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 featuring a large number of co-located antennas. This paper exploits the potential of large antenna arrays 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 modulate the radiation pattern at the symbol rate by driving only a subset of antennas in the array. This results in a directional radiation pattern that projects a sharply defined constellation in the desired direction and expanded further randomized constellation in other directions. Two techniques for implementing ASM are proposed. The first technique selects an antenna subset randomly for every symbol. While randomly switching antenna subsets does not affect the symbol modulation for a desired receiver along the main direction, it effectively randomizes the amplitude and phase of the received symbol for an eavesdropper along a sidelobe. Using a simplified statistical model, an expression for the average uncoded symbol error rate (SER) is derived as a function of the observation angle. To overcome the problem of large sidelobes in random antenna subset switching, the second technique uses an optimized antenna subset selection procedure based on simulated annealing to achieve superior performance compared with random selection. Numerical comparisons of the SER performance and secrecy capacity of the proposed techniques against those of conventional array transmission are presented to highlight the potential of ASM.

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). Their work was supported by the National Science Foundation grant 1218338.

Angel Lozano is with the Department of Information & Communication Technologies, Universitat Pompeu Fabra (UPF), Barcelona 08018, Spain (email: angel.lozano@upf.edu). His work is supported by the Spanish Ministry of Economy and Competitiveness, Ref. TEC2009-13000.
I. INTRODUCTION

Large-dimensional antenna arrays can play an important role in millimeter-wave (mm-Wave) communication. The mm-Wave band between 30 and 300 GHz offers an abundance of bandwidth for applications such as wireless backhaul, personal area networking, local area networking, and mm-Wave cellular communication [1]–[6]. Because of the large bandwidth and ensuing high noise levels, most mm-Wave systems use directional transmission in order to provide array gain to enhance the signal-to-noise ratio (SNR). The protocols of [1]–[5] are designed entirely around the support of directional transmission and reception including features such as directional device discovery, hierarchical beam selection, and beam tracking. Adaptive arrays are a flexible approach to implement directional transmission. At mm-Wave frequencies, these arrays can contain in excess of 64 antennas and may be co-located with active circuit components on a single silicon die [7], [8] due to the small wavelengths. The implementation of beamforming in mm-Wave systems is different than in microwave systems because it is mostly analog in nature so as to reduce the power consumption of the baseband circuitry [9], [10].

Security is an important requirement for commercial wireless systems, and mm-Wave communication is no exception. While 60-GHz links experience high atmospheric absorption [11], other mm-Wave bands may be more vulnerable to interception. It may be possible, for a sufficiently sensitive eavesdropper, to recover information from the signal power that escapes through sidelobes. Consequently, it is of interest to develop beamforming techniques that provide an extra layer of security by exploiting flexibility at the physical (PHY) layer.

Directional modulation (DM) is one approach for achieving enhanced security. Several related approaches have been proposed that leverage multiple transmit antennas including near-field antenna-level modulation, switched antenna phased array transmitters and spatial keying (SK) transmission techniques such as spatial modulation (SM) and space shift keying (SSK). Previous work in [12], [13] introduced an analog transmit architecture for synthesizing directional information based on near-field direct antenna modulation. In this approach, there is no digital baseband and data modulation takes place at the antenna level. Specifically, an unmodulated carrier drives a single antenna (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 far-field antenna pattern 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.
antenna arrays. Recent work in [14]–[16] demonstrates a DM technique for phased-array transmitters. By modifying the weights at each antenna, a symbol with desired phase and amplitude can be created along a particular direction while purposely distorting the constellation in other directions. A closely related DM technique using pattern-reconfigurable antennas is presented in [17]. In [18], hopping among the antennas in an array is shown to produce a directional frequency/phase modulated signal. DM for spread spectrum communication is introduced in [19] and [20], where the DM signal is modulated at both the baseband and the antenna levels. While [19] proposes a dual-beam technique to create a modulated signal using two different radiation patterns, [20] relies on switching antennas based on a chipping sequence. Apart from DM techniques designed to achieve communication secrecy, there have also been studies on the effect of multiple antennas and fading on the secrecy capacity. In [21], [22], the secrecy capacity of a SM technique, where one of several transmit antennas is active per channel use to convey information, is analyzed. By exploiting the randomness in space, due to antenna location, and the randomness of the wireless channel, due to fading, SK-based transmission techniques are seen to offer improved outage secrecy capacity.

In this paper, we propose a low-complexity DM technique called Antenna Subset Modulation (ASM). We introduce ASM as an antenna-level modulation technique that eliminates conventional baseband circuitry and takes advantage of the full antenna array with a limited number of radio frequency (RF) chains. By providing a simple inter-antenna phase shift and driving a different subset of antennas at each symbol interval, we show that it is possible to create a direction-dependent modulated signal. This allows the transmitter to introduce additional randomness in the constellations viewed at angles other than the target direction. It is worth noting that the proposed ASM technique is motivated by the large number of antennas available in mm-Wave communication and the requirements for lower complexity mixed-signal hardware, but the theory and methods hold for in general for large antenna arrays and thus are conceptually applicable to any frequency band.

We propose two antenna subset selection techniques to implement ASM in uniform linear arrays. In the first technique, the antenna subsets used for transmission are selected at random from the set of all subsets with same number of active antennas. We capture this subset selection procedure using a simplified statistical model and show that the received symbol distribution in undesired directions can be closely approximated by a Gaussian distribution. Equipped with the statistics of the received symbol distribution, we then proceed to evaluate the average uncoded symbol error rate (SER) achieved by ASM with $K$-ary PSK modulation. In the second technique, we propose an optimized antenna subset selection procedure based on simulated annealing to overcome the large sidelobe levels that may result from random antenna
selection. In this improved technique, antenna subsets are selected from a carefully constructed codebook exhibiting satisfactory sidelobe properties. Random subset selection has the advantages of being easier to analyze and implement, while the optimized subset selection offers better performance but requires either on-line optimization or off-line computation and storage of optimum antenna subsets.

Compared to DM techniques [12]–[15], [17], [19] that scramble the constellation in undesired transmission directions, ASM artificially introduces randomness in the received constellation through antenna subset selection to combine the benefits of security and directional transmission. One benefit of ASM is that it allows for a large number of antennas to be co-located, despite the increase in the design space. Exploring such larger design space to find the parameters (switch combinations in [12], [13], phase shifts in [14] or antenna weights in [15]) that produce a desired constellation along an intended direction while still enforcing a high error rate in other directions can be unwieldy. For instance, the number of switch configurations to be explored for producing a desired symbol along a particular direction increases exponentially with the array size in [12]. Another benefit of ASM is that it enables the transmitter to steer the main beam towards a desired direction while still offering DM. Prior work in [14], [15], [18], [20] does not account for beam-steering since these references consider communication at lower frequencies where spatial diversity from widely spaced antennas is more important than array gain. The DM technique in [12] can steer the beam to an arbitrary direction in a phased-array configuration, but the constellation synthesis involves searching a very large design space. In turn, [17] features only restricted beam-steering capabilities and requires a separate design procedure for every possible orientation.

