

Antenna Subset Modulation for Secure Millimeter-Wave Wireless Communication

Nachiappan Valliappan, Angel Lozano, and Robert W. Heath Jr.

Abstract

The small carrier wavelength at millimeter-wave (mm-Wave) frequencies enables the implementation of a large number of co-located antennas. This paper exploits the potential of large antenna arrays at these frequencies to develop a low-complexity directional modulation technique: Antenna Subset Modulation (ASM) for point-to-point secure wireless communication. The main idea in ASM is to communicate information by modulating the far-field radiation pattern at the symbol rate by driving only a subset of antennas in the array. Two techniques for implementing antenna subset selection are proposed. The first technique is simple where the antenna subset to be used is selected at random for every symbol transmission. While randomly switching antenna subsets does not affect the symbol modulation for a desired receiver along the main lobe direction, it effectively randomizes the amplitude and phase of the received symbol for an eavesdropper along a sidelobe. Using a simplified statistical model for random antenna subset selection, an expression for the average uncoded symbol error rate (SER) is derived as a function of observation angle for linear arrays. To overcome the problem of large peak sidelobe level in random antenna subset switching, an optimized antenna subset selection procedure based on simulated annealing is then discussed. Finally, numerical results comparing the SER performance and secrecy capacity of the proposed techniques against conventional array transmission are presented. While both methods produce a narrower information beam-width in the desired direction, the optimized antenna subset selection technique is shown to offer better security and array performance.

Nachiappan Valliappan and Robert W. Heath Jr. are with the Wireless Networking and Communications Group (WNCG), Department of Electrical and Computer Engineering, The University of Texas at Austin, Austin, TX 78712-1687, USA (email: nachi@utexas.edu, rheath@ece.utexas.edu).

Angel Lozano is with the Department of Information & Communication Technologies, Universitat Pompeu Fabra (UPF), Barcelona 08018, Spain (email: angel.lozano@upf.edu).

I. INTRODUCTION

Recent advances in storage technology and computing power have lead to an increasing demand for high-fidelity digital multimedia content. While current wireline communication standards based on fiber-optic technology can provide data rates at multi-gigabits per second to meet this demand, high infrastructure, installation and maintenance costs prohibit their use in many applications. Using wireless technology as an alternative solution is very attractive mainly because of its low-cost, inherently flexible and scalable nature. However, contemporary wireless systems cannot accommodate services at multi-gigabit rates due to the scarcity of spectrum at conventional operating frequencies (< 3 GHz). This has motivated wireless system designers to explore the millimeter-wave (mm-Wave) frequency band, the radio spectrum between 30 and 300 GHz. The huge swath of spectrum available at mm-Wave can support high-rate point-to-point wireless communication thereby enabling new broadband applications such as uncompressed HD video streaming, high-speed file transfer, console gaming, fixed wireless access, cellular distributed antenna systems and wireless backhaul for next-generation mobile communications [1], [2]. In view of this, several standards and organizations are promoting the use of mm-Wave for wireless personal area networking, local area networking and millimeter-wave mobile broadband [3]–[8].

Enabling mm-Wave radio frequency (RF) technology for large-scale consumer electronics and commercial applications will require the development of power-efficient radios. While standard wireless transceivers for sub-GHz frequencies are based on digital baseband modulation, pushing mm-Wave radios towards a “mostly analog” architecture is essential to reduce the power consumption of baseband circuitry [9], [10]. Another important area of concern for mm-Wave communication is information security. Especially with mm-Wave replacing many previously wireline communication applications such as enterprise networking and inter-base station backhaul, wireless systems in this band should start considering physical (PHY) layer security as a primary system requirement. In particular, point-to-point long-range mm-Wave links operating outside the 60 GHz band are more vulnerable to data interception because of the lower air absorption loss (< 1 dB/km) [11]. Since a conventional phased array transmits the same information in all directions (except for varying power levels), it is possible for a sufficiently sensitive receiver to recover information from the modulated signal.

To improve the security of information transmission, directional modulation (DM) techniques have been considered in the past. Previous work in [12], [13] introduced a novel analog transmit architecture for synthesizing directional information based on near-field direct antenna modulation (NFDAM). In this approach, there is no digital baseband and data modulation happens at the antenna level. Specifically, an

unmodulated carrier signal drives a single antenna element (or a phased array) with multiple reflectors and switches. By varying the antenna near-field electromagnetic boundary conditions using switches, the phase and amplitude of the antenna pattern at far-field is modulated. While carefully chosen switching configurations produce the desired modulation symbols along an intended direction, the nature of the resulting antenna pattern causes the constellation to appear scrambled in undesired directions. We note that, except for [12], [13], much of the prior work on DM techniques [14]–[20] has dealt with sub-GHz communications where small antenna arrays were employed. Recent work in [14]–[16] demonstrates a DM technique for phased array transmitters. By modifying the phase shifts or array weights in each antenna branch, a symbol with desired phase and amplitude can be created along a particular direction, while at the same time purposely distorting the constellation in other directions. A closely related DM signal synthesis technique using pattern-reconfigurable antenna elements was presented in [17]. In [18], hopping among the antenna elements in an array produces a directional frequency/phase modulated signal. DM for spread spectrum communication have been introduced in [19] and [20]. In these methods, the DM signal is modulated at both baseband and antenna level. While [19] proposes a dual beam technique to create a modulated signal using two different radiation patterns, [20] relies on switching antennas based on the chipping sequence.

The design of DM techniques specific to mm-Wave communication can be challenging for two reasons. First, since the carrier wavelength is small, a large number of antennas can be co-located which increases the design space. Exploring a larger design space to find the parameters (like switch combinations in [12], [13], phase shifts in [14] or array weights in [15]) that produce a desired constellation along an intended direction while still enforcing a high error rate in other directions can be difficult. For instance, the number of switch configurations to be explored for producing a desired symbol along a particular direction increases exponentially with array size in [12]. Second, the transmission technique must be able to steer the main beam to a desired direction while still offering directional data modulation. Prior work in [14], [15], [18], [20] do not account for beam-steering since they focus on low frequency communications where it may not be a requirement. The DM technique in [12] can steer the beam to an arbitrary direction in a phased array configuration, but constellation synthesis involves search over a very large design space which may not be practical. [17] has only restricted beam-steering capabilities and requires a separate design procedure for every possible receiver orientation.

In this paper, we propose a low-complexity directional modulation technique - Antenna Subset Modulation (ASM), for point-to-point secure communication. We introduce ASM as an antenna-level modulation technique that eliminates conventional baseband circuitry and takes advantage of the full antenna array

with limited number of RF chains. By providing a simple inter-element phase shift and driving a different subset of antennas in each symbol interval, we show that it is possible to create a direction-dependent modulated signal. Compared to other DM techniques [12]–[15], [17], [19] which scramble the constellation in undesired transmission directions, we find that ASM artificially introduces randomness in the received constellation by antenna subset selection to provide security.

We propose two antenna subset selection techniques to implement ASM in uniform linear arrays. In the first technique, antenna subsets used for transmission are selected at random. We capture this subset selection procedure using a simplified statistical model and show that the received symbol distribution in undesired transmit directions can be closely approximated by a Gaussian distribution. Equipped with the statistics of the received symbol distribution, we evaluate the average uncoded symbol error rate (SER) achieved by ASM for K -ary PSK transmission. To overcome the large peak sidelobe level that may result from random antenna selection, we then propose an optimized antenna subset selection procedure based on simulated annealing. In this technique, we only choose antenna subsets that have good sidelobe properties from a carefully constructed codebook. We perform array transmission simulations and make the following observations: (i) ASM produces a narrow information beam-width towards the desired receiver, (ii) simple random antenna subset selection approach provides better security against eavesdropping compared to conventional array transmission, (iii) optimized antenna subset selection procedure offers the best array and security performance, (iv) ASM maintains a relatively high SER independent of signal-to-noise ratio (SNR) along undesired directions, and (v) ASM achieves better secrecy capacity compared to conventional array transmission over a wide range of angles and SNR.

The key idea to providing secure data transmission in ASM lies in using the large number of degrees of freedom offered by antenna arrays at mm-Wave frequencies. It worth noting that an ASM transmitter provides security benefits while maintaining desirable properties such as fully analog transmit architecture, beam-steering to an arbitrary direction, narrow information beam-width and a simple constellation design procedure.

Organization: The remainder of this paper is organized as follows. In Section II, we introduce the system model and explain the concept of ASM. Then in Section III, we discuss the constellation synthesis procedure for ASM. In Sections IV and V, we propose two antenna subset selection techniques for implementing ASM. In Section VI, we provide simulation results comparing the security and array performance of ASM against conventional array transmission. Finally in Section VII, we draw some conclusions and point out some topics of future work.

Notation: We use the following notation throughout this paper: bold lowercase \mathbf{a} is used to denote

column vectors, bold uppercase \mathbf{A} is used to denote matrices, non-bold letters a, A are used to denote scalar values and calligraphic letter \mathcal{A} is used to denote sets. $|\mathcal{A}|$ denotes the cardinality of a set \mathcal{A} . Using this notation, $|a|$ is the magnitude of a scalar, a^* is the complex conjugate, \mathbf{a}^T is the vector transpose, \mathbf{a}^H is the vector conjugate transpose or Hermitian, \mathbf{a}_k is the k^{th} entry of vector \mathbf{a} , $[\mathbf{A}]_{i,j}$ is the scalar entry of \mathbf{A} in the i^{th} row and j^{th} column, \mathbf{A}^{-1} denotes the inverse of a square matrix, $|\mathbf{A}|$ is the determinant of a square matrix and \mathbf{I}_N denotes an identity matrix of size $N \times N$. $\mathbf{a} \circ \mathbf{b}$ indicates a Hadamard product or entrywise product of two vectors \mathbf{a} and \mathbf{b} of same dimension. We use the notation $\mathcal{N}(\boldsymbol{\mu}, \mathbf{P})$ to denote a real Gaussian random vector with mean $\boldsymbol{\mu}$ and covariance \mathbf{P} , $\mathcal{CN}(\mu, P)$ to denote a complex Gaussian distribution with mean μ and variance P , $\text{Bern}(p)$ to denote a Bernoulli random variable with parameter p and $\mathcal{U}(\cdot)$ to denote a discrete uniform distribution. We use \mathbb{P} to denote probability, $\mathbb{E}[\cdot]$ to denote expectation, $\text{var}[\cdot]$ to denote variance and $\perp\!\!\!\perp$ to denote statistical independence between random variables. $\Re[\cdot]$ and $\Im[\cdot]$ denote the real and imaginary parts, $\binom{N}{M}$ denotes the binomial co-efficient, and \triangleq denotes definition.

II. PRINCIPLE OF ANTENNA SUBSET MODULATION

In this section, we first present the system model considered in this paper. Next, we review conventional array transmission architecture and explain its vulnerability to eavesdropping. Finally, we illustrate the basic principle behind ASM and describe how it achieves direction-dependent data transmission.

A. System Model

For the sake of simplicity, consider a multiple input, single output (MISO) communication system with N transmit antennas and a single receive antenna. The transmitter is equipped with $M \leq N$ RF chains. The receiver's angular location is specified by the 2-tuple (θ, ϕ) where θ and ϕ denote the elevation and azimuth angle respectively ($0 \leq \theta \leq \pi$, $0 \leq \phi \leq 2\pi$). The transmitter is assumed to know the direction of the target receiver, but does not have knowledge on the eavesdroppers location. Assuming a narrowband channel model with perfect synchronization, after sampling the received signal along any direction (θ, ϕ) at discrete-time k can be written as

$$y(k, \theta, \phi) = \mathbf{h}^H(\theta, \phi) \mathbf{x}(k) + v(k) \quad (1)$$

where \mathbf{h} is a $N \times 1$ channel vector, \mathbf{x} is the vector transmit symbol and v is the complex zero-mean additive white Gaussian noise (AWGN) with variance $\frac{N_0}{2}$ per real dimension. The use of a narrowband channel model at mm-Wave is justified because the line-of-sight (LoS) component at these frequencies usually

dominates over multipath components due to relatively high reflection and scattering losses from indoor building materials [21]. Note that the channel vector (and hence, the received symbol) is a function of the receiver's angular location. This is because the path-lengths from the transmit antennas to the receive antenna vary depending on the orientation of the receiver.

Directional beamforming is used to provide sufficient received signal power in mm-Wave systems. With beamforming, $\mathbf{x}(k) = \mathbf{w}(k)x(k)$ where \mathbf{w} is the beamforming vector and x is a scalar transmit symbol. For the LoS channel considered, the beamforming solution that maximizes the received SNR is maximum ratio transmission (MRT). But since the channel coefficients from the transmit array to the receiving antenna have equal magnitude (as given in (3)), MRT is equivalent to equal gain transmission (EGT). Note that uniform amplitude weighting, such as in EGT, maximizes the directivity of the array among all amplitude excitation patterns [22] which is desirable. Another advantage of uniform weighting is that the feeding network is simple.

In this work, we focus on uniformly-spaced linear arrays with isotropic radiating elements; the same approach can be applied to multidimensional periodic arrays i.e., two/three-dimensional arrays that have their elements on an underlying regular grid. For the N -element linear array shown in Fig. 1, the radiating elements are located along the z -axis with uniform inter-element spacing d . The corresponding position vectors are denoted by $\mathbf{p}_0, \mathbf{p}_1, \dots, \mathbf{p}_{N-1}$ with

$$p_{x_n} = p_{y_n} = 0, \quad p_{z_n} = \left(n - \frac{N-1}{2}\right)d, \quad n = 0, 1, \dots, N-1 \quad (2)$$

where the center of the array is placed at the origin to invoke symmetry. We choose $d \leq 0.5\lambda$ to avoid creating grating lobes. The channel vector for a receiver at far-field with elevation angle θ can then be written as [22]

$$\mathbf{h}(\theta) = [e^{j(\frac{N-1}{2})\frac{2\pi d}{\lambda}\cos\theta}, e^{j(\frac{N-1}{2}-1)\frac{2\pi d}{\lambda}\cos\theta}, \dots, e^{-j(\frac{N-1}{2})\frac{2\pi d}{\lambda}\cos\theta}]^T \quad (3)$$

where the phase-shifts introduced by path-length differences are referred to the center of the array. Note that \mathbf{h} is a function of only θ because the linear array cannot resolve ϕ -direction. Next, we will apply this channel model to conventional array transmission and ASM to understand the security aspect of these transmission techniques.

