uniform linear array of $N = 24$ elements, of which $M = 16$ antennas are randomly turned on for each symbol transmission. The size of codebook (total possible combinations in which antenna subsets could be selected) is thus equal to $C_{16}^{24} = \frac{24!}{16!(24-16)!} = 7.35 \times 10^5$. The direction of IR (i.e. Bob) is known to Alice, which has been assumed to be equal to $\theta_{IR} = 60^o$. The progressive inter-element phase difference (β) is adjusted accordingly at the transmit side to point the main beam in the direction of Bob. The modulation scheme is Quadrature Phase Shift Keying (QPSK).

A. INTER-SUBSET HAMMING DISTANCE OPTIMIZED CODEBOOK

In Fig. 6, a simplified example of ASM with $N = 6$ and $M = 4$ focusing on the calculation of inter-subset hamming distance is presented. At $T = 0$, $M = 4$ antennas are randomly turned ON for transmission of one symbol. The antenna subset for $T = 0$ can be written as:

$$\mathbf{b_0} = [1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1]. \tag{17}$$

For $T = 1$, the antenna subset is:

$$\mathbf{b_1} = [0 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1]. \tag{18}$$

The normalized inter-subset hamming distance between the two antenna subsets is readily calculated, using equation 13, as:

$$d_{01} = \frac{1}{6}\sum_r (mod_2[1+0\ 1+1\ 0+1\ 1+0\ 0+1\ 1+1]) \tag{19}$$

$$\begin{aligned} d_{01} &= \frac{1}{6}\sum_r (mod_2[1 \quad 2 \quad 1 \quad 1 \quad 1 \quad 2]) \\ &= \frac{1}{6}\sum_r [1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0] \\ &= \frac{1}{6} \times 4 \\ &= 0.66 \end{aligned} \tag{20}$$

Similarly, for the next symbol duration $T = 2$, the hamming distance with respect to previous antenna subset is calculated as:

$$\mathbf{b_1} = [0 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1]. \tag{21}$$

For $T = 2$, the antenna subset is:

$$\mathbf{b_2} = [1 \quad 1 \quad 0 \quad 0 \quad 1 \quad 1]. \tag{22}$$

$$d_{12} = \frac{1}{6}\sum_r (mod_2[0+1\ 1+1\ 1+0\ 0+0\ 1+1\ 1+1]) \tag{23}$$

$$\begin{aligned} d_{12} &= \frac{1}{6}\sum_r (mod_2[1 \quad 2 \quad 1 \quad 0 \quad 2 \quad 2]) \\ &= \frac{1}{6}\sum_r [1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0] \\ &= \frac{1}{6} \times 2 \\ &= 0.33 \end{aligned} \tag{24}$$