Relative to SK-based transmission techniques such as SM and SSK, ASM is designed to facilitate directional transmission using compact arrays. First, in SK-based transmission techniques, a block of bits is mapped to spatial positions of the transmit antennas in the array [23]–[28]. Information is encoded in the choice of transmit antennas in SM and SSK, whereas symbol modulation takes place at the phase shifters in ASM and the particular choice of antennas does not convey information. Second, in SK, the wireless channel acts as a modulation unit and hence rich-scattering environment may be needed to create distinct (albeit random) spatial signatures for the different transmit antennas; the receiver then detects the set of active transmit antennas from the modulated signal to decode the transmitted information symbol. In ASM, however, the digital modulation symbols received in the desired direction are not randomized. Moreover, the receiver performs conventional digital demodulation and is unaware of the transmit antenna subset used for the symbol transmission. Finally, unlike SM technique where multiple transmit antennas are used to provide multiplexing gain at low system complexity, ASM uses multiple antennas for directional beamforming—most necessary at mm-Wave frequencies to overcome the huge
path loss, the atmospheric absorption, and the high noise levels. Essentially, SK techniques and ASM techniques are designed under different channel and array assumptions and each has its application in its preferred operating regime.

**Organization:** The remainder of this paper is organized as follows. In Section II, we introduce the channel model and explain the concept of ASM. Subsequently, in Section III, we discuss the constellation synthesis procedure for ASM. In Sections IV and V, we propose the 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 transmission. Finally in Section VII, we draw some conclusions and point to topics of future work.

**Notation:** $a_i$ is the $i$th entry of the vector $a$, $[A]_{i,j}$ is the entry of the matrix $A$ in the $i$th row and $j$th column, $a \odot b$ indicates Hadamard (entrywise) product of two vectors $a$ and $b$, $\mathcal{N}(\mu, P)$ denotes a real Gaussian random vector with mean $\mu$ and covariance $P$, $\mathcal{CN}(\mu, P)$ denotes a complex Gaussian distribution with mean $\mu$ and covariance $P$, $\text{Bern}(p)$ denotes a Bernoulli random variable with parameter $p$, and $\mathcal{U}(.)$ denotes a discrete uniform distribution. We use $\mathbb{P}[.]$ to denote probability, $\mathbb{E}[.]$ to denote expectation, $\text{var}[.]$ to denote variance, $\perp$ to denote statistical independence between random variables, $\Re[.]$ and $\Im[.]$ to denote real and imaginary parts, and $\binom{N}{M}$ to denote the binomial coefficient.

## II. PRINCIPLES OF ANTENNA SUBSET MODULATION

### A. Channel Model

Consider a multiple-input single-output (MISO) communication system with $N$ transmit and a single receive antenna; although the ideas developed in this paper can be extended to multiple receive antennas, we consider a single receive antenna for the sake of the exposition. The transmitter is equipped with $M \leq N$ RF chains. We consider uniform linear arrays with isotropic antennas; the same approach can be applied to multidimensional periodic arrays, i.e., 2D/3D arrays on regular grids. We posit an $N$-element linear array with antennas uniformly spaced by $d$ along the $x$-axis and with the array centered at the origin. Since the linear array positioned on the $x$-$y$ plane cannot resolve elevation ($\phi$), the receiver’s angular location is solely specified by the azimuth angle $\theta$. The transmitter knows the angular location of the target receiver, but not of the eavesdroppers. Assuming a narrowband channel with perfect synchronization and symbol-rate sampling, the received signal along any direction $\theta$ at discrete-time $k$ can be written as

$$y(k, \theta) = h^*(\theta)x(k) + v(k)$$  \hfill (1)
where $h$ is the $N \times 1$ channel vector, $x$ is the transmit signal vector and $v \sim \mathcal{CN}(0, N_0/2)$. Invoking a narrowband channel model is justified at mm-Wave because the line-of-sight (LoS) component usually dominates over the multipath due to relatively high reflection and scattering losses from indoor building materials [29]; incorporating a more complex channel model is a topic of future work. The channel vector (and, hence, the received symbol) is a function of the receiver’s angular location.

We specify $d \leq \lambda/2$, where $\lambda$ is the wavelength, to avoid creating grating lobes. The channel for a receiver located along the $\theta$ direction can then be written as [30]

$$h(\theta) = \begin{bmatrix} e^{-j\left(\frac{N-1}{2}\frac{2\pi d}{\lambda}\cos \theta\right)}, \quad e^{-j\left(\frac{N-1}{2}-1\right)\frac{2\pi d}{\lambda}\cos \theta}, \quad \ldots, \quad e^{j\left(\frac{N-1}{2}\right)\frac{2\pi d}{\lambda}\cos \theta} \end{bmatrix}^*$$ \hspace{1cm} (2)

where the phase-shifts introduced by path-length differences are referred to the center of the array.

We consider the use of directional beamforming to provide array gain. There is no attempt to place nulls in the locations of potential eavesdroppers because their positions are unknown. With beamforming, the transmitted vector symbol at time $k$ is $x(k) = w(k)x(k)$ where $w$ 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 the spatial matched filter. Under our LoS and uniform linear array assumptions, the channel coefficients have equal magnitude and consequently only co-phasing is required. Such uniform amplitudes maximize the directivity of the array among all amplitude excitation patterns [30] and enable a simple feed network.

**B. Conventional Array Transmission**

Fig. 1 shows the block diagram of a typical phased array transmitter where the number transmit antennas equals the number of RF chains, i.e., $N = M$. The in-phase (I) and quadrature (Q) components of the signal are modulated at baseband followed by RF up-conversion and beamforming in the RF domain. Finally, the phase shifted signal at each branch is amplified by a power amplifier (PA) before coupling onto the antenna.

Consider the situation in Fig. 1, where the array is transmitting a complex phase-modulated symbol, $x(k) = \sqrt{E_s}e^{j\psi(k)}$, to a target receiver using conventional baseband modulation. The target receiver is along the $\theta_T$ radial while another receiver located along the $\theta_U$ direction is eavesdropping. Recall that the transmitter knows $\theta_T$ but not $\theta_U$. The transmitter can orient its main beam along $\theta_T$ by setting
Fig. 1. Typical phased array transmitter with QPSK modulation.

\[ w(k) = \frac{1}{M} h(\theta_T) \forall k. \] The transmitted vector symbol is

\[ x(k) = w(k) x(k) = \sqrt{E_s} e^{j\psi(k)} \]  

(3)

Using (1), the noiseless symbol received along an arbitrary direction \( \theta \) is

\[ y(k, \theta) = h^*(\theta) x(k) \]

(5)

\[ = \frac{\sqrt{E_s} e^{j\psi(k)}}{M} h^*(\theta) h(\theta_T) \]