B. Conventional Array Transmission

Fig. 2 shows the block diagram of a typical phased array transmitter where the number transmit antennas is equal number of RF chains i.e., $N = M$. In this transmission scheme, the in-phase (I) and

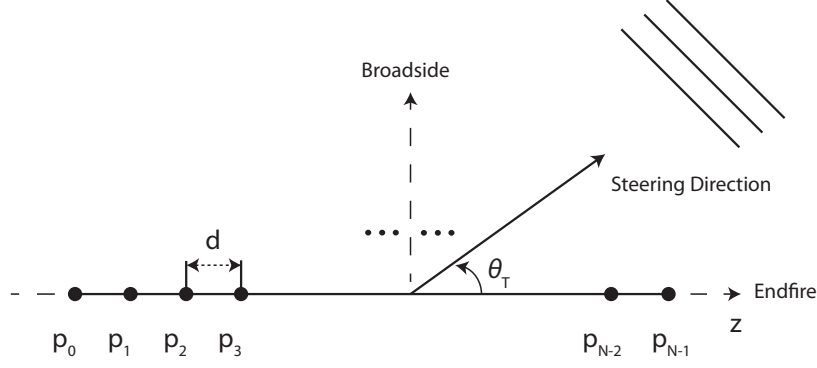


Fig. 1. A uniform linear array with N isotropic elements.

quadrature (Q) components of the signal are modulated at baseband followed by RF up-conversion and antenna array beamforming in the RF domain. Finally, the phase shifted signal in each branch is amplified by a power amplifier (PA) before coupling onto the antenna.

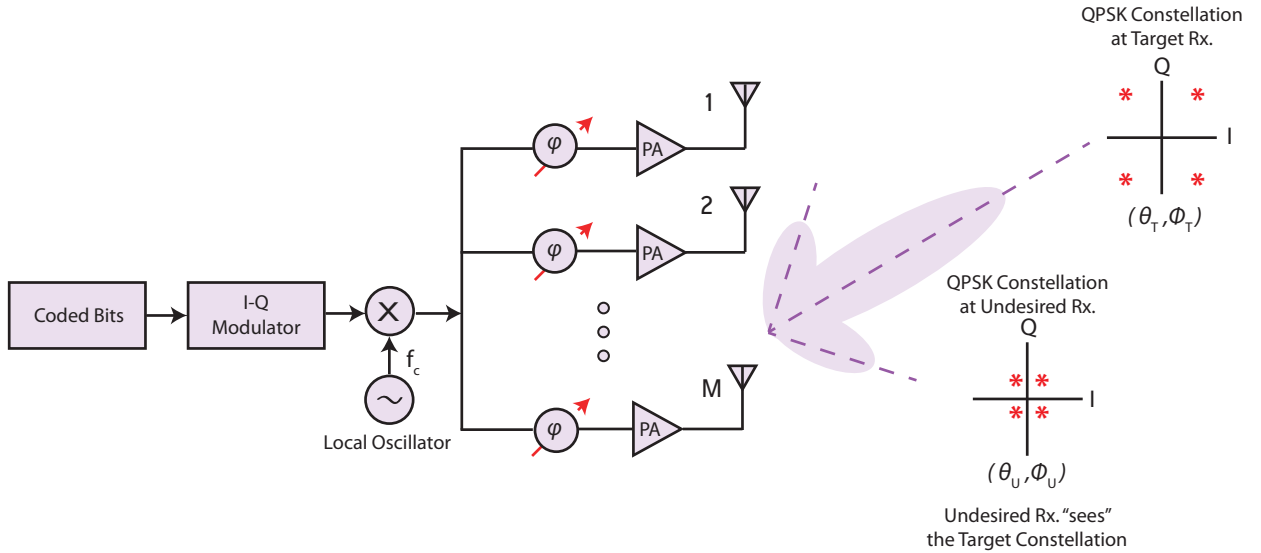


Fig. 2. Typical Phased Array Transmitter - Illustration with QPSK Modulation.

Consider the situation depicted in Fig. 2, where the array is transmitting a complex phase-modulated information symbol, $x(k) = \sqrt{E_s}e^{j\psi(k)}$, to a “target” receiver using conventional baseband modulation technique. The target receiver is oriented towards the (θ_T, ϕ_T) radial and an “undesired” receiver located along the direction (θ_U, ϕ_U) is eavesdropping on the communication. The transmitter is assumed to know the direction of the target receiver, but does not have knowledge on the eavesdropper’s location. By providing a progressive inter-element phase shift, the transmitter can orient its main beam along (θ_T, ϕ_T) i.e., $\mathbf{w}(k) = \frac{1}{M}\mathbf{h}(\theta_T) \forall k$. Using (1), the symbol received along an arbitrary direction (θ, ϕ) in the absence

of noise is

$$\begin{aligned}
y(k, \theta, \phi) &= \mathbf{h}^H(\theta) \mathbf{w}(k) \sqrt{E_s} e^{j\psi(k)} \\
&= \frac{\sqrt{E_s} e^{j\psi(k)}}{M} \sum_{n=0}^{M-1} e^{-j\left(n - \frac{M-1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta_T} e^{j\left(n - \frac{M-1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta} \\
&= \frac{\sqrt{E_s} e^{j\psi(k)}}{M} e^{-j\left(\frac{M-1}{2}\right) \frac{2\pi d}{\lambda} (\cos \theta - \cos \theta_T)} \sum_{n=0}^{M-1} e^{jn \frac{2\pi d}{\lambda} (\cos \theta - \cos \theta_T)} \\
&= \frac{\sqrt{E_s} e^{j\psi(k)}}{M} e^{-j\left(\frac{M-1}{2}\right) \frac{2\pi d}{\lambda} (\cos \theta - \cos \theta_T)} \left(\frac{1 - e^{jM \frac{2\pi d}{\lambda} (\cos \theta - \cos \theta_T)}}{1 - e^{j \frac{2\pi d}{\lambda} (\cos \theta - \cos \theta_T)}} \right) \\
&= \underbrace{\frac{1}{M} \frac{\sin\left(\frac{M(\gamma_\theta - \gamma_{\theta_T})}{2}\right)}{\sin\left(\frac{\gamma_\theta - \gamma_{\theta_T}}{2}\right)}}_{\text{a real constant for every } \theta} \underbrace{\sqrt{E_s} e^{j\psi(k)}}_{\text{information symbol}} \\
&= \rho(\theta) \sqrt{E_s} e^{j\psi(k)}
\end{aligned} \tag{4}$$

where γ_θ is defined (and used in the sequel) as $\gamma_\theta \triangleq \gamma(\theta) = \frac{2\pi d}{\lambda} \cos \theta$ and ρ denotes the (real) scaling factor for every θ . Note that $\rho(\theta) < \rho(\theta_T) = 1 \forall \theta \neq \theta_T$.

In this scenario, both the target and the undesired receiver observe effectively the same information. The constellation received in undesired transmit directions differs (from the target constellation) only in terms of the received signal power and possibly a time delay. This is because in conventional array transmission, the same information is transmitted in all directions with varying sidelobe levels. Therefore, an eavesdropper with a sufficiently sensitive receiver can still recover information from the transmitted signal as illustrated in Fig. 2.

C. Antenna Subset Modulation

1) *Principle:* The small carrier wavelength at mm-Wave enables the construction of phased arrays with a large number of antenna elements. The number of RF chains, however, is still limited by cost constraints. We leverage this possibility to suggest a transmission technique that is suitable for an analog implementation. In an ASM transmitter, there are M RF chains as before but the number of antenna elements $N > M$. A sinusoidal carrier signal drives only a *subset* of the antenna array after passing through phase shifters and PA as illustrated in Fig. 3. Since there are only M RF chains, the antenna subset used for transmission in each symbol interval contains exactly M elements. A control block determines the phase shifts for each branch and selects the subset of M active elements using an high-speed RF switch.

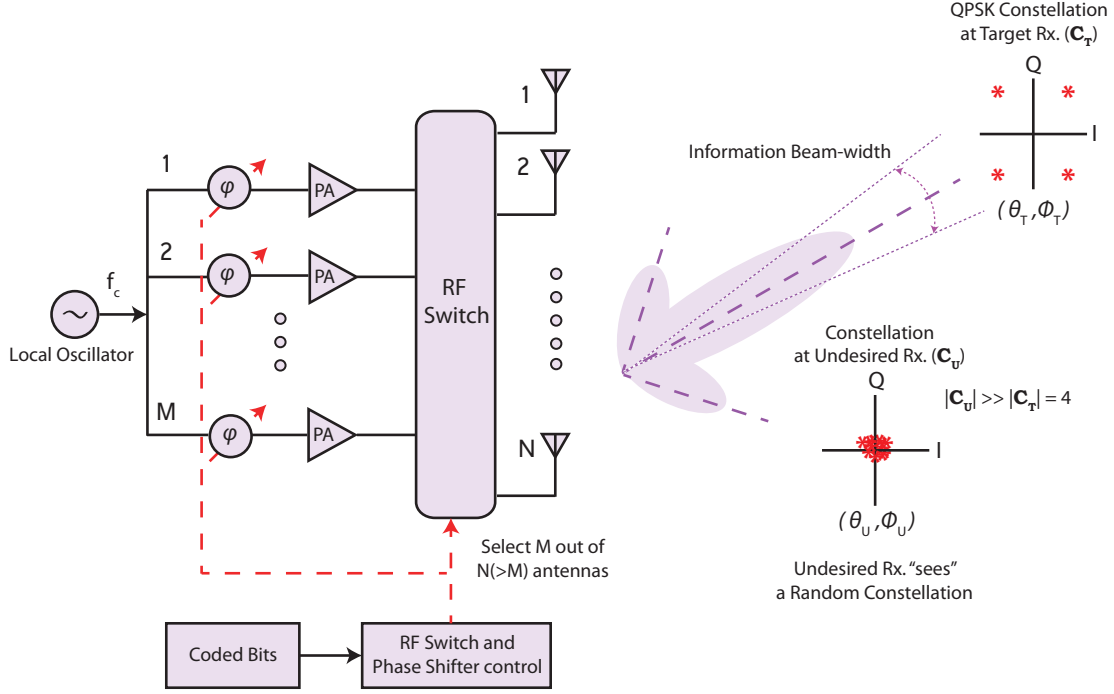


Fig. 3. ASM Transmitter - Illustration with QPSK Modulation. The red dashed line in this figure controls the selection of an antenna subset and provides the corresponding inter-element phase shift necessary for modulation and beam-steering.

The fundamental difference between ASM and conventional array transmission technique is that, modulation in ASM happens in the RF domain. Specifically, the *far-field radiation pattern* of the array is modulated *at the symbol rate* to communicate information. In each symbol duration, the control block synthesizes an array by selecting a subset of M antenna elements. The antenna subset chosen defines the array geometry and an associated far-field radiation pattern. Since the set of antennas used for transmission is changed from one symbol to the next, the far-field pattern of the array appears to be modulated at the symbol transmission rate. It is worth noting here that the changing radiation pattern of the array provides the security benefit of ASM. In the absence of any multipath, the far-field array pattern (along a particular radial) can be interpreted as a complex symbol on the I-Q plane.

Modulation of information bits to symbols and beam-steering is achieved by phase shifting the active elements in the synthesized array. By providing a phase offset besides the progressive inter-element phase shift (for beam-steering), ASM can produce the desired phase of each symbol in a constant-envelope modulation scheme along the target radial. Using the proposed system model, we can mathematically express the signal synthesis in ASM. Since there is no complex-baseband modulation involved, $x(k) = 1 \forall k$ denoting the unmodulated carrier signal. The effect of data modulation, beam-steering and antenna

subset selection operations at time k are succinctly represented by the beamforming vector $\mathbf{w}(k)$.

$$\mathbf{w}(k) = \left(\frac{\sqrt{E_s} e^{j\psi(k)}}{M} \right) [\mathbf{b}(k) \circ \mathbf{h}(\theta_T)] \quad (5)$$

where \mathbf{b} is an $N \times 1$ vector with $\mathbf{b}_i = \{0, 1\}$ and $\sum_{i=0}^N \mathbf{b}_i = M$. The binary vector $\mathbf{b}(k)$ thus encodes the M -element antenna subset picked for transmitting the k^{th} symbol. The positions with ones indicate active antenna elements while zeros indicate unused elements. Let \mathcal{B} denotes the set of all such binary vectors \mathbf{b} . In the absence of receiver noise, the received symbol can be expressed using (1) as

$$\begin{aligned} y(k, \theta, \phi) &= \mathbf{h}^H(\theta) \mathbf{w}(k) \\ &= \underbrace{\frac{1}{M} \mathbf{h}^H(\theta) [\mathbf{b}(k) \circ \mathbf{h}(\theta_T)]}_{\text{a complex scalar depending on } \theta \text{ and } \mathbf{b}(k)} \underbrace{\sqrt{E_s} e^{j\psi(k)}}_{\text{information symbol}} \\ &= \rho(\theta, \mathbf{b}(k)) \sqrt{E_s} e^{j\psi(k)} \end{aligned} \quad (6)$$

for some $\mathbf{b}(k) \in \mathcal{B}$. Note that the scaling factor ρ in (6) is complex for every $\theta \neq \theta_T$ and changes with time index k .

2) *Secure Data Transmission:* In addition to providing directional information to the target receiver, ASM sends misinformation in all undesired directions. This makes it difficult for an eavesdropper to decode any useful information even in the absence of receiver noise.