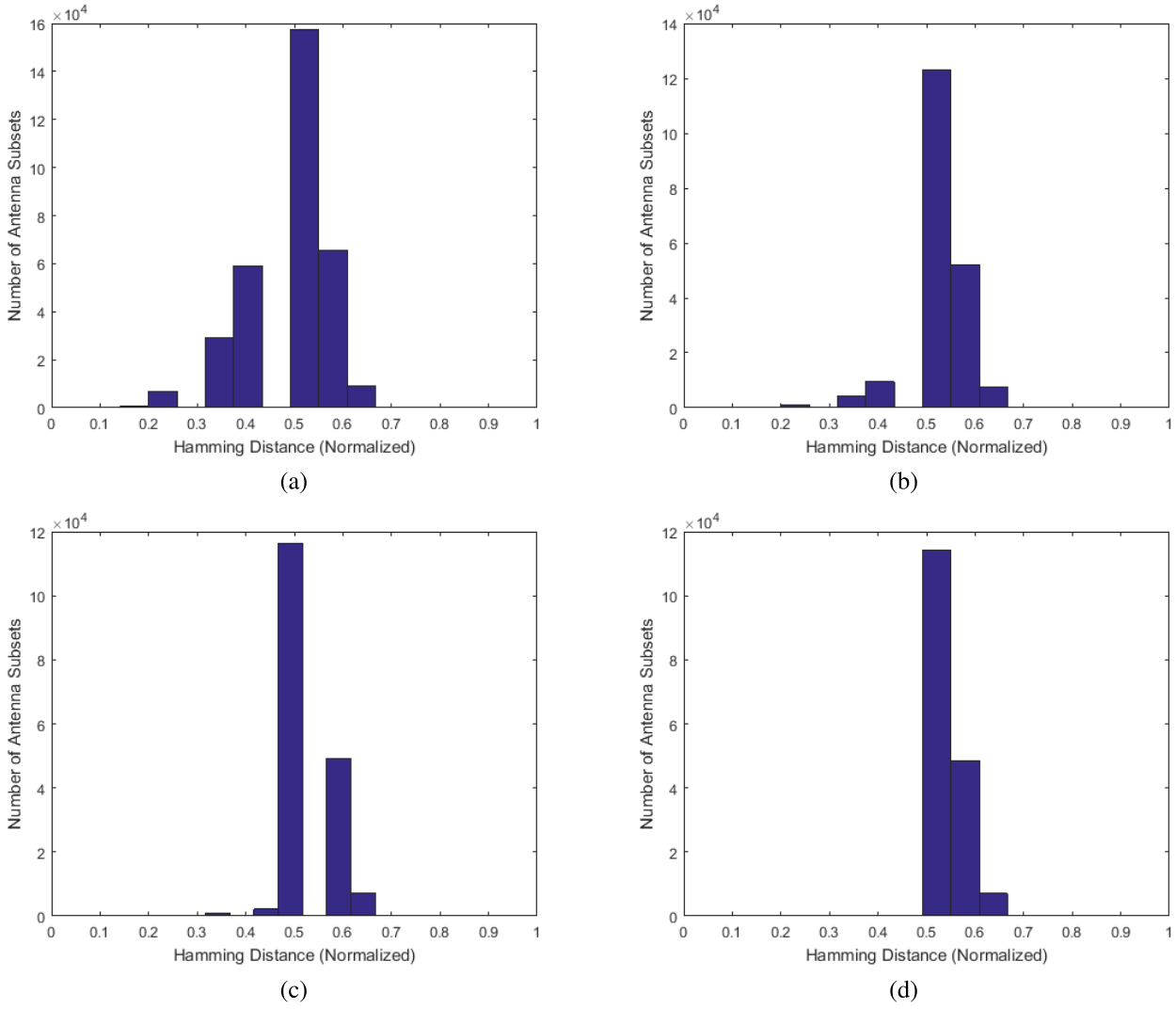

FIGURE 9. Histogram of hamming distance of antenna subsets for HD optimized ASM (a) iteration 1 (b) iteration 3 (c) iteration 5 (d) iteration 9.

In this example, d_{01} is twice the magnitude of d_{12}. This means that the first two subsets have twice the antenna positions that are non-overlapping compared to antenna positions of later two subsets. In HD-OASS, it is desirable to choose only those antenna subsets which have minimum overlap of antenna positions for successively transmitted symbols. Thus, only those antenna subsets which have high d_{ij} are selected and antenna subsets having low value of d_{ij} are discarded.

Calculations of inter-subset hamming distance of *5* randomly selected antenna subsets for different codebooks of ASM are shown in Fig. 3, 4, and 5 for HD-OASS, RASS, and SLL-OASS respectively. Shaded boxes represent the antennas that are ON for that particular symbol duration, while unshaded boxes represent the positions of OFF antennas. For every symbol duration, $M = 16$ antennas are turned on out of $N = 24$ antenna elements. From subset 1 to subset 2 in Fig. 4, the antenna positions that differ with each other are *10*. Therefore, the normalized inter-subset hamming distance is $d_{ij} = \frac{1}{24} \times 10 = 0.416$. In a similar fashion, the calculations are performed for all three codebooks, as shown in Fig. 3, 4, and 5. Notice that HD-OASS, in Fig. 3, has only those antenna subsets which have $d_{ij} \geq 0.5$. Antenna subsets having $d_{ij} \leq 0.5$ are discarded. For SLL-OASS in Fig. 5, the antenna subsets are optimized based on SLL, not hamming distance. Therefore, it contains antenna subsets having d_{ij} as low as *0.25* as well. This imply that the first two antenna subsets of SLL-OASS differ only by 25% with respect to antenna positions.

Refer to Fig. 7, 8, and 9, in which the histograms of normalized inter-subset hamming distance are plotted. Fig. 7 shows the histogram of RASS codebook. It can be seen that it contains all the $C_{16}^{24} = \frac{24!}{16!(24-16)!} = 7.35 \times 10^5$ possible antenna subsets ranging from $d_{ij} = 0.15$ to $d_{ij} = 0.65$. The peak of histogram lies at $d_{ij} = 0.4$. In Fig. 8, the histogram of SLL optimized codebook is shown. SLL optimized codebook, using simulated annealing algorithm, contains

TABLE 2. Comparison of PLR of plain, AES, and ASM encrypted image along Eve direction of 0^o.