(6)

\[ = \frac{\sqrt{E_s} e^{j\psi(k)}}{M} \sum_{n=0}^{M-1} e^{-j\left(\frac{M-1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta} e^{j\left(\frac{M-1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta_T} \]

(7)

\[ = \frac{\sqrt{E_s} e^{j\psi(k)}}{M} e^{-j\left(\frac{M-1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta} \sum_{n=0}^{M-1} e^{j\left(\frac{M-1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta_T} \]

(8)

\[ = \frac{\sqrt{E_s} e^{j\psi(k)}}{M} e^{-j\left(\frac{M-1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta} \left(1 - e^{jM \frac{2\pi d}{\lambda} \cos \theta} \right) \]

(9)

\[ = \frac{1}{M} \sin \left(\frac{M(\gamma - \gamma)}{2}\right) \frac{\sqrt{E_s} e^{j\psi(k)}}{\sin \left(\frac{\gamma - \gamma}{2}\right)} \]

(10)

\[ \text{a real value for every } \theta \]

\[ = \rho(\theta) \sqrt{E_s} e^{j\psi(k)} \]  

(11)

where \( \gamma = \gamma(\theta) = \frac{2\pi d}{\lambda} \cos \theta \) with \( \rho(\theta) \) denoting the (real) scaling factor for every \( \theta \). Note that \( \rho(\theta) < \)
\( \rho(\theta_T) = 1 \forall \theta \neq \theta_T. \)

Both the target and the undesired receiver observe effectively the same information. The constellation received in undesired transmit directions differs only in terms of power. Therefore, an eavesdropper with a sufficiently sensitive receiver can recover information from the received signal if it has enough gain to overcome the loss embodied \( \rho(\theta) \).

C. Antenna Subset Modulation

Next, we explain the principles of ASM and provide some intuition about the security aspect of this transmission technique.

1) Principles: Although at mm-Wave frequencies a large number of antennas can be accommodated, the number of RF chains is still limited by cost. In an ASM transmitter, there are \( M \) RF chains but the number of antennas is now \( N > M \). A sinusoidal carrier signal drives only a subset of the antennas after passing through phase shifters and PAs as illustrated in Fig. 2. Since there are only \( M \) RF chains, the antenna subset used for transmission at each symbol contains exactly \( M \) antennas. A control block determines the phase shifts for each branch and selects the subset of \( M \) active antennas using a high-speed RF switch.

![ASM transmitter with QPSK Modulation](image)

Fig. 2. ASM transmitter with QPSK Modulation. The dashed line controls the selection of an antenna subset and provides the corresponding inter-antenna phase shift necessary for modulation and beam steering.
A fundamental difference between ASM and conventional array transmission is that, in ASM, modulation occurs in the RF domain. At each symbol, the control block synthesizes an array by selecting a subset of $M$ antennas. The chosen subset 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, this pattern appears to be modulated at the symbol rate. This changing radiation pattern enhances the security of ASM. In the absence of any multipath, the pattern (along a particular radial) defines a complex symbol on the I-Q plane.

Modulation of information bits to symbols with simultaneous beam-steering is achieved by phase shifting the active antennas in the synthesized array. By providing a phase offset besides the progressive inter-antenna phase shift (for beam-steering), ASM can produce the desired phase of each symbol along the target radial.

Since there is no complex baseband modulation involved, $x(k) = \sqrt{E_s} \forall k$ representing the constant amplitude (unmodulated) carrier. The effects of data modulation, beam-steering and antenna subset selection at symbol $k$ are succinctly represented by the beamforming vector

$$w(k) = \frac{1}{M} [b(k) \circ h(\theta_T)] e^{j\psi(k)} \quad (12)$$

where $\psi$ is a constant data-dependent phase offset introduced in addition to the progressive inter-antenna phase shifts, $b$ is an $N \times 1$ vector with $b_i = \{0, 1\}$ and $\sum_{i=0}^{N} b_i = M$ enforcing the constraint on the total number of active antennas. The binary vector $b(k)$ thus encodes the $M$-antenna subset selected for transmitting the $k$th symbol. The positions with ones indicate active antennas while zeros indicate unused antennas. The ASM transmit signal is expressed as

$$x(k) = w(k)x(k) \quad (13)$$

$$= \sqrt{E_s} e^{j\psi(k)} \frac{1}{M} [b(k) \circ h(\theta_T)]. \quad (14)$$

If $B$ denotes the set of all such binary vectors $b$, the noiseless received symbol can be expressed from (1) as

$$y(k, \theta) = h^*(\theta) x(k) \quad (15)$$

$$= \sqrt{E_s} e^{j\psi(k)} \frac{1}{M} h^*(\theta) [b(k) \circ h(\theta_T)] \quad (16)$$

$$= \frac{1}{M} h^*(\theta) [b(k) \circ h(\theta_T)] \sqrt{E_s} e^{j\psi(k)} \quad (17)$$

complex scalar dependant on $\theta$ and $b(k)$

information symbol
\[ = \rho(\theta, b(k)) \sqrt{E_s e^{j\psi(k)}} \tag{18} \]

for some \( b(k) \in B \). The scaling factor \( \rho \) in (18) is in general complex for every \( \theta \neq \theta_T \) and changes with the symbol index \( k \).

Since the ASM technique relies on switching antennas at the symbol rate, high-speed RF switches are a critical part of the transmitter design. To achieve fast antenna switching in ASM, a series of high-frequency single-pole multi-throw (SPMT) switches capable of switching at nanosecond or sub-nanosecond speeds with low insertion loss and good isolation properties is needed. Several solid-state switch implementations such as PIN diodes, metal semiconductor field effect transistors (MESFETs) and hot electron mobility transistors (HEMTs) have been reported previously [31]–[37] for mm-Wave transceiver applications and are applicable to the ASM transmitter array design.

2) Secure Data Transmission: In addition to providing directional information to the target receiver, ASM conveys misinformation in undesired directions. This makes it more difficult for an eavesdropper to decode useful information.

Let the active antenna subset, \( b \), be chosen at random from the set \( B \) for each symbol. Because of beamforming along the target direction, the various (phase shifted) signal replicas add coherently along the mainlobe direction, i.e., \( y(k, \theta_T) = \sqrt{E_s} e^{j\psi(k)} \) since \( \rho(\theta_T, b(k)) = 1 \ \forall \ b(k) \in B \). But, outside of a narrow solid cone centered on the target radial, the signals add up misaligned in phase. Depending on the antenna subset chosen, the desired modulation symbol appears scaled and rotated to an undesired receiver. This creates a distorted constellation \( C_U \) that is very different from the target constellation \( C_T \) as shown in Fig. 2. The constellation in unintended directions appears randomized because of the random choice of an antenna subset for each symbol. Rather than 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 off as being generated by the changing far-field pattern along the sidelobes as a result of the randomized antenna selection procedure. Thus, while switching the active antenna subset does not alter the constellation along the mainlobe, the symbols are distorted in both phase and amplitude for undesired receivers on the sidelobes.