Suppose that the active element subset, \mathbf{b} , is chosen at random from the set \mathcal{B} for each symbol transmission. The received signal along any radial is the superposition of signals radiated by each antenna element. Because of transmit beamforming along the target direction, the various (phase shifted) signal replicas add coherently in the far-field along the main lobe direction i.e., $y(k, \theta_T, \phi_T) = \sqrt{E_s} e^{j\psi(k)}$ since $\rho(\theta_T, \mathbf{b}(k)) = 1 \forall \mathbf{b}(k) \in \mathcal{B}$. This constitutes creating an undistorted constellation at the target receiver. But, outside of a narrow solid cone centered about the target radial (say along (θ_U, ϕ_U)), the signals add up misaligned in phase. Depending on the antenna subset chosen, the desired modulation symbol appears scaled and rotated for an undesired receiver. This creates a distorted constellation \mathcal{C}_U that is very different from the target constellation \mathcal{C}_T as shown in Fig. 3. The constellation in unintended transmit directions appears “effectively” random because of the random choice of antenna subset for each transmission. Unlike scrambling the desired constellation in unwanted directions [12], [14], [19], ASM synthesizes a multi-point constellation to confuse undesired receivers. The additional constellation points introduced can equivalently be thought as being generated by the changing far-field pattern along the sidelobes because of random antenna subset selection. Thus, while switching the active element subset does not

alter the constellation along the main response axis of the array, the received symbols are distorted in both phase and amplitude for undesired receivers along the sidelobes.

III. ASM CONSTELLATION SYNTHESIS

In this section, we first formulate far-field pattern synthesis for thinned arrays and then make the connection to constellation design for ASM.

A. Far-field Pattern Synthesis

Consider a linear array with $N_t = N$ isotropic radiating elements spaced d apart along the z-axis as described in Fig. 1. For a plane wave propagating along an arbitrary direction \mathbf{k} , the far-field radiation pattern can be expressed as [22]

$$\begin{aligned} F(\mathbf{k}) &= \sum_{n=0}^{N-1} w_n e^{j\mathbf{k}^T \mathbf{p}_n} \\ &= \sum_{n=0}^{N-1} w_n e^{j\left(n - \frac{N-1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta} \end{aligned} \quad (7)$$

where w_n is the complex excitation co-efficient of the n^{th} element and λ is the wavelength corresponding to a carrier frequency f_c . The second equality in (7) is obtained by substituting for \mathbf{k} using $\mathbf{k} = (k_x, k_y, k_z) = \frac{2\pi}{\lambda} (\sin\theta \cos\phi, \sin\theta \sin\phi, \cos\theta)$.

By applying a time-varying excitation to each element, the far-field array pattern can be modulated. Using (7), we can represent the time-varying far-field pattern as

$$F(t, \theta) = \sum_{n=0}^{N-1} w_n(t) e^{j\left(n - \frac{N-1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta}. \quad (8)$$

In ASM, only a subset of $M(< N)$ antenna elements is selected for use during each symbol transmission. This process of selectively turning on or equivalently, turning off certain elements in an array is called *array thinning* and the array thus synthesized is referred to as a thinned array. The fraction of active elements, $\frac{M}{N}$, is called the thinning percentage. An example of a thinned array is illustrated in Fig. 4.

The M active elements of the thinned array are excited by complex constant-modulus (uniform amplitude) weights. If T denotes the symbol duration, the excitation coefficient for the n^{th} element while transmitting the k^{th} symbol, $(k-1)T < t \leq kT$, is expressed as

$$w_n(k) = \begin{cases} \alpha e^{j\varphi_n(k)} & n \in \mathcal{I}(k) \\ 0 & n \notin \mathcal{I}(k) \end{cases} \quad (9)$$

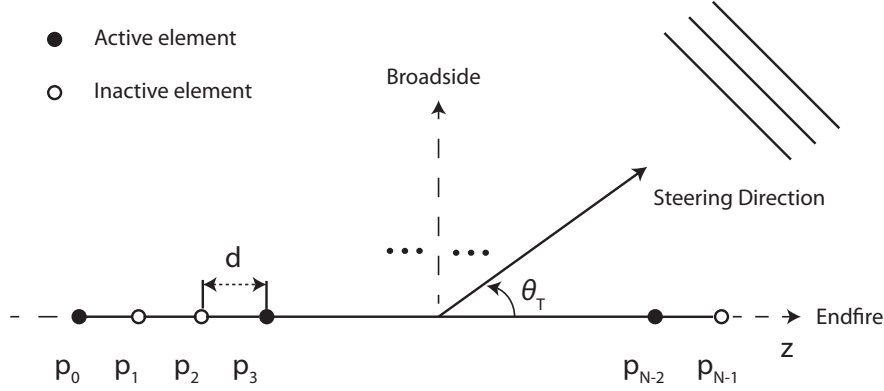


Fig. 4. An example of a thinned linear array.

where k is the discrete-time index, α is a real constant that controls signal energy, $\varphi_n(k)$ is the phase shift applied to the n^{th} antenna element and $\mathcal{I}(k)$ denotes the set of M antennas used for transmitting the k^{th} symbol. The set $\mathcal{I}(k)$ encodes the location of the active elements for time index k . An antenna element in the array is considered selected or active if and only if its position index is present in the set \mathcal{I} . Also, the cardinality of this set must be equal to M to enforce the constraint on the total number of active elements. Thus, for a given inter-element spacing d , $\mathcal{I}(k)$ completely characterizes the resulting spatially non-uniform array. Mathematically,

$$\mathcal{I}(k) \subset \{0, 1, \dots, N-1\}, |\mathcal{I}(k)| = M \quad \forall k. \quad (10)$$

In the absence of mutual coupling effects, using (9) in (8) we have,

$$F(k, \theta) = \sum_{n \in \mathcal{I}(k)} \alpha e^{j\varphi_n(k)} e^{j\left(n - \frac{N-1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta}. \quad (11)$$

Equation (11) expresses the far-field pattern of the synthesized linear array as a function of direction and time index. As an example, the synthesized far-field radiation pattern for a $N = 12$ element linear array with $d = 0.5\lambda$ and $M = 9$ active elements is shown in Fig. 5. In our notation, the set of active elements for this example is denoted by $\mathcal{I}(k) = \{1, 2, 4, 5, 6, 7, 8, 9, 11\}$.

B. Constellation Design

ASM can be used to produce the desired phase of each symbol in a constant-envelope modulation scheme. The use of constant envelope signals in ASM accounts for two characteristics that sharply distinguish mm-Wave communication from sub-GHz wireless technologies. First, the availability of large spectral space at mm-Wave frequencies has promoted the use of low modulation techniques that have low spectral efficiency such as K -ary PSK. Second, the use of constant envelope signals minimizes

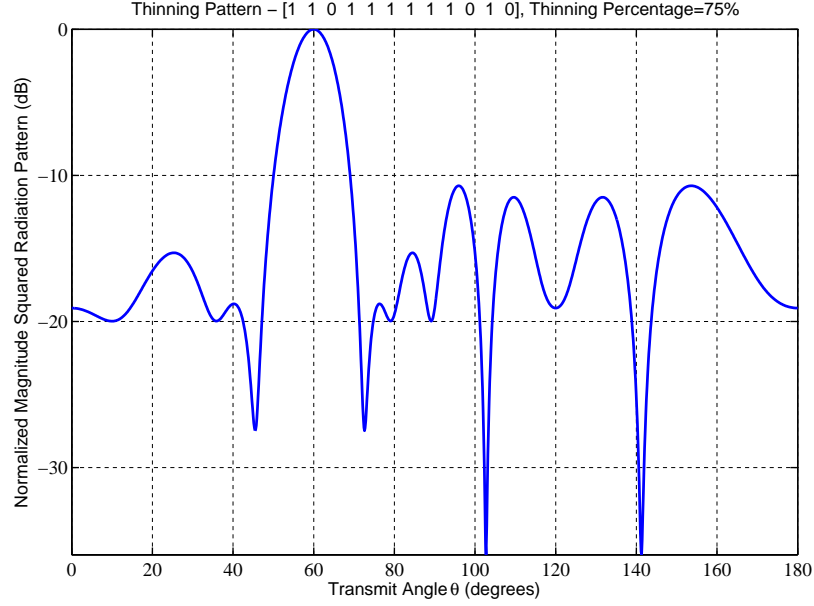


Fig. 5. Far-field magnitude squared radiation pattern of a thinned linear array steered to $\theta_T = 60^\circ$. Thinning pattern is represented by a binary vector.

the linearity requirement on the PA and provides high power-efficiency by operating near the saturation region. Also, modulation schemes such as multi-level QAM are challenging to implement at mm-Wave mainly because of their sensitivity to the relatively high phase noise [9]. Nevertheless, ASM can still use a highly efficient switching PA to transmit non-constant envelope modulated signals. But we defer this extension to future work.

Data modulation in ASM is based solely on the active element phase shifts. Since EGT also involves configuring phase shifts in each branch, we will perform modulation and beam-steering operations jointly. Suppose that the desired modulation symbol to be synthesized at time k has magnitude and phase given by $\sqrt{E_s}$ and $\psi(k)$ respectively. Equivalently, we require the far-field pattern produced along θ_T to equal the desired modulation symbol i.e., $F(k, \theta_T) = \sqrt{E_s}e^{j\psi(k)}$.

First, we identify the set of phase shifts to perform beam-steering towards the target receiver. It is well known that by applying a simple progressive inter-element phase shift, it is possible to steer the main response axis of an N -element uniform linear array to an arbitrary direction. The phase shift applied to the n^{th} element to achieve beam-steering towards the θ_T direction is given by [22]

$$\delta_n = -\left(n - \frac{N-1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta_T, \quad n = 0, 1, \dots, N-1 \quad (12)$$

where the phase shift is referred to the center of the array to invoke symmetry. For a thinned linear array where only a subset of M elements are active, the inter-element phase shifts needed to perform

beam-steering are still given by (12). In this case, however, n takes values only from the active element subset $\mathcal{I}(k)$. Hence, the beam-steering vector changes depending on the active element subset chosen for symbol transmission.

Substituting $\varphi_n(k) = \delta_n$ in (11) and using (12),

$$\begin{aligned} F(k, \theta_T) &= \sum_{n \in \mathcal{I}(k)} \alpha e^{-j\left(n - \frac{N-1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta_T} e^{j\left(n - \frac{N-1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta_T} \\ &= M\alpha. \end{aligned} \quad (13)$$

The array response in (13), or equivalently, the modulation symbol produced at far-field along the target radial is real (has only an in-phase component) with magnitude $M\alpha$. To produce the desired magnitude, $\sqrt{E_s}$, the scaling factor α is chosen to be

$$\alpha = \frac{\sqrt{E_s}}{M}. \quad (14)$$

Next, to obtain a symbol with the desired phase, $\psi(k)$, the beam-steering vector has to be rotated by the same amount. Note that any phase rotation on the steering vector does not alter the beamforming characteristics of the array. Thus, the inter-element phase shift to be provided on each branch to produce the desired complex symbol along θ_T direction is given by

$$\begin{aligned} \varphi_n(k) &= \psi(k) + \delta_n \\ &= \psi(k) - \left(n - \frac{N-1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta_T, \quad n \in \mathcal{I}(k). \end{aligned} \quad (15)$$

Finally, using (14) and (15) in (11), the far-field pattern of the array along θ_T is

$$\begin{aligned} F(k, \theta_T) &= \sum_{n \in \mathcal{I}(k)} \alpha e^{j\left(\psi(k) - \left(n - \frac{N-1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta_T\right)} e^{j\left(n - \frac{N-1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta_T} \\ &= \sqrt{E_s} e^{j\psi(k)}. \end{aligned} \quad (16)$$

It is critical to recognize that the signals from each antenna element add up with perfect alignment along the mainlobe direction to produce the desired symbol at far-field *irrespective of the antenna subset picked* i.e., any randomness in the choice of antenna subset $\mathcal{I}(k)$ disappears along $\theta = \theta_T$. Thus, by appropriately varying the inter-element phase shifts, ASM can produce the phase of each symbol in a constant-envelope modulation scheme.

Notice that only the inter-element phase shift needs to be changed to transmit along an arbitrary direction. This makes the constellation design procedure in ASM much simpler compared to other DM techniques such as [12], [14], [23] where one must typically run an optimization algorithm to identify

the right set of weights, phase shifts or switching combinations required to produce a desired modulation symbol for each target direction. Moreover, these directional transmission methods may suffer from symbol approximation errors with respect to a true constellation point whereas the symbols synthesized by ASM are exact along any target radial. In the next section, we demonstrate how ASM achieves secure transmission using a simple antenna subset selection technique.

IV. ASM FOR SECURE COMMUNICATION

This section describes the security aspect of ASM. It is assumed that the location of the eavesdropper is unknown to the transmitter. If the antenna subset used for each transmission is chosen independently at random, it is shown that outside of a solid cone centered towards the target, the modulation symbol synthesized by ASM appears effectively “random” and can be well-approximated by a two-dimensional Gaussian distribution as the number of antennas become large.

A. Random Antenna Subset Selection

Random Antenna Subset Selection (RASS) is a simple antenna subset selection technique for ASM. In this technique, we select a set of M antenna elements (out of N) to be independently at random for each symbol transmission. Therefore, the antenna subset chosen for transmitting a particular symbol is equally likely to be picked from the set of all possible subsets containing M active elements. This random selection of antenna subsets modifies the array geometry and hence the associated far-field pattern. While the signals from each antenna element add *coherently* along the main lobe direction independent of the antenna subset picked (see (16)), they add up *misaligned* in phase and constitute signal defocussing along any sidelobe direction. The resultant is a cluster of points being transmitted in unwanted directions even when the same transmit symbol is communicated along the target direction. Thus, a *one-to-many* bit-symbol mapping is created in all undesired directions, rendering it difficult to demodulate information for a receiver off the target angle. The presence of receiver noise only makes it more difficult to demodulate information as the variance of the received symbol is now increased compared to the noiseless case. An example illustrating the randomization of a transmit symbol in an undesired direction is shown in Fig. 6. The choice of an antenna subset defines an array geometry and the associated far-field radiation pattern. Since the antenna subsets used for transmission are picked at random, the arrays synthesized using RASS have a larger sidelobe level on average. Nevertheless, RASS technique yields itself to a simplified statistical analysis and provides the basic intuition behind secure transmission using ASM. In

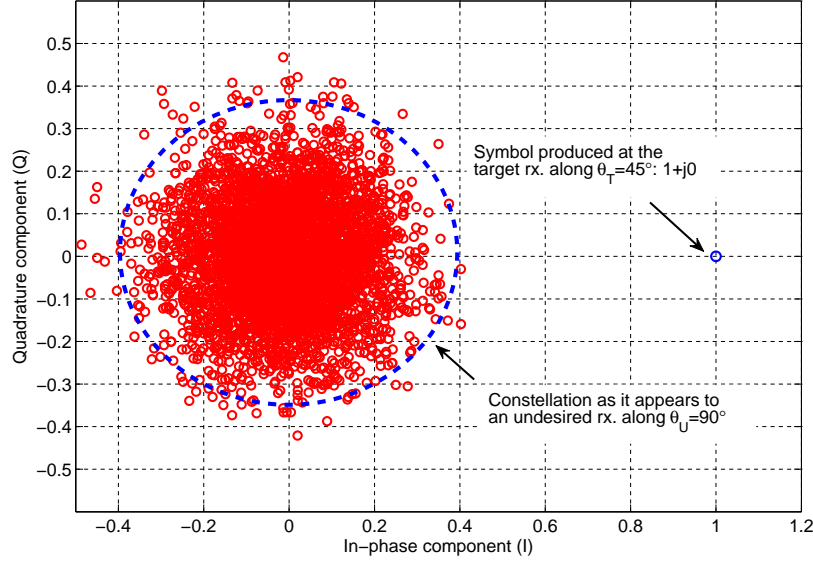


Fig. 6. Received constellation as it appears to an undesired and desired receiver when using RASS in ASM to transmit the symbol $1 + j0$ repeatedly. The parameters of the randomly synthesized array are $N = 20$, $M = 12$ and $\theta_T = 45^\circ$.