Image Data	P_F	ζ	P_B	ζ	P_R	ζ	P_L	ζ	P_K	ζ	P_D	ζ	P_N	ζ	P_O	ζ	P_U	ζ	P_C	ζ	P_T	ζ	P_A	ζ	P_S	ζ	P_E	ζ	P_V	ζ	PLR
Plaintext	0.044	1	0.046	1	0	F	0.0003	F	0	F	0.258	2	0	F	0	F	0	F	0.406	4	0	F	0	F	1	5	0.059	1	0.441	4	18+**8F**
AES	0.426	4	0.406	4	0.253	2	0.311	3	0.03	1	0.564	5	0.41	4	0.124	1	0.316	3	0.398	3	0.079	1	0.244	2	1	5	0.361	3	0.397	3	44
HD-OASS - 0^o	0.423	4	0.403	4	0.253	2	0.306	3	0.027	1	0.562	5	0.337	3	0.028	1	0.422	4	0.411	4	0.018	1	0.242	2	1	5	0.290	2	0.394	3	44
RASS - 0^o	0.406	4	0.399	3	0.225	2	0.294	2	0.028	1	0.561	5	0.165	1	0	F	0.136	1	0.376	3	0	F	0.226	2	1	5	0.389	3	0.399	3	35+**2F**
SLL-OASS - 0^o	0.332	3	0.357	3	0.150	1	0.232	2	0.032	1	0.552	5	0	F	0	F	0	F	0.376	3	0	F	0.155	1	1	5	0.377	3	0.422	4	31+**4F**

TABLE 3. Comparison of PLR of plain, AES, and ASM encrypted image along Eve direction of 40^o.

Image Data	P_F	ζ	P_B	ζ	P_R	ζ	P_L	ζ	P_K	ζ	P_D	ζ	P_N	ζ	P_O	ζ	P_U	ζ	P_C	ζ	P_T	ζ	P_A	ζ	P_S	ζ	P_E	ζ	P_V	ζ	PLR
Plaintext	0.044	1	0.046	1	0	F	0.0003	F	0	F	0.258	2	0	F	0	F	0	F	0.406	4	0	F	0	F	1	5	0.059	1	0.441	4	18+**8F**
AES	0.426	4	0.406	4	0.253	2	0.311	3	0.03	1	0.564	5	0.41	4	0.124	1	0.316	3	0.398	3	0.079	1	0.244	2	1	5	0.361	3	0.397	3	44
HD-OASS - 40^o	0.420	4	0.404	4	0.248	2	0.306	3	0.027	1	0.561	5	0.326	3	0.036	1	0.384	3	0.469	4	0.011	1	0.240	2	1	5	0.364	3	0.393	3	44
RASS - 40^o	0.263	2	0.285	2	0.114	1	0.191	1	0.026	1	0.514	5	0	F	0	F	0	F	0.460	4	0	F	0.100	1	1	5	0.362	3	0.380	3	28+**4F**
SLL-OASS - 40^o	0.337	3	0.355	3	0.172	1	0.238	2	0.030	1	0.560	5	0	F	0	F	0	F	0.424	4	0	F	0.173	1	1	5	0.371	3	0.367	3	31+**4F**

FIGURE 10. Image reconstructed in the direction of IR along $\theta_{IR} = 60^o$.

only those antenna subsets which have low SLL properties. Antenna subsets with high SLL are discarded. Significant reduction of codebook size can be observed in Fig. 8 for SLL-OASS compared to RASS in Fig. 7. The total number of antenna subsets (key space) has declined from 7.35×10^5 for RASS to *9*, *242* for SLL-OASS. This means that limited configurations of antenna subsets for SLL-OASS are to be repeatedly used, the effect of which will be seen in diminished randomness, as discussed later in the paper.

According to the algorithm discussed in section III for inter-subset hamming distance maximization, the codebook is iteratively optimized until all the subsets in the codebook have $d_{ij} \geq 0.5$. In Fig. 9 (a)-(d), histograms of HD-OASS after iteration 1, iteration 3, iteration 5, and iteration 9 are shown respectively. During each iteration, the antenna subsets having $d_{ij} \leq 0.5$ are recursively discarded. After 9^{th} iteration, all the antenna subsets have $d_{ij} \geq 0.5$ as shown in Fig. 9(d). This is the final HD optimized codebook.