III. ASM CONSTELLATION SYNTHESIS

ASM can be produce the desired phase of each symbol for any constant-envelope modulation scheme. The use of constant envelope signals in ASM minimizes the linearity requirement on the PAs, enabling high power efficiency by operating near the saturation region.
Suppose that the 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 radiation pattern, denoted henceforth by $F(\theta)$, to equal $\sqrt{E_s}e^{\imath \psi(k)}$ along $\theta_T$. Note that the dependence of the far-field pattern on symbol index $k$ is implicit.

As remarked earlier, only a subset of $M (< N)$ antennas is selected for use during each symbol in ASM. The process of selectively turning off certain antennas in an array is called array thinning and the array thus synthesized is referred to as a thinned array. Let $\mathcal{I}(k)$ denote the set of $M$ antennas used for transmitting the $k$th symbol, i.e.,

$$\mathcal{I}(k) = \{ n \in \{0, 1, \ldots, N - 1\} : b_{n+1}(k) = 1 \}, \ |\mathcal{I}(k)\rangle = M \ \forall k. \quad (19)$$

The set $\mathcal{I}(k)$ encodes the location of the active antennas for time index $k$. Thus, for a given antenna spacing $d$, $\mathcal{I}(k)$ completely characterizes the resulting spatially nonuniform array.

In ASM, we perform the modulation and beam-steering operations jointly. The inter-antenna phase shift applied to each branch to steer the mainlobe towards $\theta_T$ can be obtained using (2), (12) and (19) as

$$w_{n+1}(k) = \begin{cases} \frac{1}{M} e^{\imath \left(\psi(k) - \left(n - \frac{N - 1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta_T\right)} & n \in \mathcal{I}(k) \\ 0 & n \notin \mathcal{I}(k) \end{cases} \quad (20)$$

Thus the composite inter-antenna phase shift, denoted by $\varphi_n$, needed to produce the desired complex symbol along $\theta_T$ is

$$\varphi_n(k) = \underbrace{\psi(k)}_{\text{modulation component}} - \underbrace{\left(n - \frac{N - 1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta_T}_{\text{beam-steering component}}, \ n \in \mathcal{I}(k). \quad (21)$$

Using (20) as beam-steering vector, the far-field radiation pattern (in the absence of mutual coupling) of the synthesized linear array along an arbitrary direction $\theta$ is

$$F(\theta) = h^*(\theta)x(k) \quad (22)$$

$$= \sqrt{E_s}h^*(\theta)w(k) \quad (23)$$

$$= \sqrt{E_s} \sum_{n \in \mathcal{I}(k)} \frac{1}{M} e^{\imath \left(\psi(k) - \left(n - \frac{N - 1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta_T\right)} e^{\imath \left(n - \frac{N - 1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta} \quad (24)$$

$$= \frac{\sqrt{E_s} e^{\imath \psi(k)}}{M} \sum_{n \in \mathcal{I}(k)} \ e^{\imath \left(n - \frac{N - 1}{2}\right) \frac{2\pi d}{\lambda} \left(\cos \theta - \cos \theta_T\right)} \quad (25)$$

and the pattern of the array along the desired orientation $\theta_T$ is

$$F(\theta_T) = \sqrt{E_s} e^{\imath \psi(k)}. \quad (26)$$
It is critical to recognize that the signals from each antenna add up with perfect alignment along the mainlobe direction to produce the desired symbol irrespective of the antenna subset picked, i.e., any randomness in the choice of the antenna subset $\mathcal{I}(k)$ disappears along $\theta = \theta_T$. Thus, by appropriately varying the inter-antenna phase shifts, ASM can produce every symbol in any constant-envelope modulation scheme.

Notice that only the inter-antenna phase shift needs to be changed to transmit along an arbitrary direction. This makes the constellation design procedure in ASM much simpler than other DM techniques such as [12], [14], [38], where one must typically run an optimization algorithm to identify the correct set of weights, phase shifts or switching combinations required to produce a desired modulation symbol for each target direction. Moreover, these DM 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.

IV. ASM FOR SECURE COMMUNICATION

A. Random Antenna Subset Selection

Random Antenna Subset Selection (RASS) is a simple antenna subset selection technique for ASM. In RASS, the antenna subset chosen for a particular symbol is equally likely to be any of the subsets containing $M$ active antennas. While the signals from each antenna add coherently along the mainlobe irrespective of the selected antenna subset (cf. (26)), they add up misaligned in phase causing signal defocusing along any sidelobe direction. An example illustrating the randomization of a transmit symbol in an undesired direction is shown in Fig. 3. Since the antenna subsets used for transmission are picked at random, the arrays synthesized have large sidelobes on average. Nevertheless, the RASS technique yields itself to a simplified statistical analysis and provides the basic intuition behind secure transmission using ASM. In Section V we propose an optimized antenna subset selection technique that offers reduced sidelobe levels.

B. Statistical Model and Analysis

The modulation symbols are represented by

$$s_\ell = \sqrt{E_s} e^{j\ell\pi/K}, \quad \ell = 0, 1, \ldots, K - 1.$$  

(27)

Let $\theta_T$ and $\Omega$ denote, respectively, the target radial and the angular region outside of a solid cone centered on that target radial, 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 antennas are chosen independently at random for every symbol, we can model each antenna as an independent Bernoulli random variable with parameter \( p \) denoting the probability of antenna selection. Choosing \( p = M/N \), the thinning ratio, ensures that the arrays synthesized have \( M \) active antennas asymptotically. The pattern \( F(\theta) \) 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 these statistics to approximate the uncoded SER (hereafter referred to as simply SER) produced by RASS. Note that, while the proposed statistical model closely approximates the pattern of the actual array synthesized by RASS for \( \theta \in \Omega \), the approximation may not be accurate outside of \( \Omega \). This is because, inside the cone, the signals from different antennas add constructively; the randomness introduced by RASS disappears and the constellation produced approaches \( C_T \).

Let \( X_n(k) \) be a complex random variable denoting the weighting coefficient at the \( n \)th antenna when transmitting the \( k \)th symbol. We can express \( X_n(k) \) as
\[
X_n(k) = Y_n(k)Z_n
\] (28)
where \( Y_n(k) \) models randomness in transmit symbol selection whereas \( Z_n \) models randomness in antenna subset selection. According to the proposed statistical model,
\[
Y_n(k) = \frac{\sqrt{E_s}}{M}e^{j\psi(k)}e^{-j(n-\frac{N-1}{2})\frac{2\pi d}{\lambda}\cos \theta_T}, \quad n = 0, 1, \ldots, N - 1
\] (29)
\[ \psi(k) \sim U \left( \frac{1}{K} \right) \quad \forall k \text{i.e., } P \left( \psi(k) = \ell \frac{2\pi}{K} \right) = \frac{1}{K} \quad \ell = 0,1,\ldots,K-1, \]

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

By construction, \( Y_n(i) \perp Y_n(j) \) if \( i \neq j \), \( Z_i \perp Z_j \) if \( i \neq j \), and \( Y_i \perp Z_j \) \( \forall i,j \in \{0,1,\ldots,N-1\} \).