Section V we propose an optimized antenna subset selection technique that achieves improved sidelobe level and error rate performance.

B. Statistical Model and Analysis

Consider an N -element linear array with inter-element spacing d communicating a K -ary PSK signal to the target. The constellation has an average symbol energy E_s and each symbol is equally likely to be picked. The modulation symbols are represented by

$$s_\ell = \sqrt{E_s} e^{j\ell 2\pi/K}, \quad \ell = 0, 1, \dots, K-1. \quad (17)$$

Let θ_T denote the target orientation and Ω denote the angular region outside of a solid cone around the target radial where the signals add incoherently i.e., $\Omega \triangleq \{(\theta, \phi) : \theta \notin (\theta_T - \zeta, \theta_T + \zeta)\}$ for some small value $\zeta > 0$ (usually $\zeta \approx$ distance to the first null). Since the antenna elements in the array are picked independently at random for every symbol transmission, we can model each element as an independent derived Bernoulli random variable with parameter p denoting the probability of element selection. Choosing $p = \frac{M}{N}$, the thinning ratio, ensures that the arrays synthesized have M active elements asymptotically. The far-field pattern of the array $F(k, \theta)$ is then modeled as a sum of N independent complex random variables (for each k) whose first- and second-order statistics can be derived analytically. We will then use this statistics to approximate the uncoded SER (hereafter referred

to as simply SER) produced by randomized antenna selection technique. While the proposed statistical model closely approximates the far-field pattern of the actual array synthesized by RASS for $\theta \in \Omega$, the approximation may not be accurate inside the solid cone. This is because inside the cone, the signals from different antennas add constructively. Thereby, any randomness introduced by antenna subset selection disappears and the constellation produced approaches \mathcal{C}_T , which is far from random.

Let $X_n(k)$ be a complex random variable denoting the weighting coefficient on the n^{th} antenna element when transmitting the k^{th} symbol. We can express $X_n(k)$ as a product of two independent random variables $Y_n(k)$ and Z_n i.e.,

$$X_n(k) = Y_n(k)Z_n \quad (18)$$

where $Y_n(k)$ - models randomness in transmit symbol selection, Z_n - models randomness in antenna element selection. According to the proposed statistical model, $Y_n(k)$ and Z_n are distributed as follows:

$$Y_n(k) = \alpha e^{j\delta_n} e^{j\psi(k)}, \quad n = 0, 1, \dots, N-1, \quad (19)$$

$$\psi(k) \sim \mathcal{U}\left(\frac{1}{K}\right) \quad \forall k \text{ i.e., } \mathbb{P}\left(\psi(k) = \ell \frac{2\pi}{K}\right) = \frac{1}{K} \quad \ell = 0, 1, \dots, K-1, \quad (20)$$

$$Z_n \sim \text{Bern}\left(\frac{M}{N}\right) = \begin{cases} 1 & \text{w.p. } \frac{M}{N} \\ 0 & \text{w.p. } 1 - \frac{M}{N} \end{cases} \quad n = 0, 1, \dots, N-1 \quad (21)$$

where δ_n and α are defined previously in (12) and (14) respectively. By construction, $Z_i \perp\!\!\!\perp Z_j$ if $i \neq j$, $\forall i, j \in \{0, 1, \dots, N-1\}$ and $Y_n(i) \perp\!\!\!\perp Y_n(j)$ if $i \neq j$. Therefore, $Y_n(k)$ is non-random for any given symbol index k , but can take values independently (based on the distribution of $\psi(k)$) from one symbol transmission to the next. Rewriting $X_n(k)$ in terms of $Y_n(k)$ using (18) and (21),

$$X_n(k) = \begin{cases} Y_n(k) & \text{w.p. } \frac{M}{N} \\ 0 & \text{w.p. } 1 - \frac{M}{N} \end{cases} \quad (22)$$

Analogous to equation (11), an approximate stochastic model for the far-field pattern of a thinned array synthesized using RASS can be written as

$$\tilde{F}(k, \theta) = \sum_{n=0}^{N-1} X_n(k) e^{j\left(n - \frac{N-1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta} \quad (23)$$

where the \sim differentiates the stochastic model from the true far-field pattern $F(k, \theta)$ produced by RASS. For any given k , (23) is a weighted sum of N independent and identically distributed (i.i.d.) complex random variables. In view of central limit theorem, this sum can be closely approximated by a complex Gaussian distribution, for N large enough i.e., $\tilde{F}(k, \theta) \sim \mathcal{CN}(\tilde{\mu}(k, \theta), \tilde{P}(k, \theta))$. Equivalently, the real

(in-phase) and imaginary (quadrature) part of $\tilde{F}(k, \theta)$ can be stacked to form a two-dimensional real Gaussian vector $\tilde{\mathbf{f}}(k, \theta)$

$$\tilde{\mathbf{f}}(k, \theta) = \begin{bmatrix} \Re[\tilde{F}(k, \theta)] \\ \Im[\tilde{F}(k, \theta)] \end{bmatrix} \sim \mathcal{N}(\tilde{\boldsymbol{\mu}}(k, \theta), \tilde{\mathbf{P}}(k, \theta)) \quad (24)$$

where $\tilde{\boldsymbol{\mu}}(k, \theta) \in \mathbb{R}^{2 \times 1}$ and $\tilde{\mathbf{P}}(k, \theta) \in \mathbb{R}^{2 \times 2}$ denote the mean and covariance of the two-dimensional real Gaussian distribution. Note that the parameters of the distribution depend on the observation angle θ and implicitly on the transmit symbol through time index k . The normal approximation improves as N increases and is better when the thinning ratio $\frac{M}{N}$ is not too close to 0 or 1. Fig. 7 depicts the goodness of a Gaussian fit to the empirical distribution of the I and Q components produced by RASS along an undesired transmit direction. In this example, the main response axis of a 35-element linear array was steered towards $\theta_T = 36^\circ$. A histogram of the I and Q components of the received symbol along $\theta = 10^\circ$ is shown.

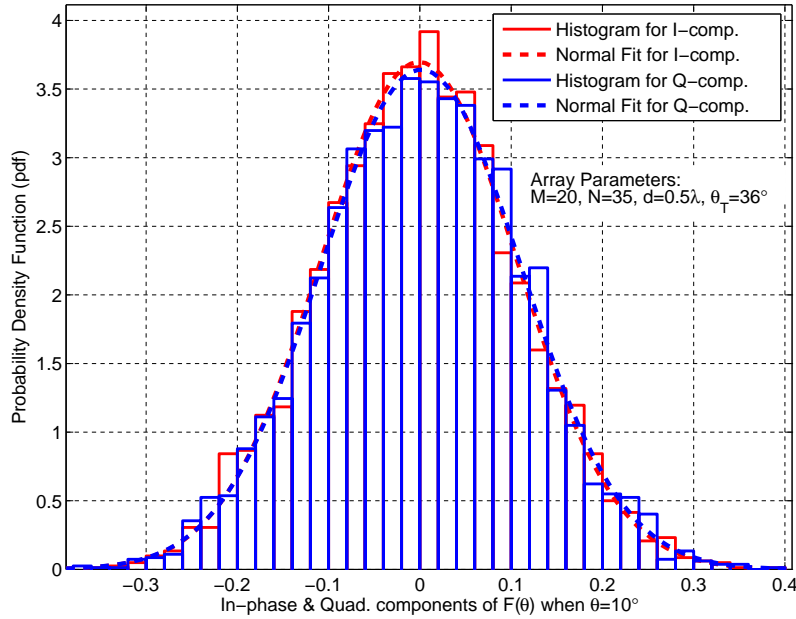


Fig. 7. Histogram of the I and Q components of the symbol received along an undesired direction when using RASS. The corresponding Gaussian fits are overlaid.

To analyze the average SER for ASM under RASS, we only need a statistical description of the received symbol cluster (as a function of direction) when transmitting an arbitrary symbol to the target. Therefore, for SER analysis we remove any randomness in transmit symbol selection i.e., $Y_n(k) = Y_n =$

$\alpha e^{j\delta_n} e^{j\psi}, \forall k$ and focus on characterizing the distribution of the received symbol using our statistical model (23). To emphasize this assumption and simplify notation, we will drop the dependence of $X_n, \tilde{F}, \tilde{\mathbf{f}}$ and associated model statistics on the symbol index k .

Since the received symbol is approximately Gaussian distributed in undesired transmit directions, we only need the mean and covariance to characterize its distribution. Taking the expectation on both sides of (23) and using the definitions in (12) and (14), the complex mean is given by

$$\begin{aligned}
\tilde{\mu}(\theta) &\triangleq \mathbb{E}[\tilde{F}(\theta)] = \mathbb{E} \left[\sum_{n=0}^{N-1} X_n e^{j(n - \frac{N-1}{2}) \frac{2\pi d}{\lambda} \cos \theta} \right] \\
&= \sum_{n=0}^{N-1} \mathbb{E}[X_n] e^{j(n - \frac{N-1}{2}) \frac{2\pi d}{\lambda} \cos \theta} \\
&= \sum_{n=0}^{N-1} \alpha e^{j\psi} e^{j\delta_n} \left(\frac{M}{N} \right) e^{j(n - \frac{N-1}{2}) \frac{2\pi d}{\lambda} \cos \theta} \\
&= \frac{\sqrt{E_s} e^{j\psi}}{N} \sum_{n=0}^{N-1} e^{-j(n - \frac{N-1}{2}) \frac{2\pi d}{\lambda} \cos \theta_T} e^{j(n - \frac{N-1}{2}) \frac{2\pi d}{\lambda} \cos \theta} \\
&= \frac{\sqrt{E_s} e^{j\psi}}{N} e^{-j(\frac{N-1}{2}) \frac{2\pi d}{\lambda} (\cos \theta - \cos \theta_T)} \sum_{n=0}^{N-1} e^{jn \frac{2\pi d}{\lambda} (\cos \theta - \cos \theta_T)} \\
&= \frac{\sqrt{E_s} e^{j\psi}}{N} e^{-j(\frac{N-1}{2}) \frac{2\pi d}{\lambda} (\cos \theta - \cos \theta_T)} \left(\frac{1 - e^{jN \frac{2\pi d}{\lambda} (\cos \theta - \cos \theta_T)}}{1 - e^{j \frac{2\pi d}{\lambda} (\cos \theta - \cos \theta_T)}} \right) \\
&= \frac{\sqrt{E_s} e^{j\psi}}{N} \left(\frac{\sin \left(\frac{N \frac{2\pi d}{\lambda} (\cos \theta - \cos \theta_T)}{2} \right)}{\sin \left(\frac{\frac{2\pi d}{\lambda} (\cos \theta - \cos \theta_T)}{2} \right)} \right) \\
&= \frac{1}{N} \frac{\sin \left(\frac{N(\gamma_\theta - \gamma_{\theta_T})}{2} \right)}{\sin \left(\frac{\gamma_\theta - \gamma_{\theta_T}}{2} \right)} \sqrt{E_s} e^{j\psi}.
\end{aligned} \tag{25}$$

Using (25), we can express $\tilde{\boldsymbol{\mu}}(\theta)$ as

$$\begin{aligned}
\tilde{\boldsymbol{\mu}}(\theta) &\triangleq \mathbb{E}[\tilde{\mathbf{f}}(\theta)] = \begin{bmatrix} \Re[\tilde{\mu}(\theta)] \\ \Im[\tilde{\mu}(\theta)] \end{bmatrix} \\
&= \begin{bmatrix} \frac{\sqrt{E_s}}{N} \left(\frac{\sin \left(\frac{N(\gamma_\theta - \gamma_{\theta_T})}{2} \right)}{\sin \left(\frac{\gamma_\theta - \gamma_{\theta_T}}{2} \right)} \right) \cos \psi \\ \frac{\sqrt{E_s}}{N} \left(\frac{\sin \left(\frac{N(\gamma_\theta - \gamma_{\theta_T})}{2} \right)}{\sin \left(\frac{\gamma_\theta - \gamma_{\theta_T}}{2} \right)} \right) \sin \psi \end{bmatrix}.
\end{aligned} \tag{26}$$

From (25), we see that the mean of $\tilde{F}(\theta)$ is a function of the transmit symbol $\sqrt{E_s} e^{j\psi}$ for any observation angle and decays to zero in an oscillatory manner as we move away from the target.