B. DIRECTIONAL ENCRYPTION OF IMAGE USING ASM

In this section, the encryption strength of various antenna subset selection techniques of ASM for image data is evaluated. According to NIST recommendations [21], an image of minimum size of 16 MB is transmitted in the intended direction of Bob along $\theta_{IR} = 60^o$. An eavesdropper, situated outside the mainlobe of the antenna array, receives QPSK symbols that are distorted both in phase and amplitude. The adverse effects of SLL-OASS due to codebook size reduction is discussed. Furthermore, HD-OASS has been shown to outperform RASS and SLL-OASS codebooks in terms of physical layer randomness.

The plaintext image transmitted in the direction of Bob, shown in Fig. 10, has the least magnitude of p-values for all the randomness tests, as indicated by red line in Fig. 11. The calculation of PLR of plaintext is given in Table 2. Plaintext has the PLR of *18* and failure of *8* randomness tests, obviously since it is non-encrypted and hence least randomized. AES encrypted image has high magnitude of p-values for all the tests, as indicated by blue line in Fig. 11. It has the PLR of *44* and no *F* rank, as suggested by calculations in Table 2. It is the highest value of PLR and serves as a benchmark for comparing randomness of physical layer security techniques like ASM.

In the direction of Eve, the images reconstructed along $\theta = 0^o$ and 40^o are shown in Fig. 12 and 13 respectively. Following observations can be made in Fig. 12:

1. The image for HD-OASS, in Fig. 12 (a), can be seen to be strongly randomized. Its p-values are plotted as yellow line in Fig. 11 (a) and can be seen to be comparable to AES. It has the PLR of *44* and no *F* ranks, as calculated in Table 2. The encryption strength in this direction is, therefore, equal to that of AES.
2. The image in Fig. 12 (b) for RASS is mildly randomized. The features of the image are visible and reduced p-values can be observed in Fig. 11 (a). It has the PLR of *35* and failure of *2* randomness tests of overlapping template matching and serial test.

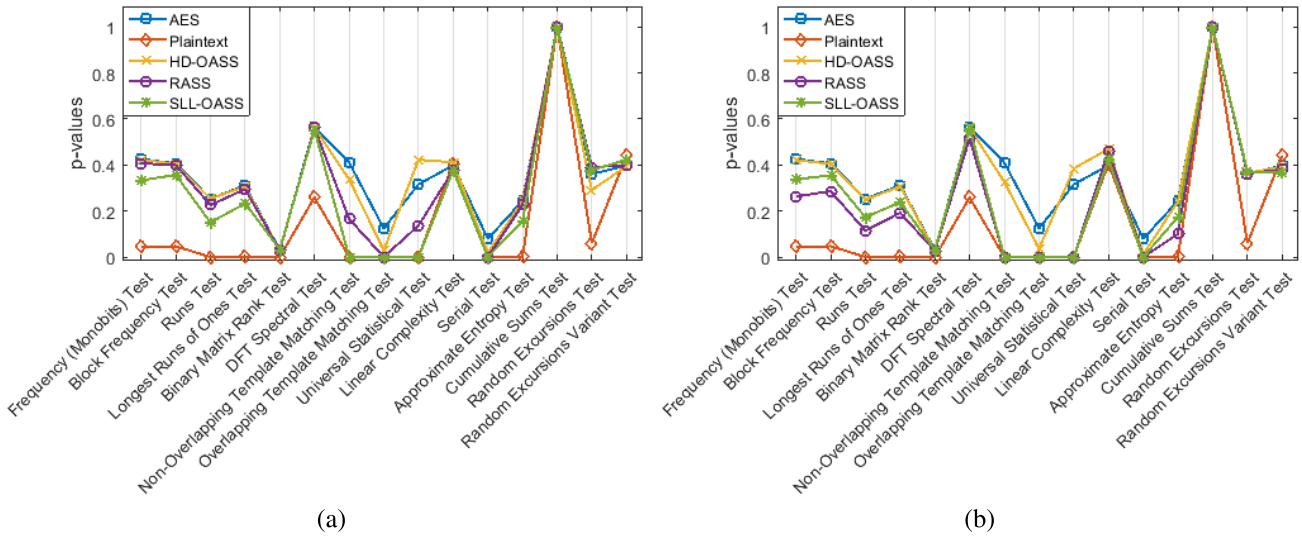

FIGURE 11. Comparison of p-values of AES with ASM for (a) Image along 0^o (b) Audio along 40^o. In general, it can be observed that the magnitude of p-values tend to decrease with SLL optimization, as indicated by green and light blue solid lines in the graphs.