Rewriting \( X_n(k) \) in terms of \( Y_n(k) \) using (28) and (31),

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

Analogous to (24), an approximate stochastic model for the pattern of a thinned array synthesized using RASS is

\[ \tilde{F}(\theta) = \sum_{n=0}^{N-1} X_n(k) e^{j \left( (n-N-1) \frac{2\pi}{N} \cos \theta \right)} \]

where \( \sim \) differentiates the stochastic model from the true pattern \( F(\theta) \). For any given \( k \), (33) is a weighted sum of \( N \) independent and identically distributed (i.i.d.) complex random variables and it is thereby closely approximated by a complex Gaussian distribution for large enough \( N \), i.e., \( \tilde{F}(\theta) \sim \mathcal{CN}(\tilde{\mu}(\theta), \tilde{P}(\theta)) \).

The I and Q parts of \( \tilde{F}(\theta) \) can be stacked to form a two-dimensional real Gaussian vector

\[ \tilde{f}(\theta) = \begin{bmatrix} \Re[\tilde{F}(\theta)] \\ \Im[\tilde{F}(\theta)] \end{bmatrix} \sim \mathcal{N}(\tilde{\mu}(\theta), \tilde{P}(\theta)) \]

where \( \tilde{\mu}(\theta) \in \mathbb{R}^{2 \times 1} \) and \( \tilde{P}(\theta) \in \mathbb{R}^{2 \times 2} \) denote the mean and covariance of the two-dimensional real Gaussian distribution. Note that the parameters of the distribution depend on the observation angle \( \theta \) and implicitly on the actual transmit symbol. The Gaussian approximation improves with \( N \) and is better when the thinning ratio \( M/N \) is not too close to 0 or 1.

Fig. 4 depicts the goodness of a Gaussian fit to the empirical distribution of the I and Q components produced by RASS along an undesired direction. In this example, a 35-antenna 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 also shown.

To analyze the average SER under RASS, we only need a statistical description of the received symbol cluster (as a function of direction) when transmitting an arbitrary symbol. To simplify the notation, we drop the dependence of \( X_n, Y_n \) and \( \psi \) on the symbol index \( k \).
Fig. 4. Histogram of the I and Q components of the symbol received along an undesired direction when using RASS. The corresponding Gaussian fits are overlaid.

Since the received symbol is approximately Gaussian distributed in undesired directions, we only need the mean and covariance to characterize its distribution. Exploiting both sides of (33), the mean is

$$\tilde{\mu}(\theta) = \mathbb{E}[\tilde{F}(\theta)]$$

$$= \mathbb{E} \left[ \sum_{n=0}^{N-1} X_n e^{j\left(n - \frac{N-1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta} \right]$$

$$= \sum_{n=0}^{N-1} \mathbb{E}[X_n] e^{j\left(n - \frac{N-1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta}$$

$$= \sum_{n=0}^{N-1} \mathbb{E}[Y_n] \mathbb{E}[Z_n] e^{j\left(n - \frac{N-1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta}$$

$$= \frac{\sqrt{E_s} e^{j\psi}}{N} \sum_{n=0}^{N-1} e^{-j\left(n - \frac{N-1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta} e^{j\left(n - \frac{N-1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta}$$

$$= \frac{\sqrt{E_s} e^{j\psi}}{N} e^{-j\left(\frac{N-1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta} \sum_{n=0}^{N-1} e^{j\frac{n\pi d}{\lambda} \cos \theta}$$

$$= \frac{\sqrt{E_s} e^{j\psi}}{N} e^{-j\left(\frac{N-1}{2}\right) \frac{2\pi d}{\lambda} \cos \theta} \left(1 - e^{j\frac{2\pi d}{\lambda} \cos \theta} \right) \left(1 - e^{j\frac{2\pi d}{\lambda} \cos \theta} \right)$$

$$= \frac{\sqrt{E_s} e^{j\psi}}{N} \left( \frac{\sin \left(\frac{2\pi d}{\lambda} \cos \theta \right)}{\sin \left(\frac{\pi d}{\lambda} \cos \theta \right)} \right) \left(1 - e^{j\frac{2\pi d}{\lambda} \cos \theta} \right)$$

January 5, 2013 DRAFT
\[
\begin{align*}
\frac{\sqrt{E_s}}{N} \sin \left( \frac{N(\gamma_\theta - \gamma_{\theta_1})}{2} \right) e^{j\psi},
\end{align*}
\]

(43)

from which we can define

\[
\tilde{\mu}(\theta) = \mathbb{E} \left[ \tilde{f}(\theta) \right]
\]

(44)

\[
= \begin{bmatrix}
\Re[\tilde{\mu}(\theta)] \\
\Im[\tilde{\mu}(\theta)]
\end{bmatrix}
\]

(45)

\[
= \begin{bmatrix}
\sqrt{E_s} \\
N \\
\sqrt{E_s} \\
N \\
\end{bmatrix}
\begin{bmatrix}
\sin \left( \frac{N(\gamma_\theta - \gamma_{\theta_1})}{2} \right) \\
\frac{\sin \left( \frac{N(\gamma_\theta - \gamma_{\theta_1})}{2} \right)}{\sin \left( \frac{\gamma_\theta - \gamma_{\theta_1}}{2} \right)} \\
\sin \left( \frac{N(\gamma_\theta - \gamma_{\theta_1})}{2} \right) \\
\frac{\sin \left( \frac{N(\gamma_\theta - \gamma_{\theta_1})}{2} \right)}{\sin \left( \frac{\gamma_\theta - \gamma_{\theta_1}}{2} \right)}
\end{bmatrix}
\begin{bmatrix}
\cos \psi \\
\sin \psi
\end{bmatrix}
\]

(46)

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 radial.

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

\[
\tilde{f}_1(\theta) = \Re[\tilde{F}(\theta)]
\]

(47)

\[
= \tilde{F}(\theta) + \tilde{F}^*(\theta)
\]

(48)

\[
= \frac{1}{2} \sum_{n=0}^{N-1} \left( X_n e^{j(n - \frac{N-1}{2})\gamma_\theta} + X_n^* e^{-j(n - \frac{N-1}{2})\gamma_\theta} \right)
\]

(49)

\[
= \frac{1}{2} \sum_{n=0}^{N-1} \left( Y_n Z_n e^{j(n - \frac{N-1}{2})\gamma_\theta} + Y_n^* Z_n^* e^{-j(n - \frac{N-1}{2})\gamma_\theta} \right).
\]

(50)

Noting that \( Z_n \) is real and plugging (29) into (50),

\[
\tilde{f}_1(\theta) = \frac{1}{2} \sum_{n=0}^{N-1} \frac{\sqrt{E_s}}{M} Z_n \left( e^{j(\psi + (n - \frac{N-1}{2})(\gamma_\theta - \gamma_{\theta_1}))} + e^{-j(\psi + (n - \frac{N-1}{2})(\gamma_\theta - \gamma_{\theta_1}))} \right)
\]