To derive the covariance matrix of $\tilde{\mathbf{f}}(\theta)$ we decompose $\tilde{F}(\theta)$ into its real and imaginary parts. The real part of $\tilde{F}(\theta)$ can be expressed as

$$\begin{aligned}\tilde{\mathbf{f}}_1(\theta) &\triangleq \Re[\tilde{F}(\theta)] = \frac{\tilde{F}(\theta) + \tilde{F}^*(\theta)}{2} \\ &= \frac{1}{2} \sum_{n=0}^{N-1} \left(X_n e^{j(n - \frac{N-1}{2})\gamma_\theta} + X_n^* e^{-j(n - \frac{N-1}{2})\gamma_\theta} \right) \\ &= \frac{1}{2} \sum_{n=0}^{N-1} \left(Y_n Z_n e^{j(n - \frac{N-1}{2})\gamma_\theta} + Y_n^* Z_n^* e^{-j(n - \frac{N-1}{2})\gamma_\theta} \right).\end{aligned}\quad (27)$$

Noting that Z_n is real, Y_n is deterministic and using (19) in (27), we have

$$\begin{aligned}\tilde{\mathbf{f}}_1(\theta) &= \frac{1}{2} \sum_{n=0}^{N-1} \alpha Z_n \left(e^{j(\psi + (n - \frac{N-1}{2})(\gamma_\theta - \gamma_{\theta_T}))} + e^{-j(\psi + (n - \frac{N-1}{2})(\gamma_\theta - \gamma_{\theta_T}))} \right) \\ &= \sum_{n=0}^{N-1} \alpha Z_n \cos \left(\psi + \left(n - \frac{N-1}{2} \right) (\gamma_\theta - \gamma_{\theta_T}) \right).\end{aligned}\quad (28)$$

Similarly, we can express the imaginary part of $\tilde{F}(\theta)$ as

$$\tilde{\mathbf{f}}_2(\theta) \triangleq \Im[\tilde{F}(\theta)] = \sum_{n=0}^{N-1} \alpha Z_n \sin \left(\psi + \left(n - \frac{N-1}{2} \right) (\gamma_\theta - \gamma_{\theta_T}) \right).\quad (29)$$

We first find $[\tilde{\mathbf{P}}(\theta)]_{1,1}$ - the variance of the real component of the received symbol under our stochastic model. From (28), we see that the variance of the $\Re[\tilde{F}(\theta)]$ is simply the variance of a weighted sum of N independent Bernoulli random variables and is given by

$$\begin{aligned}[\tilde{\mathbf{P}}(\theta)]_{1,1} &\triangleq \text{var}[\tilde{\mathbf{f}}_1(\theta)] = \text{var} \left[\sum_{n=0}^{N-1} \alpha Z_n \cos \left(\psi + \left(n - \frac{N-1}{2} \right) (\gamma_\theta - \gamma_{\theta_T}) \right) \right] \\ &= \alpha^2 \sum_{n=0}^{N-1} \text{var}[Z_n] \cos^2 \left(\psi + \left(n - \frac{N-1}{2} \right) (\gamma_\theta - \gamma_{\theta_T}) \right) \\ &= \frac{E_s}{NM} \left(1 - \frac{M}{N} \right) \sum_{n=0}^{N-1} \cos^2 \left(\psi + \left(n - \frac{N-1}{2} \right) (\gamma_\theta - \gamma_{\theta_T}) \right)\end{aligned}\quad (30)$$

where we have substituted for α from (14) and used the fact that $Z_n \sim \text{Bern}(\frac{M}{N})$. Using trigonometric identities we can simplify the summation in (30) as

$$\sum_{n=0}^{N-1} \cos^2 \left(\psi + \left(n - \frac{N-1}{2} \right) (\gamma_\theta - \gamma_{\theta_T}) \right) = \frac{1}{2} \left(N + \cos(2\psi) \frac{\sin(N(\gamma_\theta - \gamma_{\theta_T}))}{\sin(\gamma_\theta - \gamma_{\theta_T})} \right).\quad (31)$$

Thus, the variance of the real component of the received symbol is

$$[\tilde{\mathbf{P}}(\theta)]_{1,1} = \frac{E_s}{2NM} \left(1 - \frac{M}{N} \right) \left(N + \cos(2\psi) \frac{\sin(N(\gamma_\theta - \gamma_{\theta_T}))}{\sin(\gamma_\theta - \gamma_{\theta_T})} \right).\quad (32)$$

A similar analysis on the imaginary component of the received symbol (29) yields

$$[\tilde{\mathbf{P}}(\theta)]_{2,2} = \frac{E_s}{2NM} \left(1 - \frac{M}{N}\right) \left(N - \cos(2\psi) \frac{\sin(N(\gamma_\theta - \gamma_{\theta_T}))}{\sin(\gamma_\theta - \gamma_{\theta_T})}\right). \quad (33)$$

It is important to note that the variance of the real and imaginary components of $\tilde{F}(\theta)$ exhibit oscillatory behavior and depend on the transmitted symbol like the mean. However, the total variance $\tilde{P}(\theta)$ is a constant (independent of the observation angle θ) for a given array configuration. Using (32) and (33),

$$\begin{aligned} \tilde{P}(\theta) &\triangleq \text{var}[\tilde{F}(\theta)] = [\tilde{\mathbf{P}}(\theta)]_{1,1} + [\tilde{\mathbf{P}}(\theta)]_{2,2} \\ &= \frac{E_s}{M} \left(1 - \frac{M}{N}\right). \end{aligned} \quad (34)$$

There are some interesting observations that can be made from (32), (33), and (34). First, when $M = N$ the thinned array degenerates to a uniform array and there is no randomness in the received symbol in any direction. This is indicated by the individual variances of the I and Q components going zero for all transmit angles θ . Second, for a fixed M , adding more antennas to the array (thereby reducing the thinning ratio $\frac{M}{N}$) increases the total variance. An increase in the variance of the received symbol in undesired directions is helpful because it increases randomness in the constellation and thereby provides more security. Also, increasing the total number of antenna elements in the array increases the effective aperture size which enables the randomly synthesized thinned array to have a reduced main lobe width compared to a uniform array with M elements. This leads to a narrow information beam-width towards the target receiver which is desirable.

Next, we compute the covariance between the real and imaginary components of the received symbol as a function of direction using our statistical model. The covariance between $\tilde{\mathbf{f}}_1(\theta)$ and $\tilde{\mathbf{f}}_2(\theta)$ is defined as

$$\begin{aligned} [\tilde{\mathbf{P}}(\theta)]_{1,2} &= [\tilde{\mathbf{P}}(\theta)]_{2,1} \triangleq \mathbb{E}[\tilde{\mathbf{f}}_1(\theta)\tilde{\mathbf{f}}_2(\theta)] - \mathbb{E}[\tilde{\mathbf{f}}_1(\theta)]\mathbb{E}[\tilde{\mathbf{f}}_2(\theta)] \\ &= \mathbb{E}[\tilde{\mathbf{f}}_1(\theta)\tilde{\mathbf{f}}_2(\theta)] - \tilde{\boldsymbol{\mu}}_1(\theta)\tilde{\boldsymbol{\mu}}_2(\theta). \end{aligned} \quad (35)$$

Using (28) and (29), we can express the first term in (35) as

$$\begin{aligned} \mathbb{E}[\tilde{\mathbf{f}}_1(\theta)\tilde{\mathbf{f}}_2(\theta)] &= \mathbb{E} \left[\sum_{m,n=0}^{N-1} \alpha^2 Z_m Z_n \cos \left(\psi + \left(m - \frac{N-1}{2} \right) (\gamma_\theta - \gamma_{\theta_T}) \right) \sin \left(\psi + \left(n - \frac{N-1}{2} \right) (\gamma_\theta - \gamma_{\theta_T}) \right) \right] \\ &= \alpha^2 \left\{ \sum_{n=0}^{N-1} \mathbb{E}[Z_n^2] \cos \left(\psi + \left(n - \frac{N-1}{2} \right) (\gamma_\theta - \gamma_{\theta_T}) \right) \sin \left(\psi + \left(n - \frac{N-1}{2} \right) (\gamma_\theta - \gamma_{\theta_T}) \right) \right. \\ &\quad \left. + \sum_{\substack{m,n=0 \\ m \neq n}}^{N-1} \mathbb{E}[Z_m Z_n] \cos \left(\psi + \left(m - \frac{N-1}{2} \right) (\gamma_\theta - \gamma_{\theta_T}) \right) \sin \left(\psi + \left(n - \frac{N-1}{2} \right) (\gamma_\theta - \gamma_{\theta_T}) \right) \right\}. \end{aligned} \quad (36)$$

Since $Z_m \perp Z_n, \forall m \neq n$, $\mathbb{E}[Z_m Z_n] = \mathbb{E}[Z_m] \mathbb{E}[Z_n] = \left(\frac{M}{N}\right)^2$, equation (36) becomes

$$\begin{aligned} \mathbb{E}[\tilde{\mathbf{f}}_1(\theta) \tilde{\mathbf{f}}_2(\theta)] &= \frac{\alpha^2 M}{N} \left\{ \sum_{n=0}^{N-1} \cos \left(\psi + \left(n - \frac{N-1}{2} \right) (\gamma_\theta - \gamma_{\theta_T}) \right) \sin \left(\psi + \left(n - \frac{N-1}{2} \right) (\gamma_\theta - \gamma_{\theta_T}) \right) \right\} \\ &\quad + \frac{\alpha^2 M^2}{N^2} \left\{ \sum_{\substack{m,n=0 \\ m \neq n}}^{N-1} \cos \left(\psi + \left(m - \frac{N-1}{2} \right) (\gamma_\theta - \gamma_{\theta_T}) \right) \sin \left(\psi + \left(n - \frac{N-1}{2} \right) (\gamma_\theta - \gamma_{\theta_T}) \right) \right\}. \end{aligned} \quad (37)$$

Again, using trigonometric identities we can simplify the two parenthetical expressions in (37) as follows:

$$\begin{aligned} \sum_{n=0}^{N-1} \cos \left(\psi + \left(n - \frac{N-1}{2} \right) (\gamma_\theta - \gamma_{\theta_T}) \right) \sin \left(\psi + \left(n - \frac{N-1}{2} \right) (\gamma_\theta - \gamma_{\theta_T}) \right) \\ = \frac{1}{2} \frac{\sin(N(\gamma_\theta - \gamma_{\theta_T}))}{\sin(\gamma_\theta - \gamma_{\theta_T})} \sin(2\psi), \end{aligned} \quad (38)$$

$$\begin{aligned} \sum_{\substack{m,n=0 \\ m \neq n}}^{N-1} \cos \left(\psi + \left(m - \frac{N-1}{2} \right) (\gamma_\theta - \gamma_{\theta_T}) \right) \sin \left(\psi + \left(n - \frac{N-1}{2} \right) (\gamma_\theta - \gamma_{\theta_T}) \right) \\ = \frac{\sin \left(\frac{N(\gamma_\theta - \gamma_{\theta_T})}{2} \right)}{\sin \left(\frac{\gamma_\theta - \gamma_{\theta_T}}{2} \right)} \frac{\sin \left(\frac{(N-1)(\gamma_\theta - \gamma_{\theta_T})}{2} \right)}{\sin(\gamma_\theta - \gamma_{\theta_T})} \sin(2\psi). \end{aligned} \quad (39)$$

Substituting for α from (14) and using (38), (39) in (37) we have

$$\begin{aligned} \mathbb{E}[\tilde{\mathbf{f}}_1(\theta) \tilde{\mathbf{f}}_2(\theta)] &= \frac{E_s}{2MN} \frac{\sin(N(\gamma_\theta - \gamma_{\theta_T}))}{\sin(\gamma_\theta - \gamma_{\theta_T})} \sin(2\psi) \\ &\quad + \frac{E_s}{N^2} \frac{\sin \left(\frac{N(\gamma_\theta - \gamma_{\theta_T})}{2} \right)}{\sin \left(\frac{\gamma_\theta - \gamma_{\theta_T}}{2} \right)} \frac{\sin \left(\frac{(N-1)(\gamma_\theta - \gamma_{\theta_T})}{2} \right)}{\sin(\gamma_\theta - \gamma_{\theta_T})} \sin(2\psi). \end{aligned} \quad (40)$$

Using (26), the product of the means is

$$\tilde{\mu}_1(\theta) \tilde{\mu}_2(\theta) = \frac{E_s}{2N^2} \left(\frac{\sin \left(\frac{N(\gamma_\theta - \gamma_{\theta_T})}{2} \right)}{\sin \left(\frac{\gamma_\theta - \gamma_{\theta_T}}{2} \right)} \right)^2 \sin(2\psi). \quad (41)$$

Finally, substituting equations (40) and (41) in (35), we arrive at the expression for the covariance between the real and imaginary parts as

$$[\tilde{\mathbf{P}}(\theta)]_{1,2} = [\tilde{\mathbf{P}}(\theta)]_{2,1} = \frac{E_s}{2MN} \left(1 - \frac{M}{N} \right) \frac{\sin(N(\gamma_\theta - \gamma_{\theta_T}))}{\sin(\gamma_\theta - \gamma_{\theta_T})} \sin(2\psi). \quad (42)$$

Thus, from (42) we see that the artificial randomness introduced in the real and imaginary components of the received symbol along undesired transmit directions may be correlated depending on the transmit symbol and observation angle. However, the magnitude of the correlation is usually small (< 0.1) in most directions.

Equations (26), (32), (33), and (42), are the parameters of the Gaussian approximation to the received symbol distribution in undesired transmission directions in the absence of noise. The situation where we have zero-mean AWGN at the receiver is easy to incorporate as it modifies only the covariance $\tilde{\mathbf{P}}(\theta)$. If N_0 denotes the total noise variance, the mean and covariance of the received symbol in undesired directions is given by

$$\tilde{\boldsymbol{\mu}}_{\text{N}}(\theta) = \tilde{\boldsymbol{\mu}}(\theta), \quad (43)$$

$$\tilde{\mathbf{P}}_{\text{N}}(\theta) = \tilde{\mathbf{P}}(\theta) + \frac{N_0}{2} \mathbf{I}_2. \quad (44)$$

It is worth noting that the Gaussian approximation statistics derived to model the received symbol distribution is accurate only in the angular region outside the target cone i.e., when $\theta \in \Omega$.

C. Secure Communication Link

Equipped with the necessary statistics of the Gaussian approximation to the received symbol, we now analyze the error rates provided by ASM under RASS. For computing the average SER, we first consider the case when there is no receiver noise and assume optimal maximum-likelihood (ML) detection by the eavesdropper. Analyzing the average SER in a noiseless setting is important because it helps quantify the level of security inherent to the modulation technique. Also note that, conventional array transmission cannot guarantee any security benefits in this scenario because an eavesdropper with a sufficiently sensitive receiver can still potentially demodulate information.