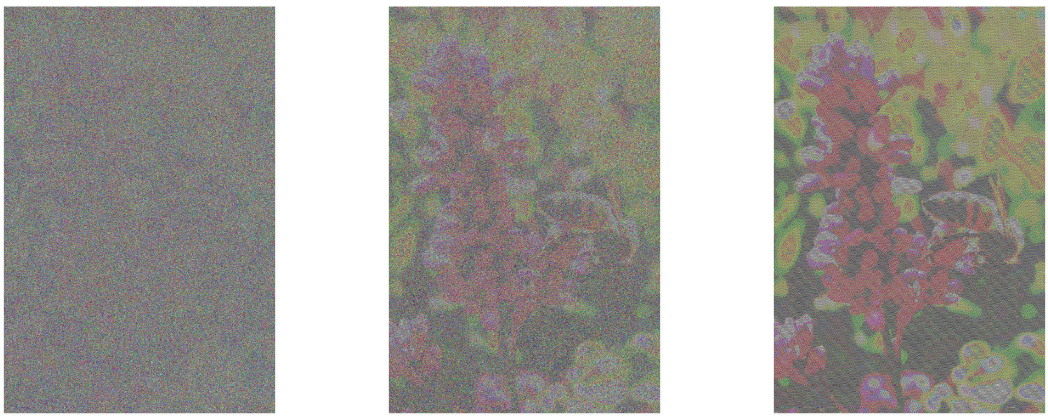

FIGURE 12. Images reconstructed by eavesdropper at 0^o for (a) HD-OASS (b) RASS (c) SLL-OASS.

3. The image is least randomized for SLL-OASS, as shown in Fig. 12 (c). The image features are the most prominent for SLL optimized codebook. Significantly declined p-values are shown as green line in Fig. 11 (a). It has the PLR of *31* and *4 F* ranks, signifying the failure of; non-overlapping template matching, overlapping template matching, universal statistical test, and serial test. Calculations of PLR are summarized in Table 2.

Similar observations can be made for image along $\theta = 40^o$ in Fig. 13, its p-values in Fig. 11 (b), and PLR calculations in Table 3. In both cases, the performance of HD optimized codebook is better than RASS and SLL optimized codebook performs the worst.

C. PLR RESULTS AND PLOTS

As discussed in Section IV, PLR comprises of two components; the magnitude of PLR and the number of failed tests. While high value of PLR is indicative of high encryption strength and good randomness, failed tests signify the existence of patterns of binary data making the data susceptible to eavesdropping. Therefore, for high communication security, it is desirable to have high PLR and least number of failed tests (ideally zero). How much high PLR is sufficient for data security against eavesdropper? AES is the strongest block cipher which is commercially used today. Therefore, the PLR of AES has been used in this work to benchmark the encryption strength of different codebooks of ASM.

Refer to Fig. 14 in which the PLR of HD-OASS is compared to that of RASS and AES for a range of transmit angle ($\theta_{IR} = 60^o$ being the direction of IR). On left y-axis the magnitude of PLR, while on right y-axis the number of failed tests are plotted. The PLR of AES, shown as dotted green line, does not vary with direction because AES is not a directional modulation technique. It provides equally strong encryption for all directions. It can be seen that HD-OASS codebook of

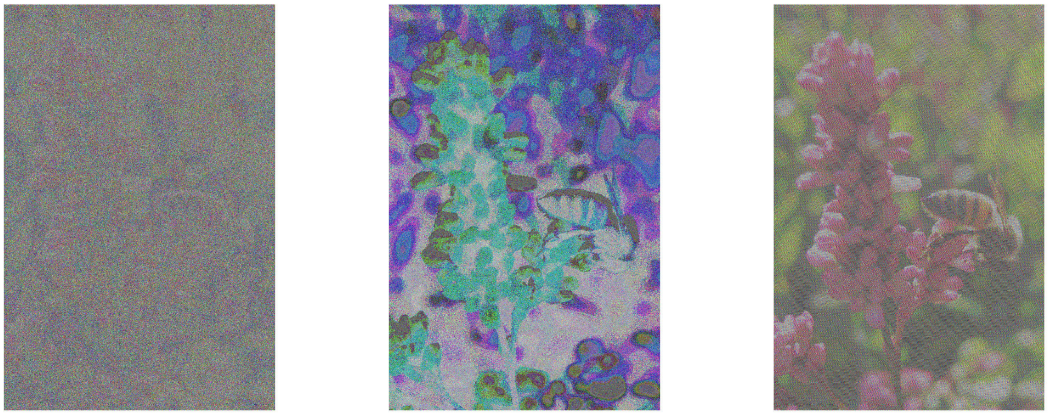

FIGURE 13. Images reconstructed by eavesdropper at 40^o for (a) HD-OASS (b) RASS (c) SLL-OASS.