(51)

\[
= \frac{\sqrt{E_s}}{M} \sum_{n=0}^{N-1} Z_n \cos \left( \psi + \left( n - \frac{N-1}{2} \right)(\gamma_\theta - \gamma_{\theta_1}) \right).
\]

(52)

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

\[
\tilde{f}_2(\theta) = \Im[\tilde{F}(\theta)]
\]

(53)

\[
= \frac{\sqrt{E_s}}{M} \sum_{n=0}^{N-1} Z_n \sin \left( \psi + \left( n - \frac{N-1}{2} \right)(\gamma_\theta - \gamma_{\theta_1}) \right).
\]

(54)
We first find \( \tilde{P}(\theta) \), the variance of the real component of the received symbol under our stochastic model. From (52), we see that the variance of \( \Re[\tilde{F}(\theta)] \) is

\[
[\tilde{P}(\theta)]_{1,1} = \text{var}[\tilde{F}_1(\theta)]
\]

(55)

\[
= \text{var} \left[ \sum_{n=0}^{N-1} \frac{\sqrt{E_s}}{M} Z_n \cos \left( \psi + \left( n - \frac{N - 1}{2} \right) (\gamma_\theta - \gamma_{\theta T}) \right) \right]
\]

(56)

\[
= \frac{E_s}{M^2} \sum_{n=0}^{N-1} \text{var} [Z_n] \cos^2 \left( \psi + \left( n - \frac{N - 1}{2} \right) (\gamma_\theta - \gamma_{\theta T}) \right)
\]

(57)

\[
= \frac{E_s}{NM} \left( 1 - \frac{M}{N} \right) \sum_{n=0}^{N-1} \cos^2 \left( \psi + \left( n - \frac{N - 1}{2} \right) (\gamma_\theta - \gamma_{\theta T}) \right)
\]

(58)

where we have used \( Z_n \sim \text{Bern}(\frac{M}{N}) \). Using trigonometric identities we can simplify (58) as

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

(59)

A similar analysis on the imaginary component of the received symbol (54) yields

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

(60)

It is important to note that, like the mean, the variances of the real and imaginary components of \( \tilde{F}(\theta) \) oscillate and depend on the transmitted symbol. However, the total variance \( \tilde{P}(\theta) \) is constant (in terms of the observation angle \( \theta \)) for a given array configuration. Indeed, using (59) and (60),

\[
\tilde{P}(\theta) = \text{var}[\tilde{F}(\theta)]
\]

(61)

\[= [\tilde{P}(\theta)]_{1,1} + [\tilde{P}(\theta)]_{2,2}
\]

(62)

\[= \frac{E_s}{M} \left( 1 - \frac{M}{N} \right).
\]

(63)

Several observations can be made from (59), (60), and (63). 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 confirmed by the individual variances of the I and Q components going to zero irrespective of \( \theta \). Second, for a fixed \( M \), adding more antennas to the array (thereby reducing the thinning ratio \( M/N \)) increases the total variance. An increase in the variance of the received symbol in undesired directions is helpful because it provides more security. Also, increasing the total number of antennas in the array increases the effective aperture size thereby enabling the randomly synthesized thinned array to have a reduced mainlobe width compared to a uniform array with \( M \) antennas. This leads to a narrow beamwidth towards the target receiver, which is desirable.
Using (52) and (54), we can express the first term in (64) as a function of angle using our statistical model. The covariance between \( \tilde{f}_1(\theta) \) and \( \tilde{f}_2(\theta) \) is

\[
[\hat{\mathbf{P}}(\theta)]_{1,2} = [\hat{\mathbf{P}}(\theta)]_{2,1} = \mathbb{E}[\tilde{f}_1(\theta)\tilde{f}_2(\theta)] - \mu_1(\theta)\mu_2(\theta). \tag{64}
\]

Using (52) and (54), we can express the first term in (64) as

\[
\mathbb{E}[\tilde{f}_1(\theta)\tilde{f}_2(\theta)] = \mathbb{E} \left[ \sum_{m,n=0}^{N-1} E_s \mathbb{E}[Z_mZ_n]\cos \left( \psi + \left( m - \frac{N-1}{2} \right)(\gamma_\theta - \gamma_{\theta_1}) \right) \sin \left( \psi + \left( n - \frac{N-1}{2} \right)(\gamma_\theta - \gamma_{\theta_1}) \right) \right] \tag{65}
\]

\[
= \frac{E_s}{M^2} \left\{ \sum_{n=0}^{N-1} \mathbb{E}[Z_n^2]\cos \left( \psi + \left( n - \frac{N-1}{2} \right)(\gamma_\theta - \gamma_{\theta_1}) \right) \sin \left( \psi + \left( n - \frac{N-1}{2} \right)(\gamma_\theta - \gamma_{\theta_1}) \right) \right. \\
+ \sum_{m,n=0}^{N-1} \mathbb{E}[Z_mZ_n]\cos \left( \psi + \left( m - \frac{N-1}{2} \right)(\gamma_\theta - \gamma_{\theta_1}) \right) \sin \left( \psi + \left( n - \frac{N-1}{2} \right)(\gamma_\theta - \gamma_{\theta_1}) \right) \right\}. \tag{66}
\]

Since \( Z_m \perp Z_n, \forall m \neq n, \mathbb{E}[Z_mZ_n] = \mathbb{E}[Z_m]\mathbb{E}[Z_n] = (M/N)^2 \) and (66) becomes

\[
\mathbb{E}[\tilde{f}_1(\theta)\tilde{f}_2(\theta)] = \frac{E_s}{MN} \left\{ \sum_{n=0}^{N-1} \cos \left( \psi + \left( n - \frac{N-1}{2} \right)(\gamma_\theta - \gamma_{\theta_1}) \right) \sin \left( \psi + \left( n - \frac{N-1}{2} \right)(\gamma_\theta - \gamma_{\theta_1}) \right) \right. \\
+ \left. \frac{E_s}{N^2} \sum_{m,n=0}^{N-1} \cos \left( \psi + \left( m - \frac{N-1}{2} \right)(\gamma_\theta - \gamma_{\theta_1}) \right) \sin \left( \psi + \left( n - \frac{N-1}{2} \right)(\gamma_\theta - \gamma_{\theta_1}) \right) \right\}. \tag{67}
\]