The method for computing the average SER achieved by RASS, is similar to the one used for deriving the error rates for conventional digital modulation schemes [24]. The only difference here is that the zero-mean AWGN model for receiver noise must now be replaced with a statistical model for the randomness introduced by antenna subset selection (discussed in the previous subsection). For a K -ary PSK modulation, the modulation symbols are represented by s_l for $l = 0, 1, \dots, K - 1$ as in (17). As discussed previously, the received symbol in undesired transmit directions can be approximated by a two-dimensional real Gaussian distribution. From the model statistics (equations (26), (32), (33), and (42)), we see that the parameters of the received distribution depend on the transmit symbol s_l unlike the zero-mean AWGN model assumption. To emphasize this dependence explicitly, we will use $\tilde{\boldsymbol{\mu}}_l(\theta)$ and $\tilde{\mathbf{P}}_l(\theta)$ to denote the mean and covariance of the received symbol respectively.

Under ML detection, a received symbol is declared to be in error if it falls outside the Voronoi region of the actual symbol transmitted along θ_{T} . Assuming each symbol is equally likely, the average SER

according to our statistical model for the received symbol distribution can be expressed as

$$P_s(\theta) = 1 - \frac{1}{M} \sum_{\ell=0}^{K-1} \int_{\Lambda_\ell} \frac{1}{2\pi |\tilde{\mathbf{P}}_\ell(\theta)|^{\frac{1}{2}}} \exp \left\{ -\frac{1}{2} (\mathbf{z} - \tilde{\boldsymbol{\mu}}_\ell(\theta))^T \tilde{\mathbf{P}}_\ell(\theta)^{-1} (\mathbf{z} - \tilde{\boldsymbol{\mu}}_\ell(\theta)) \right\} d\mathbf{z} \quad (45)$$

where Λ_ℓ is the Voronoi region associated with the modulation symbol s_ℓ and $\tilde{\mathbf{P}}_\ell(\theta) > 0$. When $K = 4$ i.e., for QPSK modulation, (45) can be simplified by using symmetry and invoking the fact that $\tilde{\mathbf{P}}_\ell(\theta)$ is diagonal. However, since there are no closed form expressions for (45) when $K > 4$, we have to perform a numerical integration to compute the average SER. Note that the above expression for SER represents the irreducible error rate achieved by RASS. The presence of noise only increases the average SER.

Fig. 8 shows the SER achieved using RASS when transmitting a QPSK constellation. We see that the statistical approximation using (45) is close to the average SER from simulations even for moderate values of N . For the case when there is zero-mean AWGN at the receiver, the average SER can be computed again using (45), but with the modified mean and covariance parameters from (43), (44).

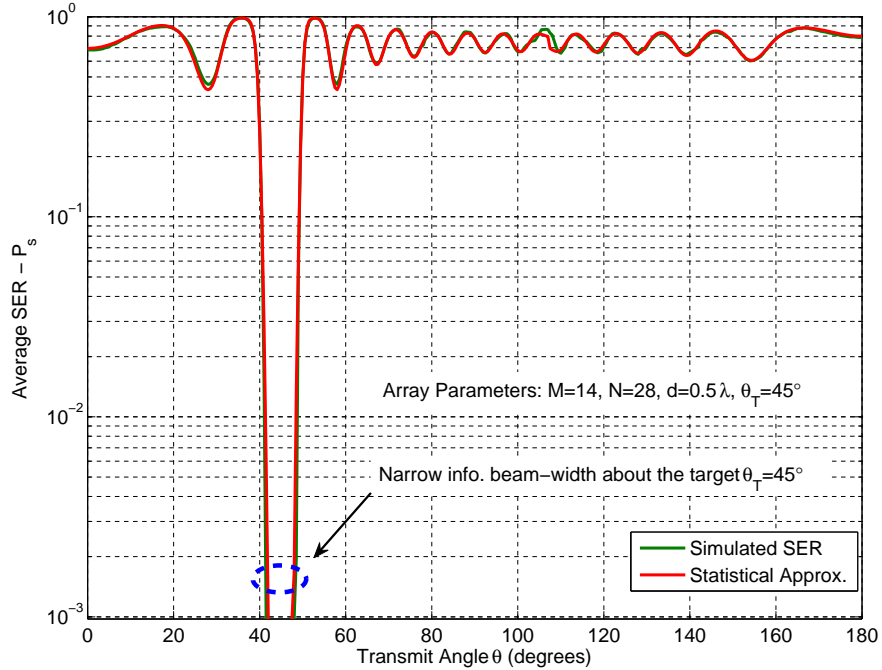


Fig. 8. Comparison of the average SER for RASS from simulation and the statistical approximation for a linear array steered to $\theta_T = 45^\circ$.

One can also quantify the degree of transmission security, in an information-theoretic sense, using the notion of secrecy capacity. The *secrecy capacity* of a channel is the maximum transmission rate at

which information can be communicated reliably and securely. In [25], it was shown that for a Gaussian wire-tap channel the secrecy capacity, denoted by C_S , is the difference between the capacity of the main and wire-tap channels. Adopting this definition, we calculate the secrecy capacity for both conventional array transmission and ASM. Since there is no closed form expression for the channel capacity (as a function of the received SNR) when using a finite-alphabet constellation, we have to numerically evaluate the channel capacity. Denoting the target and undesired receiver's capacity by C_T and C_U respectively, we have

$$C_S \triangleq C_T - C_U. \quad (46)$$

For the case of QPSK transmission considered in the previous example, the secrecy capacity as given by (46) is

$$C_S(\theta) = C_{\text{qpsk}}(\text{SNR}(\theta_T)) - C_{\text{qpsk}}(\text{SNR}(\theta)) \quad (47)$$

where $C_{\text{qpsk}}(\cdot)$ denotes the AWGN channel capacity when using QPSK signaling. Since the received SNR depends on the observation angle, C_S is a function of θ for a fixed transmit symbol energy.

We need to find the average received SNR for the two transmission schemes to calculate the secrecy capacity. For conventional array transmission, the signal power can be calculated simply using the far-field radiation pattern of a uniform linear array [22]. Using (4), the received SNR assuming rectangular pulse-shaping is

$$\text{SNR}(\theta) = \left(\frac{E_s}{2N_0} \right) \left(\frac{1}{M} \frac{\sin \left(\frac{M(\gamma_\theta - \gamma_{\theta_T})}{2} \right)}{\sin \left(\frac{\gamma_\theta - \gamma_{\theta_T}}{2} \right)} \right)^2. \quad (48)$$

Note that $\text{SNR}(\theta_T) = \frac{E_s}{2N_0}$, as expected.

For ASM transmission, the SNR at the target receiver's location is the same as that of conventional array transmission since the constellation is undistorted in this direction. To calculate the SNR along undesired transmit directions, we will make use of the Gaussian approximation to the received symbol distribution. Specifically, the square of the mean of the received symbol distribution ($\tilde{\mu}_N(\theta)$) from (43)) for every angle is a measure of the average symbol energy in that direction. The noise variance (in undesired directions) is composed of two components: 1) receiver thermal noise and, 2) artificial noise introduced by RASS. Since the artificial noise is uncorrelated with the receiver thermal noise, the effective noise covariance is the sum of individual covariances ($\tilde{\mathbf{P}}_N(\theta)$ from (44)).

For QPSK modulation, the noise introduced by ASM has zero-mean and uncorrelated real and imaginary components i.e., $[\tilde{\mathbf{P}}]_{1,2} = [\tilde{\mathbf{P}}]_{2,1} = 0$. Therefore, the effect of artificial noise can be modeled as complex zero-mean AWGN with modified variance parameter given by

$$\tilde{P}_N = 2N_0 + \frac{E_s}{M} \left(1 - \frac{M}{N}\right). \quad (49)$$

If $\tilde{\mu}_N$ denotes the mean of the received complex symbol, the average received SNR for ASM can be expressed as

$$\begin{aligned} \text{SNR}(\theta) &= \frac{|\tilde{\mu}_N|^2}{2N_0 + \frac{E_s}{M} \left(1 - \frac{M}{N}\right)} \\ &= \left(\frac{E_s}{2N_0 + \frac{E_s}{M} \left(1 - \frac{M}{N}\right)} \right) \left(\frac{1}{N} \frac{\sin\left(\frac{N(\gamma_\theta - \gamma_{\theta_T})}{2}\right)}{\sin\left(\frac{\gamma_\theta - \gamma_{\theta_T}}{2}\right)} \right)^2 \quad \forall \theta \in \Omega. \end{aligned} \quad (50)$$

A numerical example comparing secrecy capacity of ASM and conventional array transmission is presented in Section VI.

Thus, we see that using RASS in ASM synthesizes a constellation that is a function of direction. While the constellation for the intended receiver is not affected by the random choice of antenna subset, the undesired receiver sees an effectively random constellation because of mis-aligned signal addition. This enables ASM establish a secure communication link to the target receiver. In the next section, we propose an optimized antenna subset selection technique that offers better security and array performance.

V. OPTIMIZED ANTENNA SUBSET SELECTION

When randomized antenna subset selection technique is employed in ASM, every possible antenna subset (with a fixed number of active elements) is equally probable to be used. Though the spatially non-uniform arrays these subsets correspond to have a similar main lobe performance, the sidelobes behave very differently which is explained simply by virtue of the resulting active element array geometry. The large sidelobe levels produced by RASS may be a source of interference to other receivers which is not desirable. Therefore, we seek to create a codebook of antenna subsets that possess good sidelobe characteristics and choose an antenna subset at random only from this collection for each symbol transmission. Note that since the set of all antenna subsets are equivalent along the main lobe direction, restricting the set of possibilities to a smaller set does not affect our ability to communicate information to the desired receiver. In this section, we will develop an optimized antenna subset selection technique based on simulated annealing algorithm to achieve this goal.

A. Thinned Array Pattern Synthesis

The problem of synthesizing thinned arrays with some desirable characteristics such as low main lobe width, good sidelobe behavior, null-steering capability etc. is a combinatorial optimization problem and has been studied extensively in the past [26]–[34]. The effect of thinning on the array gain and main lobe width is predictable. However, it is hard to characterize the effect of thinning on peak sidelobe level performance because it depends on both the location and number of active elements. Unfortunately, there are no closed-form synthesis techniques to synthesize a thinned array with certain sidelobe behavior. For an array N -element array, the number of subsets with exactly $M(< N)$ active elements is

$$\binom{N}{M} = \frac{N!}{(N-M)!M!}. \quad (51)$$

Even for moderate values of N and M , the number of possible subsets can be large. For example, when $N = 64$ and $M = 32$, $\binom{N}{M} \sim 10^{18}$. Clearly, an exhaustive search over the entire space to find arrays with good sidelobe behavior is impractical. Therefore, heuristic optimization techniques based on simulated annealing, genetic algorithms and its variants have been proposed to find near-optimal solutions to the array thinning problem [26]–[34]. Since simulated annealing based methods have been reported [35] achieve best array performance compared to other techniques, we will use it to develop an efficient optimization algorithm for antenna subset selection.

B. Optimized Antenna Subset Selection using Simulated Annealing

Simulated annealing [36], [37] is a probabilistic iterative algorithm for finding good approximate solutions to the global optimum of a function in a large search space. It emulates the physical process of annealing whereby heating and controlled cooling of a substance results in a molecular configuration with lower internal energy compared to the initial state.

For optimized antenna subset selection, we seek to build a codebook \mathcal{B} consisting of antenna subsets that correspond to non-uniform arrays with lower peak sidelobe levels. The constraint on the optimization is that the number of active elements, M , in the thinned array is fixed. Since we have a large number of possible antenna subsets, we can hope to find a good collection that exhibit the desirable array characteristics. The simulated annealing algorithm as applied to the antenna subset selection problem is illustrated below using pseudo code.

Algorithm Simulated Annealing

```

1: procedure ANTENNA_SUBSET_SELECTION ( $M, N$ )
2:   Initialize( $\mathbf{b}_0, T_0, iter\_count$ )  $\triangleright \mathbf{b}_i$  is the thinning pattern rep. as a binary vector
3:   for  $i = 1$  to  $iter\_count$  do
4:      $T_i = \beta T_{i-1}$  ensure  $\beta < 1$   $\triangleright$  Exponential cooling schedule
5:      $\mathbf{b}^* = \text{swap}(\mathbf{b}_{i-1})$   $\triangleright$  Perturb  $\mathbf{b}_{i-1}$  by swapping the loc. of a 0 and 1 at random
6:      $\Delta E = E(\mathbf{b}^*) - E(\mathbf{b}_{i-1})$   $\triangleright$  Compute the change in cost  $\Delta E$ 
7:     if  $\Delta E < 0$  or  $\exp\left[-\frac{\Delta E}{T_i}\right] > \text{rand}[0, 1]^2$  then
8:        $\mathbf{b}_i = \mathbf{b}^*$   $\triangleright$  Probabilistically accept the new solution if  $\Delta E \geq 0$ 
9:     else
10:       $\mathbf{b}_i = \mathbf{b}_{i-1}$   $\triangleright$  Try another perturbation
11:    end if
12:  end for
13: end procedure

```

The simulated annealing algorithm retains only one array solution (and an associated temperature) at any instant. At the beginning, the algorithm is initialized with a random array configuration containing M active elements. Then, at every iteration we perturb the array solution from the previous iteration. By allowing perturbations that only swap the location of an “on” element for an “off” element we ensure that the number of active elements in the array is M at each iteration. If the perturbed solution results in lowering the cost function E we accept it and move to the next iteration. Otherwise, we probabilistically accept the perturbed solution and this acceptance probability decreases as the temperature goes down. The replacement of better solutions by worse ones at higher temperatures ensures that the algorithm does not get stuck in a local optimum. After a sufficient number of iterations the algorithm converges to a near-optimal solution that has a lower cost.

The performance of any simulated annealing algorithm depends heavily on the choice of cost function and cooling schedule used. In this work, an exponential cooling schedule is used since it produced the best results. The algorithm seeks to minimize a cost function which is the maximum magnitude squared of the sidelobe level in dB scale. Mathematically,

$$E \triangleq \max |\text{SLL}|_{dB}^2 = \max_{(\theta, \phi) \in \Omega} 20 \log_{10} |F(\theta, \phi)| \quad (52)$$

²rand[0,1] generates a number uniformly distributed on the interval[0,1].

where SLL abbreviates sidelobe level of the array, F is the far-field radiation pattern of the array, and Ω denotes the angular region outside the location of the first null. As long as the number of possible subsets is large, we can get a sufficient collection of array configurations with similar sidelobe properties after multiple runs of the algorithm. The random initialization and the probabilistic nature of the simulated annealing algorithm ensures that we do not converge to the same local optimum after each run. The arrays thus synthesized are stacked to form the codebook \mathcal{B} that the transmitter will use to pick antenna subsets for each transmission.