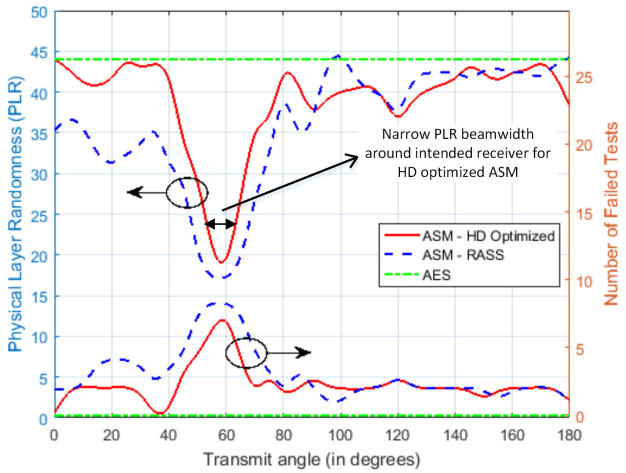

FIGURE 14. Comparison of PLR of inter-subset hamming distance OASS with; RASS and Advanced Encryption Standard.

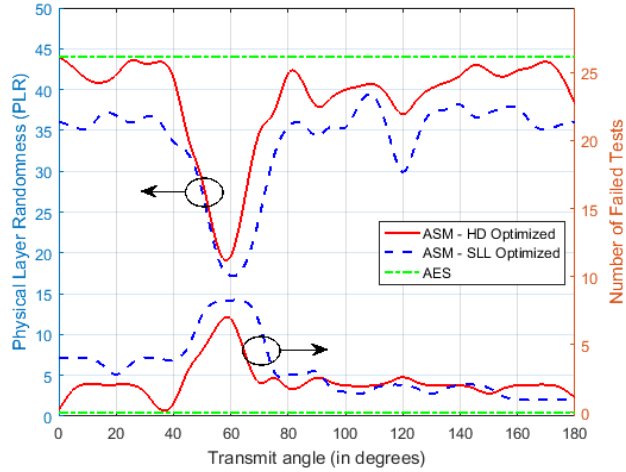

FIGURE 15. Comparison of PLR of inter-subset hamming distance OASS with; sidelobe level OASS and Advanced Encryption Standard.

ASM has better PLR along several directions compared to RASS. In some directions, its PLR is comparable to that of AES. Furthermore, in the vicinity of the direction of IR along $\theta_{IR} = 60^o$, the beamwidth of PLR is about 10^o narrower compared to RASS. Therefore, HD-OASS provides higher directional communication security by producing narrow randomness beamwidth about the desired direction.

A similar comparison of HD-OASS with SLL-OASS can be seen in Fig. 15. For all directions, the PLR of SLL optimized ASM is much lower than HD optimized codebook and the number of failed tests are higher for SLL-OASS. PLR beamwidth of HD-OASS around the intended direction of $\theta_{IR} = 60^o$ is narrower compared to SLL-OASS.

VI. CONCLUSION

In this work, the physical layer encryption strength of ASM has been analyzed. Inter-subset hamming distance maximization has been proposed as a new antenna subset selection technique for ASM which has been shown to significantly outperform previously proposed techniques in terms of PLR. The performance of ASM has been benchmarked against the strong cryptographic standard of AES. HD-OASS has been shown to provide encryption strength comparable to AES along several eavesdropper directions. Furthermore, it is shown that the conventional approach to increase physical layer security by decreasing sidelobe levels (and increasing SER in the undesired directions) using SLL optimized antenna subset selection exhibit rather poor randomness performance compared to randomized antenna subset selection. It renders SLL as inappropriate parameter of optimization for enhancing physical layer security. Diminished PLR of SLL-OASS is attributed to the reduced number of antenna subsets. By discarding antenna subsets having high SLL in the unwanted directions, usable combinations of antenna subsets are significantly reduced, same antenna subsets are used repeatedly, resulting in degraded encryption strength.

REFERENCES

[1] N. N. Alotaibi and K. A. Hamdi, "Switched phased-array transmission architecture for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1303–1312, Mar. 2016.

[2] A. Babakhani, D. B. Rutledge, and A. Hajimiri, "Transmitter architectures based on near-field direct antenna modulation," *IEEE J. Solid-State Circuits*, vol. 43, no. 12, pp. 2674–2692, Dec. 2008.

[3] X. Chen, D. W. K. Ng, W. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1027–1053, 2nd Quart., 2017.

[4] M. P. Daly and J. T. Bernhard, "Directional modulation technique for phased arrays," *IEEE Trans. Antennas Propag.*, vol. 57, no. 9, pp. 2633–2640, Sep. 2009.