Again, using trigonometric identities we can simplify the two parenthetical expressions in (67) as follows:

\[
\sum_{n=0}^{N-1} \cos \left( \psi + \left( n - \frac{N-1}{2} \right)(\gamma_\theta - \gamma_{\theta_1}) \right) \sin \left( \psi + \left( n - \frac{N-1}{2} \right)(\gamma_\theta - \gamma_{\theta_1}) \right) = \frac{1}{2} \frac{\sin (N(\gamma_\theta - \gamma_{\theta_1}))}{\sin (\gamma_\theta - \gamma_{\theta_1})} \sin (2\psi), \tag{68}
\]

\[
\sum_{m,n=0}^{N-1} \cos \left( \psi + \left( m - \frac{N-1}{2} \right)(\gamma_\theta - \gamma_{\theta_1}) \right) \sin \left( \psi + \left( n - \frac{N-1}{2} \right)(\gamma_\theta - \gamma_{\theta_1}) \right) \\
= \frac{\sin \left( \frac{(N-1)(\gamma_\theta - \gamma_{\theta_1})}{2} \right)}{\sin \left( \frac{\gamma_\theta - \gamma_{\theta_1}}{2} \right)} \sin \left( \frac{(N-1)(\gamma_\theta - \gamma_{\theta_1})}{2} \right) \sin (2\psi). \tag{69}
\]

Substituting (68) and (69) into (67),

\[
\mathbb{E}[\tilde{f}_1(\theta)\tilde{f}_2(\theta)] = \frac{E_s}{2MN} \frac{\sin (N(\gamma_\theta - \gamma_{\theta_1}))}{\sin (\gamma_\theta - \gamma_{\theta_1})} \sin (2\psi) \\
+ \frac{E_s}{N^2} \frac{\sin \left( \frac{N(\gamma_\theta - \gamma_{\theta_1})}{2} \right)}{\sin \left( \frac{\gamma_\theta - \gamma_{\theta_1}}{2} \right)} \sin \left( \frac{(N-1)(\gamma_\theta - \gamma_{\theta_1})}{2} \right) \sin (2\psi). \tag{70}
\]
Using (46), the product of the means is

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

(71)

Finally, substituting (70) and (71) into (64), we obtain the covariance between the real and imaginary parts as

\[ [\hat{\mathbf{P}}(\theta)]_{1,2} = [\hat{\mathbf{P}}(\theta)]_{2,1} \]

\[ = \frac{E_s}{2MN} \left( 1 - \frac{M}{N} \right) \frac{\sin \left( N(\gamma_\theta - \gamma_{\theta_T}) \right)}{\sin \left( \gamma_\theta - \gamma_{\theta_T} \right)} \sin(2\psi) \]  

(72)

(73)

which evidences that the artificial randomness introduced in the I and Q 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 small (< 0.1) for most angles.

Eqs. (46), (59), (60), and (73) are the parameters of the Gaussian approximation to the noiseless received symbol distribution in undesired directions. Additive White Gaussian Noise (AWGN) is easily incorporated by modifying the covariance \( \hat{\mathbf{P}}(\theta) \): if \( N_0 \) denotes the total noise variance, the mean and covariance of the received symbol in undesired directions becomes

\[ \tilde{\mu}_N(\theta) = \tilde{\mu}(\theta), \]

(74)

\[ \tilde{\mathbf{P}}_N(\theta) = \hat{\mathbf{P}}(\theta) + \frac{N_0}{2} \mathbf{I}_2. \]  

(75)

It is worth restating that the Gaussian approximation to the received symbol distribution is accurate as long as the eavesdropper is in the angular region outside the target cone.

C. Secure Communication Link

Equipped with the statistics of the Gaussian approximation to the received symbol, we now analyze the corresponding SER. We first consider the case when there is no AWGN 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 RASS. Note that conventional array transmission cannot guarantee any security in the absence of noise.

The computation of the average SER with RASS parallels the one used for deriving the error rates for conventional digital modulation [39], only with the AWGN replaced by the statistical model for the randomness introduced by antenna subset selection (discussed in the previous subsection). For \( K \)-ary PSK, the modulation symbols are represented by \( s_\ell \) for \( \ell = 0, 1, \ldots, K - 1 \) as in (27). As discussed previously,
the received symbol in undesired transmit directions can be regarded as approximately Gaussian. From (46), (59), (60), and (73), we see that, unlike in AWGN, the parameters of the received distribution depend on the transmit symbol $s_\ell$. To make this dependence explicit, we denote the mean and covariance of the received symbol by $\tilde{\mu}(\ell, \theta)$ and $\tilde{P}(\ell, \theta)$, respectively.

Under ML detection, a received symbol is in error if it falls outside the Voronoi region of the actual symbol transmitted along $\theta_T$. The average SER according to our statistical model for the received symbol distribution can be expressed as

$$P_s(\theta) = 1 - \frac{1}{K} \sum_{\ell=0}^{K-1} \int_{\Lambda_\ell} \frac{1}{2\pi |\tilde{P}(\ell, \theta)|^2} \exp \left\{ -\frac{1}{2} (z - \tilde{\mu}(\ell, \theta))^T \tilde{P}(\ell, \theta)^{-1} (z - \tilde{\mu}(\ell, \theta)) \right\} dz$$

(76)

where $\Lambda_\ell$ is the Voronoi region associated with $s_\ell$ and $\tilde{P}(\ell, \theta) > 0$. When $K = 4$, i.e., with QPSK, (76) can be simplified by virtue of the symmetry and the diagonal form of $\tilde{P}(\ell, \theta)$ as

$$P_s(\theta) = 1 - \frac{1}{2\pi \sqrt{|\tilde{P}(0, \theta)|}} \int_{\Lambda_0} \exp \left\{ -\frac{1}{2} \left( \frac{(z_1 - \tilde{\mu}_1(0, \theta))^2}{|\tilde{P}(0, \theta)|_{1,1}} + \frac{(z_2 - \tilde{\mu}_2(0, \theta))^2}{|\tilde{P}(0, \theta)|_{2,2}} \right) \right\} dz_1 dz_2$$

(77)

where

$$\tilde{\mu}(0, \theta) = \begin{bmatrix} \sqrt{E_s} \left( \frac{\sin(N(\gamma - \gamma_T))}{\sin(\frac{\gamma}{2})} \right) \\ 0 \end{bmatrix}$$

(78)

$$\tilde{P}(0, \theta) = \begin{bmatrix} E_s \left( 1 - \frac{M}{N} \right) \left( N + \frac{\sin(N(\gamma_0 - \gamma_T))}{\sin(\gamma_0/2)} \right) \\ 0 \\ 0 \frac{E_s}{2MN} \left( 1 - \frac{M}{N} \right) \left( N - \frac{\sin(N(\gamma_0 - \gamma_T))}{\sin(\gamma_0/2)} \right) \end{bmatrix}$$

(79)

$$\Lambda_0 = \{ (z_1, z_2) \in \mathbb{R} : z_1 + z_2 \geq 0, \ z_1 - z_2 \geq 0 \}$$

(80)

and the 2-D integral in (77) can be evaluated using the cumulative distribution function of the bivariate normal distribution. For $K > 4$, however, no closed forms exist for (76) and numerical integration is required. Note that (76) represents the irreducible SER with RASS, which can only increase with AWGN.