Reducing the peak sidelobe level not only leads to better array performance compared to RASS but can also benefit us in terms of transmission security. While the magnitude of the received symbols in undesired directions (which is equal to the sidelobe level of the array's radiation pattern) is now lower, the randomization in phase caused by antenna subset selection is still maintained by using a large enough codebook. Therefore, the resulting symbol distribution in undesired directions has a mean closer to zero and hence is more susceptible to symbol errors.

It is important to observe that for a given array configuration, the codebook is constructed only once and is *independent of the target direction* i.e., the antenna subset to be used is chosen at random from the same codebook irrespective of the desired receiver's orientation. This keeps the antenna subset selection procedure in ASM simple. It is also possible to construct a similar codebook of antenna subsets that have other desirable properties such as null-steering towards an interferer or jammer, sidelobe cancellation etc. by appropriately modifying the cost function (52). The next section presents simulation results illustrating the better SER and sidelobe performance offered by optimized antenna subset selection in ASM.

VI. SIMULATION RESULTS

In this section, we present and discuss some numerical examples illustrating constellation synthesis, array performance and transmission security of ASM. Linear antenna arrays with omnidirectional elements were considered for the study. The parameters of the array for each simulation study are overlaid on the corresponding plots.

A. Constellation Synthesis Results

First, we show the constellation synthesized by ASM when using the proposed antenna subset selection techniques (discussed in Sections IV and V) to transmit a QPSK modulated signal. As is evident from Fig. 9, the constellation produced by ASM along the target direction is exact. However along an undesired transmit direction, the received symbols appear to be randomly distributed. Notice that the received

symbol cluster has a lower magnitude when using optimized antenna subset selection compared to RASS. This is a consequence of choosing only antenna subsets that have reduced sidelobe level from a carefully constructed codebook. Also shown in Fig. 9 is the constellation produced by conventional array transmission in these directions. Although the magnitude of the received symbol produced by a conventional array is lower compared to ASM, the constellation is still separated enough for a sensitive receiver to demodulate information.

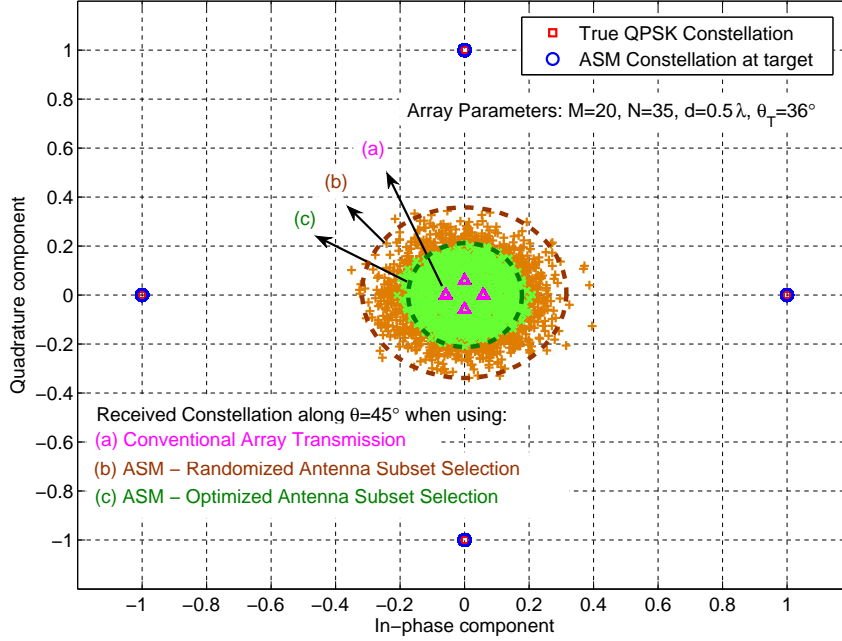


Fig. 9. Comparison of the constellation produced by ASM and conventional array along intended and undesired directions.

B. Array Performance Results

Here we compare the array performance of the two antenna subset selection techniques. Fig. 10 depicts the magnitude squared radiation pattern of a randomly thinned array and an array synthesized using simulated annealing algorithm discussed in the previous section. The optimized array exhibits a lower peak sidelobe level as expected. The reduction in sidelobe level comes with a small increase in the main-lobe width which can be observed from Fig. 10. However, both arrays possess a narrower main-lobe width compared to a conventional array (with the same number of active elements) even when the array is steered away from broadside.

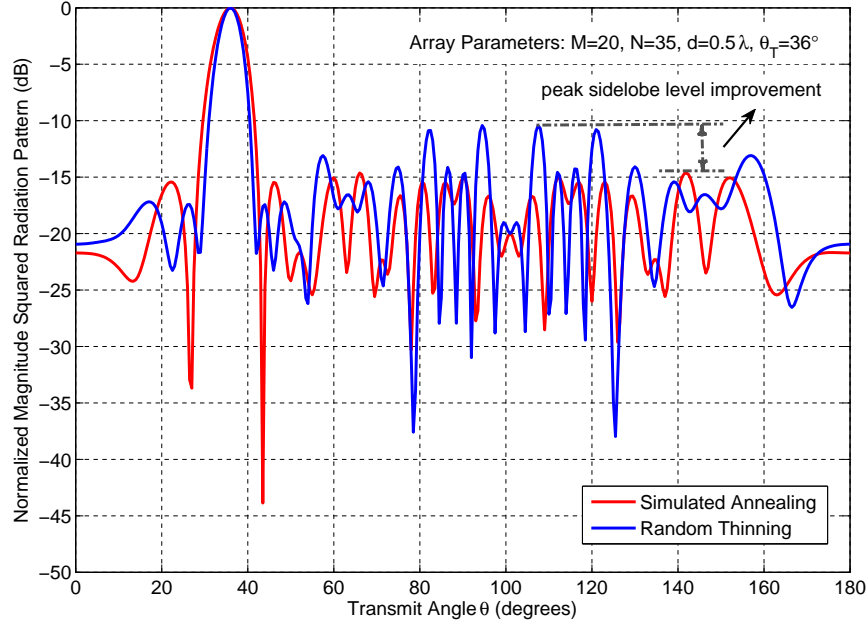


Fig. 10. Far-field radiation pattern for arrays synthesized by the proposed antenna subset selection techniques. The peak sidelobe level of the randomly thinned array and algorithmically optimized array shown are -10.4 dB and -14.7 dB respectively.

A histogram of the resulting peak sidelobe levels while using the two antenna subset selection techniques is shown in Fig. 11. Note that the sidelobe behavior of the optimized array is better compared to a conventional array which has a fixed peak sidelobe level ≈ -13.5 dB when steered to broadside [22].

C. Transmission Security Results

In this section, we demonstrate using simulation examples that ASM can achieve a low SER in a narrow beam-width around the target angle, while enforcing a high SER in undesired directions. The simulation setup is as follows. Consider a standard linear array with $N = 35$ antenna elements of which only $M = 20$ are active at any time. The array is beamformed to the target along $\theta_T = 36^\circ$. First, the simulated annealing algorithm was run to construct a codebook of thinned arrays that are optimized for minimum sidelobe level. In this example, the size of the codebook was chosen to be 500. Note that the codebook size need not be very large. Randomly selecting from a collection of a few hundred of optimized antenna subsets is sufficient to create a complete randomization in both amplitude and phase of the received symbol along undesired directions. For the simulation study, approximately 10^7 QPSK-modulated symbols were transmitted for each angle (in 0.5° increments). During symbol transmission, one among the 500 antenna subsets was selected at random and used. Zero-mean AWGN was added to the received symbol in all directions and the symbol error rates were calculated assuming ML decoding

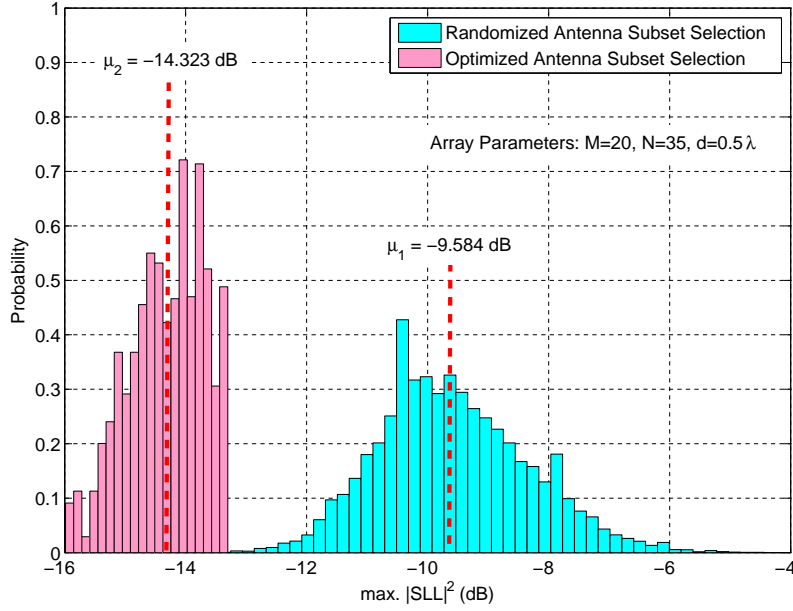


Fig. 11. Empirical histogram of the peak sidelobe level for the two proposed antenna subset selection techniques in ASM.

at the receiver. A similar simulation methodology was adopted to compute the average SER of ASM under randomized antenna subset selection technique. But, this time the antenna subsets were selected independently at random from $\binom{35}{20} \sim 10^9$ possible array configurations. Fig. 12 illustrates the SER performance of ASM under the two subset selection techniques.

To compare the SER performance of ASM with conventional array transmission we consider a uniform linear array with the same number of active elements. The main response axis of the array is steered towards the target and employs traditional baseband modulation. Since a conventional array transmits the same constellation in all directions, the average SER can be calculated by using the symbol error probability expression for the modulation scheme employed. The exact symbol error probability for QPSK signaling considered in this example, and in general for K -ary PSK, in a zero-mean AWGN channel can be computed using [38]

$$P_s(\theta) = F\left(1, \sqrt{\frac{2E_s}{N_0}}, \cot \frac{\pi}{K}\right) \quad (53)$$

where F is the cumulative distribution function of the non-central t -distribution and E_s is the received symbol energy which is equal to the squared magnitude of the far-field radiation pattern of the array. The average SER for conventional array transmission is thus computed using (53) and is shown in Fig. 12. It is confirmed that ASM under both antenna subset selection techniques achieves a higher SER compared to conventional array transmission in unwanted directions. Moreover, it produces a narrow

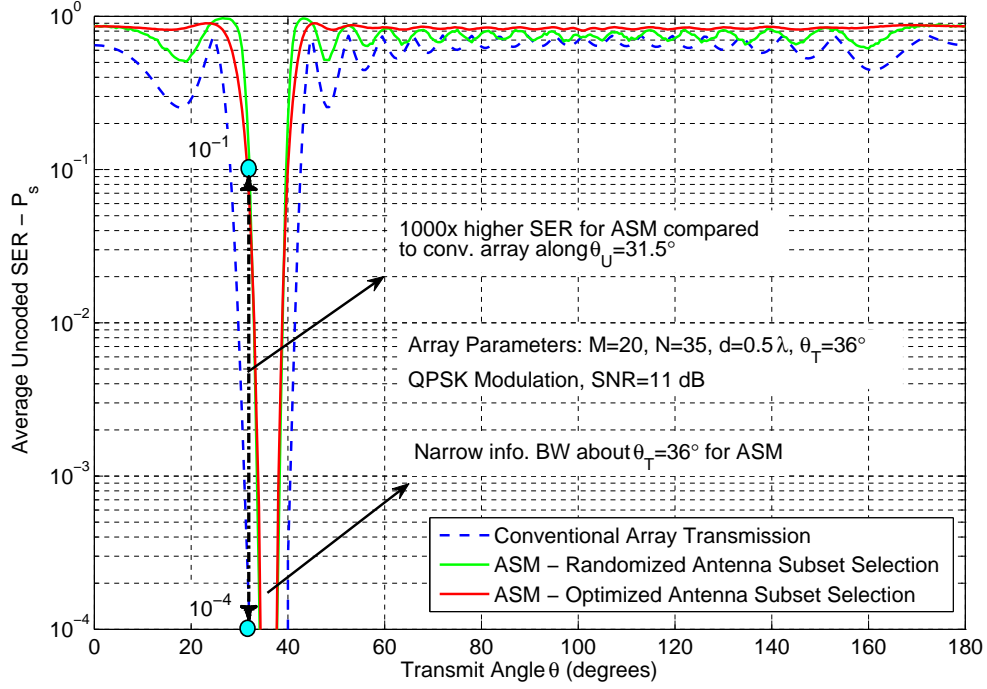


Fig. 12. Comparison of the average SER between ASM and conventional array transmission for a linear array steered towards $\theta_T = 36^\circ$.

information beam-width around the target angle and the error rates rise steeply to a higher value outside this narrow region. One can also see that optimized antenna subset selection has better a transmission security compared to randomized antenna subset selection. This can be explained by the fact that the former technique synthesized modulation symbols whose mean was closer to zero, thus making it more difficult to distinguish the actual transmitted symbol in undesirable directions. It is worth noting that ASM achieves the aforementioned security benefits with no additional transmit power requirement unlike other DM techniques [14], [15] which trade-off security for a small increase in transmission power.

Next, we present simulation results on the average SER performance versus SNR of ASM for an eavesdropper and compare it against conventional array transmission in Fig 13. For this simulation experiment, a 12-element array with 9 active elements was considered and RASS was employed in ASM. When the target receiver was located along $\theta_T = 45^\circ$, two angular locations were considered for the eavesdropper: Scenario (a) $\theta_a = \theta_T + 10^\circ = 55^\circ$, and Scenario (b) $\theta_b = \theta_T + 122^\circ = 167^\circ$. Scenario (a) depicts the situation where the angular location of the eavesdropper is close to the target while scenario (b) is when the eavesdropper is far away from the target angle. In both situations, ASM under randomized antenna subset selection is shown to outperform conventional array transmission. Even as the SNR increases, ASM maintains a high SER while for a conventional array the average error rate

falls off exponentially with SNR.