[5] M. P. Daly, E. L. Daly, and J. T. Bernhard, "Demonstration of directional modulation using a phased array," *IEEE Trans. Antennas Propag.*, vol. 58, no. 5, pp. 1545–1550, May 2010.

[6] Q. Zhu, S. Yang, R. Yao, and Z. Nie, "Directional modulation based on 4-D antenna arrays," *IEEE Trans. Antennas Propag.*, vol. 62, no. 2, pp. 621–628, Feb. 2014.

[7] T. Hong, M.-Z. Song, and Y. Liu, "Dual-beam directional modulation technique for physical-layer secure communication," *IEEE Antennas Wireless Propag. Lett.*, vol. 10, pp. 1417–1420, Dec. 2011.

[8] Y. Ding and V. Fusco, "A review of directional modulation technology," *Int. J. Microw. Wireless Technol.*, vol. 8, no. 7, pp. 981–993, Nov. 2016.

[9] S. Y. Nusenu, W.-Q. Wang, and S. Ji, "Secure directional modulation using frequency diverse array antenna," in *Proc. IEEE Radar Conf. (RadarConf)*, May 2017, pp. 378–382.

[10] J. Xiong, S. Y. Nusenu, and W.-Q. Wang, "Directional modulation using frequency diverse array for secure communications," *Wireless Pers. Commun.*, vol. 95, no. 3, pp. 2679–2689, Aug. 2017.

[11] J. Hu, S. Yan, F. Shu, J. Wang, J. Li, and Y. Zhang, "Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays," *IEEE Access*, vol. 5, pp. 1658–1667, 2017.

[12] Q. Cheng, J. Zhu, T. Xie, J. Luo, and Z. Xu, "Time-invariant angle-range dependent directional modulation based on time-modulated frequency diverse arrays," *IEEE Access*, vol. 5, pp. 26279–26290, 2017.

[13] M. Bloch and J. Barros, *Physical Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[14] Y. Ding and V. Fusco, *Developments in Directional Modulation Technology*, vol. 13. Orlando, FL, USA: Univ. of Central Florida, Forum for Electromagnetic Research Methods and Application Technologies (FERMAT), Feb. 2016.

[15] N. Valliappan, A. Lozano, and R. W. Heath, "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3231–3245, Aug. 2013.

[16] A. T. V. Murino and C. S. Regazzoni, "Synthesis of unequally spaced arrays by simulated annealing," *IEEE Trans. Signal Process.*, vol. 44, no. 1, pp. 119–123, Jan. 1996.

[17] N. N. Alotaibi and K. A. Hamdi, "A low-complexity antenna subset modulation for secure millimeter-wave communication," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Apr. 2016, pp. 1–6.

[18] A. Akl, A. Elnakib, and S. Kishk, "Antenna array thinning for interference mitigation in multi-directional antenna subset modulation," *Phys. Commun.*, vol. 26, pp. 31–39, Feb. 2018.

[19] C. Chen, Y. Dong, X. Cheng, and N. Yi, "An iterative FFT-based antenna subset modulation for secure millimeter wave communications," in *Proc. Int. Conf. Comput., Netw. Commun. ICNC)*, Silicon Valley, CA, USA, Jan. 2017, pp. 454–459.

[20] Y. Hong, S. Im, and J. Ha, "Secure antenna subset modulation with coordinate interleaved orthogonal designs," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2014, pp. 97–98.

[21] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Nat. Inst. Standards Technol. (NIST), Gaithersburg, MD, USA, NIST special Publication, Tech. Rep. 800-22 Rev 1a, 2010.

[22] O. Ansari, M. Amin, and A. Ahmad, "Analyzing physical layer security of antenna subset modulation as block encryption ciphers," *IEEE Access*, vol. 7, pp. 185063–185075, 2019.

[23] R. Daemen, *The Design of Rijndael*. Berlin, Germany: Springer-Verlag, 2002.

[24] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 2001.

OMAR ANSARI received the B.E. degree in electrical engineering from the University of Engineering and Technology, Taxila, Pakistan, in 2015, and the M.S. degree *(summa cum laude)* in electrical engineering with specialization in RF and microwave from the Institute of Space Technology, Islamabad, Pakistan, in 2019.

He is currently working as a Graduate Research Assistant with the Institute of Space Technology, where he is also involved in the design and development of millimeter-wave front end for high-altitude platform (HAP). His research interests include, but are not limited to, directional modulation techniques for physical layer security, antenna design, RF circuits, and electromagnetics.