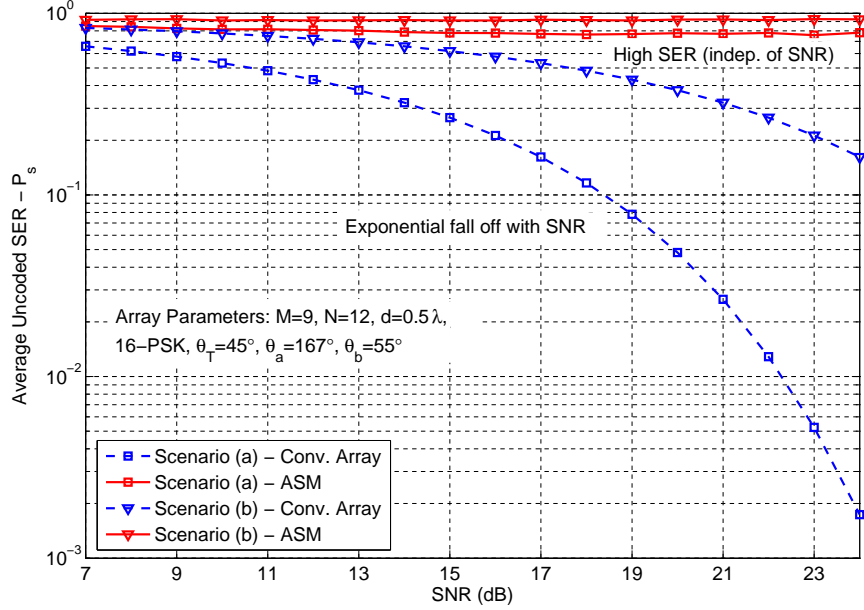


Fig. 13. Average SER versus SNR for an eavesdropper when using ASM and conventional array transmission for two scenarios when $\theta_T = 45^\circ$. Scenario (a) Eavesdropper is close to the target angle - along $\theta_a = 55^\circ$. Scenario (b) - Eavesdropper is far off the target angle - along $\theta_b = 167^\circ$.

Finally, we show the improved secrecy capacity performance of ASM in Fig. 14. Equations (47), (48) and (50) were used to evaluate the secrecy capacity of conventional array transmission and ASM under QPSK modulation. As shown in Fig 14, ASM achieves better secrecy capacity compared to conventional array transmission which has multiple transmit angles where the secrecy capacity is low. Another desirable characteristic of ASM which is evident from the plot is the ability to create a communication link with secrecy capacity close to the actual capacity without eavesdropping (in this case, 2 bits/s/Hz) over a wide range of angles. Moreover, the secrecy capacity of ASM is non-zero even as $\text{SNR} \rightarrow \infty$ because of the irreducible artificial noise inherent to the transmission technique.

VII. CONCLUSION

In this paper, Antenna Subset Modulation (ASM) was proposed to take advantage of massive antenna arrays at mm-Wave frequencies. In ASM, the far-field pattern of the array was modulated at the symbol rate to achieve direction-dependent data transmission. Unlike other directional modulation techniques that scramble the desired constellation in unwanted directions, ASM has been shown to provide security by

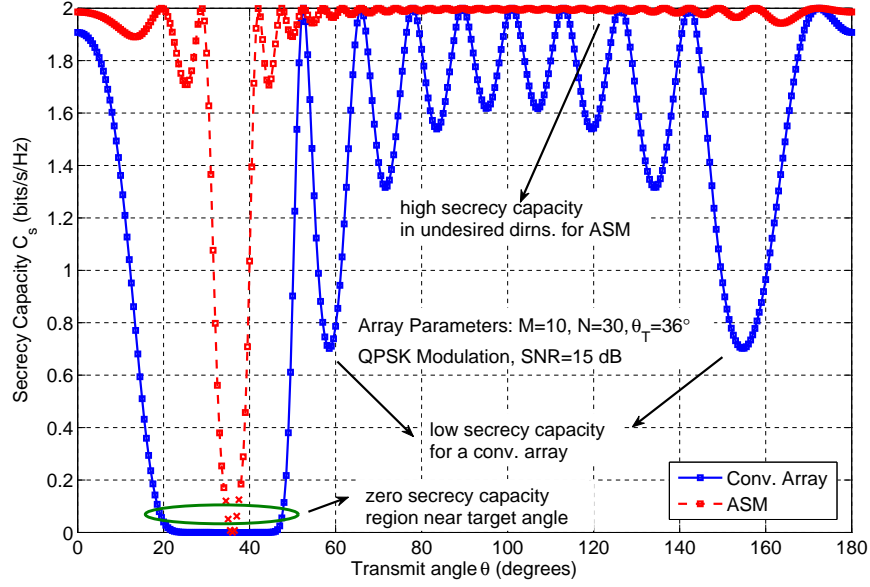


Fig. 14. Secrecy capacity performance for different eavesdropper locations when using ASM and conventional array transmission. The red crosses are the interpolated values of the secrecy capacity of ASM for θ near the target angle θ_T .

introducing additional points in the constellation that appear effectively random to an undesired receiver. A simple constellation design procedure involving the calculation of progressive inter-element phase shifts was described. Two different antenna subset selection techniques were proposed for implementing ASM: (i) Random antenna subset selection, and (ii) Optimized antenna subset selection. In the first technique, the antenna subset to be used for transmission was selected independently at random. A statistical model that closely approximates this subset selection technique was discussed. To overcome the problem of large peak sidelobe level associated with random antenna subset selection, an optimized antenna subset selection technique was then proposed based on simulated annealing algorithm. Finally, simulation examples were used to compare and validate the security benefits of ASM against conventional array transmission. It was concluded that ASM achieves a narrow information beam-width in the desired direction and a high SER in undesired directions under both subset selection techniques. The optimized antenna subset selection was found to improve the array performance and provided the best security benefits.

Future work will involve an extension of the analysis and results presented to multidimensional periodic arrays followed by a demonstration of the proposed approach. Including the synthesis of non-constant envelope-modulated signals in ASM is one possibility. This can be accomplished by choosing antenna subsets with a variable number of active elements to control the amplitude or by employing non-uniform amplitude tapering. Incorporating multi-directional data transmission in ASM using array partitioning techniques is also an interesting research problem that merits further study.

REFERENCES

- [1] P. Xia, X. Qin, H. Niu, H. Singh, H. Shao, J. Oh, C. Y. Kweon, S. S. Kim, S. K. Yong, and C. Ngo, "Short range gigabit wireless communications systems: Potentials, challenges and techniques," in *Proc., IEEE Intl. Conf. Ultra-Wideband (ICUWB)*, pp. 123 –128, Sept. 2007.
- [2] R. Daniels and R. Heath, "60 GHz wireless communications: emerging requirements and design recommendations," *IEEE Veh. Technol. Mag.*, vol. 2, pp. 41 –50, Sept. 2007.
- [3] "IEEE standard for information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements. Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPANs) Amendment 2: Millimeter-wave-based Alternative Physical Layer Extension," *IEEE Std 802.15.3c-2009 (Amendment to IEEE Std 802.15.3-2003)*, pp. c1 –187, Dec. 2009.
- [4] ECMA International, "High rate 60 GHz PHY, MAC and HDMI PAL," *ECMA-387*, Dec. 2008.
- [5] "WirelessHD Specification Overview," *WirelessHD Std. Overview*, Aug. 2009.
- [6] E. Perahia, C. Cordeiro, M. Park, and L. Yang, "IEEE 802.11ad: Defining the Next Generation Multi-Gbps Wi-Fi," in *Proc., IEEE Consum. Commun. Netw. Conf. (CCNC)*, pp. 1 –5, Jan. 2010.
- [7] "WiGig White Paper: Defining the Future of Multi-Gigabit Wireless Communications," July 2010.
- [8] Z. Pi and F. Khan, "An introduction to millimeter-wave mobile broadband systems," *IEEE Commun. Mag.*, vol. 49, pp. 101 –107, June 2011.
- [9] C. Doan, S. Emami, D. Sobel, A. Niknejad, and R. Brodersen, "Design considerations for 60 GHz CMOS radios," *IEEE Commun. Mag.*, vol. 42, pp. 132 – 140, Dec. 2004.
- [10] D. Cabric, M. S. W. Chen, D. A. Sobel, S. Wang, J. Yang, and R. W. Brodersen, "Novel radio architectures for UWB, 60 GHz, and cognitive wireless systems," *EURASIP J. Wireless Commun. Netw.*, vol. 2006, pp. 1–18, Jan. 2006.
- [11] J. Wells, "Faster than fiber: The future of multi-G/s wireless," *IEEE Microw. Mag.*, vol. 10, pp. 104 –112, May 2009.
- [12] A. Babakhani, D. Rutledge, and A. Hajimiri, "Transmitter architectures based on near-field direct antenna modulation," *IEEE J. Solid-State Circuits*, vol. 43, pp. 2674 –2692, Dec. 2008.
- [13] A. Babakhani, D. Rutledge, and A. Hajimiri, "A near-field modulation technique using antenna reflector switching," in *Proc., IEEE Intl. Solid-State Circuits Conf. (ISSCC)*, pp. 188 –605, Feb. 2008.
- [14] M. Daly and J. Bernhard, "Directional modulation technique for phased arrays," *IEEE Trans. Antennas Propag.*, vol. 57, pp. 2633 –2640, Sept. 2009.
- [15] M. Daly and J. Bernhard, "Directional modulation and coding in arrays," in *Proc., IEEE Intl. Symposium on Antennas and Propag. (APSURSI)*, pp. 1984 –1987, July 2011.
- [16] M. Daly, E. Daly, and J. Bernhard, "Demonstration of directional modulation using a phased array," *IEEE Trans. Antennas Propag.*, vol. 58, pp. 1545 –1550, May 2010.
- [17] M. Daly and J. Bernhard, "Beamsteering in pattern reconfigurable arrays using directional modulation," *IEEE Trans. Antennas Propag.*, vol. 58, pp. 2259 –2265, July 2010.
- [18] E. Baghdady, "Directional signal modulation by means of switched spaced antennas," *IEEE Trans. Commun.*, vol. 38, pp. 399 –403, Apr. 1990.
- [19] 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, 2011.

- [20] T. Hong, M.-Z. Song, and Y. Liu, "RF directional modulation technique using a switched antenna array for physical layer secure communication applications," *Progress In Electromagnetics Research (PIER)*, vol. 116, pp. 363–379, 2011.
- [21] P. F. M. Smulders, "Deterministic modelling of indoor radio propagation at 40-60 GHz," *Wireless Personal Communications*, vol. 1, pp. 127–135, 1994. 10.1007/BF01098690.
- [22] H. L. Van Trees, *Optimum Array Processing (Detection, Estimation, and Modulation Theory, Part IV)*. Wiley-Interscience, 1 ed., Mar. 2002.
- [23] J. Lavaei, A. Babakhani, A. Hajimiri, and J. Doyle, "A study of near-field direct antenna modulation systems using convex optimization," in *Proc., American Control Conf. (ACC)*, pp. 1065–1072, July 2010.
- [24] A. Goldsmith, *Wireless Communications*. New York, NY, USA: Cambridge University Press, 2005.
- [25] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Info. Theory*, vol. 24, pp. 451–456, July 1978.
- [26] R. Haupt, "Thinned arrays using genetic algorithms," *IEEE Trans. Antennas Propag.*, vol. 42, pp. 993–999, July 1994.
- [27] M. T. Ali, R. Abdolee, and T. A. Rahman, "Decimal genetics algorithms for null steering and sidelobe cancellation in switch beam smart antenna system," *Intl. J. of Comput. Sci. and Security*, vol. 1, pp. 19–26, Oct. 2007.
- [28] M. Skolnik, G. Nemhauser, and I. Sherman, J., "Dynamic programming applied to unequally spaced arrays," *IEEE Trans. Antennas Propag.*, vol. 12, pp. 35–43, Jan. 1964.
- [29] R. Arora and N. Krisnamacharyulu, "Synthesis of unequally spaced arrays using dynamic programming," *IEEE Trans. Antennas Propag.*, vol. 16, pp. 593–595, Sept. 1968.
- [30] V. Murino, A. Trucco, and C. Regazzoni, "Synthesis of unequally spaced arrays by simulated annealing," *IEEE Trans. Signal Process.*, vol. 44, pp. 119–122, Jan. 1996.
- [31] C. Meijer, "Simulated annealing in the design of thinned arrays having low sidelobe levels," in *Proc., South African Symposium on Commun. Signal Process. (COMSIG)*, pp. 361–366, Sept. 1998.
- [32] J.-F. Hopperstad, "Optimization of thinned arrays," Master's thesis, Department of Informatics, University of Oslo, May 1998.
- [33] J.-F. Hopperstad and S. Holm, "Optimization of sparse arrays by an improved simulated annealing algorithm," *Proc., Intl. Workshop on Sampling Theory and Appl.*, pp. 91–95, Aug. 1999.
- [34] L. Zhang, Y.-C. Jiao, Z.-B. Weng, and F.-S. Zhang, "Design of planar thinned arrays using a Boolean differential evolution algorithm," *IET Microw., Antennas Propag.*, vol. 4, pp. 2172–2178, Dec. 2010.
- [35] S. Holm, "Sparse and irregular sampling in array processing," in *Proc., IEEE Intl. Conf. Acoust., Speech, Signal Process. (ICASSP)*, vol. 6, pp. 3850–3853 vol.6, 2000.
- [36] S. Kirkpatrick, C. D. Gelatt, and M. P. Vecchi, "Optimization by simulated annealing," *Science*, vol. 220, no. 4598, pp. 671–680, 1983.
- [37] D. Bertsimas and J. Tsitsiklis, "Simulated annealing," *Statistical Science*, vol. 8, no. 1, pp. 10–15, 1993.
- [38] J. Lassing, E. Strom, T. Ottosson, and E. Agrell, "The exact symbol and bit error probabilities of coherent M-ary PSK," in *Proc., IEEE Intl. Symposium Info. Theory (ISIT)*, p. 11, June 2003.