MUHAMMAD AMIN received the B.E. degree in avionics from the PAF College of Aeronautical Engineering, NED University, Karachi, Pakistan, in 1988, the master's degree in electrical engineering with specialization in high-frequency techniques from Ruhr University, Bochum, Germany, in 1998, and the Ph.D. degree from Queen's University Belfast (QUB), Belfast, U.K., in 2006. He was an Assistant Professor with the College of Electrical and Mechanical Engineering, National University of Sciences and Technology, Rawalpindi, Pakistan, from 1998 to 2002. He was a Consultant with TDK Electronics to develop phased array antenna for automotive collision avoidance radar. He was a Research Fellow with QUB for approximately one year and an Associate Professor with the Institute of Space Technology (IST), Islamabad, Pakistan, from October 2007 to October 2009. From October 2009 to December 2014, he was the Head of the Antenna and EMI/EMC Labs, Satellite Research and Development Centre, Lahore (SRDC-L), Pakistan, where he was involved in developing monopulse tracking system for satellite and EMI/EMC space qualification tests of the satellite communications systems. Since 2015, he has been a Professor with IST, the Head of the Avionics Department, and the Director of the Cyber and Information Security Laboratory (CISL). His research interests include the development of antennas for radar and cellular communication systems, novel techniques for modulation, and RCS reduction. His research work has resulted in more than 70 publications in major journals and refereed national and international conferences. He is the Inventor of a lowest profile dual polarized antenna. He is mentioned in "Marquis Who is Who in the World" 2008 edition published in USA.

MOAZAM MAQSOOD (Member, IEEE) was born in Faisalabad, Pakistan, in 1983. He received the B.Sc. degree in communication systems engineering from the Institute of Space Technology, Islamabad, Pakistan, in 2006, and the M.S. degree in microwave engineering and wireless subsystem design and the Ph.D. degree in integrated antennas and arrays for GNSS from the University of Surrey, Guildford, U.K., in 2009 and 2013, respectively. He is currently an Assistant Professor with the Department of Electrical Engineering, Institute of Space Technology.

ABDUL RAHMAN MUHAMMAD MAUD (Member, IEEE) received the B.Sc. degree in electrical engineering from the University of Engineering and Technology, Lahore, in 2008, and the M.S. and Ph.D. degrees in electrical and computer engineering from Purdue University, USA, in 2012 and 2015, respectively. He has been working as an Assistant Professor with the Electrical Engineering Department, IST, since 2015. His research interests include signal processing in general, including radar/array signal processing, exploitation of sparsity in signal models, and application of machine learning to various problems.

MUDDASSAR FAROOQ (Member, IEEE) received the B.E. degree from NUST, the M.S. degree from UNSW, Australia, and the Ph.D. degree from TU Dortmund, Germany. He is currently working as the Dean of the Faculty of Engineering, Air University, and also advising the National Center of Cybersecurity, Air University. He has a vast academic, research, and teaching experience that spans over a period of 20 years. During his lifelong teaching, research, and administrative career, he held senior teaching and research appointments at NUST, TU Dortmund, the FAST National University of Computer and Emerging Sciences, and the Institute of Space Technology (IST). Moreover, he has also successfully supervised four Ph.D. students and more than 25 M.S. students in their theses. His H-index stands at 33 and the total number of citations to his research papers is more than 3900. His Ph.D. thesis has been published by Springer Verlag—among the top three publishers in the field of computer science and engineering in the world—as a peer reviewed book titled *Bee-Inspired Protocol Engineering: From Nature to Networks*. After returning to Pakistan, he successfully founded a State-of-the-Art Research Center, nexGIN RC, which has earned an international repute for cyber/information security and e-health/telemedicine research. The center won competitive research funding in the field of cyber security of more than PKR 50 million from different national funding agencies. The research impact of the projects could be judged from more than 55 peer reviewed research papers in world-class journals, conferences, and Lecture Notes in Computer Science (LNCS) series. The projects were state-of-the-art in applying AI and ML research to the fields of network security, information security, malware detection, smart phone security, e-health, tele-medicine, and information and cyber-security. His AI-Based User Authentication System won the Silver Medal in Montreal, Canada, in 2009, in Hummies Competition. His Smart Phone Security Project won the Silver Medal in Montreal, Canada, in Hummies Competition, in 2009. His Intelligent E-Health Project won the Best Project Award in Mexico, in which 110 countries submitted more than 600 projects. His research has received international recognition evident from more than 2000 citations to his work. He is the Co-Founder of a startup with the name—PI INVENT—that deals with 5G/6G communication systems and their security.