Fig. 5 shows the SER achieved by RASS with QPSK. We observe that the statistical error rate expression derived from (76) closely approximates the simulated error rate even for a moderate value of $N = 28$. From Fig. 5, it is evident that the theoretical average SER approaches zero as $\theta$ approaches $\theta_T$ since it is the error rate in the absence of any additive noise. From analysis and simulations, the limit point in $\theta$ where the average error rate plummets to zero is approximately given by the location of the
first null from $\theta_T$ i.e., $\theta \approx \cos^{-1}\left(\frac{\lambda}{Nd} \pm \cos(\theta_T)\right)$ for an $N$-element linear array. Thus, for a given $\frac{d}{\lambda}$ and $\theta_T$, a larger aperture size ($N$) leads to a narrower cone where the error rate approaches zero.

Fig. 6 compares the simulated and theoretical SER for different values of $M$ and $N$. We observe that the Gaussian assumption on the received symbol distribution in unwanted directions is valid even for small values of $N$ and the approximation becomes tighter as the number of antennas, $N$, increases.

With additive white Gaussian noise (AWGN), the average SER can be computed again using (76), but with the modified mean and covariance parameters in (74) and (75).

\[ C_S = \begin{cases} 
C_T - C_U & \text{if } C_T > C_U \\
0 & \text{otherwise} \end{cases}, \quad \text{(81)} \]

One can also quantify the degree of transmission security in an information-theoretic sense, using the notion of \textit{secrecy capacity}. The secrecy capacity of a channel is the maximum transmission rate at which information can be communicated reliably and securely. In [40], it was shown that for a Gaussian wiretap channel the secrecy capacity, denoted by $C_S$, is the difference between the capacity of the main and the wiretap channels. Adopting this definition, we calculate the secrecy capacity for both conventional array transmission and ASM. Since there are no closed forms for the constrained capacity with discrete constellations, we must numerically evaluate them. Denoting the target and undesired receiver’s capacity by $C_T$ and $C_U$, respectively,
Fig. 6. Comparison between the statistical approximation of the average SER and simulated error rates for linear arrays with different length when steered towards $\theta_T = 36^\circ$.

For QPSK symbol transmission,

$$C_S(\theta) = C_{\text{QPSK}}(\text{SNR}(\theta_T)) - C_{\text{QPSK}}(\text{SNR}(\theta))$$  \hspace{1cm} (82)

where $C_{\text{QPSK}}(\cdot)$ denotes the AWGN constrained capacity with QPSK.

We need to find the average SNR for the two transmission schemes to calculate their secrecy capacities.

For conventional array transmission, invoking (5), the SNR assuming rectangular pulse-shaping is

$$\text{SNR}(\theta) = \frac{E_s}{2N_0} \left( \frac{1}{M} \sin \left( \frac{M(\gamma_\theta - \gamma_{\theta_T})}{2} \right) \right)^2.$$  \hspace{1cm} (83)

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

For ASM, the SNR at the target receiver’s location equals that of conventional array transmission since the constellation is undistorted in this direction. To calculate the SNR along undesired directions, we invoke the Gaussian approximation to the received symbol distribution. Specifically, the square of $\tilde{\mu}_N(\theta)$ in (74) for every angle is a measure of the average symbol energy in that direction. The noise variance (in undesired directions) consists of AWGN plus the artificial noise introduced by RASS. Since such artificial noise is uncorrelated with the AWGN, the effective noise covariance is the sum of individual covariances $\tilde{P}_N(\theta)$ from (75).

With QPSK, the noise introduced by ASM has zero-mean and uncorrelated I and Q components, i.e.,
\[ [\hat{P}]_{1,2} = [\hat{P}]_{2,1} = 0. \]

Therefore, the aggregate noise can be modeled as AWGN with the modified variance
\[
\hat{P}_N = 2N_0 + \frac{E_s}{M} \left( 1 - \frac{M}{N} \right).
\] (84)

The average SNR for ASM is thus
\[
\text{SNR}(\theta) = \frac{|\hat{\mu}_N|^2}{2N_0 + \frac{E_s}{M} \left( 1 - \frac{M}{N} \right)}
\] (85)
\[
= \frac{E_s}{2N_0 + \frac{E_s}{M} \left( 1 - \frac{M}{N} \right)} \left( \frac{1}{N} \sin \left( \frac{\gamma_\theta - \gamma_{\theta T}}{2} \right) \right)^2 \forall \theta \in \Omega.
\] (86)

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

Thus, we see that the use of 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. In the next section, we propose an optimized antenna subset selection technique that offers even better security and array performance.

V. OPTIMIZED ANTENNA SUBSET SELECTION

Every antenna subset having a fixed number of active antennas is equally probable in RASS. Though the spatially nonuniform arrays these subsets correspond to have a similar mainlobe, the sidelobes can be rather different. Therefore, we next seek to create a smaller codebook of antenna subsets that possess low sidelobes so as to select antenna subsets at random only from this collection. Note that, since all antenna subsets are equivalent along the mainlobe, restricting the set of possibilities does not affect our ability to communicate with the target receiver.

A. Thinned Array Pattern Synthesis

The problem of synthesizing thinned arrays with desirable characteristics is a combinatorial optimization problem that has been studied extensively in the past [41]–[49]. The effect of thinning on the array gain and mainlobe width is predictable. Harder to characterize is the effect of thinning on the sidelobe levels because that depends on both the location and the number of active antennas. Unfortunately, there are no analytical techniques to synthesize a thinned array with certain sidelobe behavior. For an \( N \)-antenna array, the number of subsets with exactly \( M (< N) \) active antennas is \( \binom{N}{M} = \frac{N!}{(N-M)!M!} \). Even for moderate values of \( N \) and \( M \), this number can be enormous; for \( N = 64 \) and \( M = 32 \), for instance,
\( \binom{N}{M} \sim 10^{18} \). Given the impracticality of an exhaustive search, heuristic optimization techniques based on simulated annealing, genetic algorithms and its variants have been proposed to find near-optimal solutions [41]–[49]. We henceforth focus on simulated annealing.

### B. Optimized Antenna Subset Selection Based on Simulated Annealing

Simulated annealing [50], [51] is a probabilistic iterative algorithm for finding 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 \( B \) consisting of antenna subsets that correspond to nonuniform arrays with low sidelobe levels, with the constraint that the number of active antennas in the thinned array, \( M \), be fixed. The simulated annealing algorithm as applied to antenna subset selection is illustrated below using pseudo code.

The simulated annealing algorithm retains only one array solution (and an associated temperature) at each instant. The algorithm is initialized with a random array configuration containing \( M \) active antennas. Then, at every iteration, the solution is perturbed. By allowing perturbations that only swap the location of an “on” antenna for an “off” antenna we ensure that the number of active antennas is always \( M \). 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 diminishes. The replacement of better solutions by worse ones at higher temperatures ensures that the algorithm does not gets stuck in a local optimum. After a sufficient number of iterations, the algorithm converges to a near-optimal solution that has a lower cost.
Algorithm Simulated Annealing

1: procedure ANTEA_SUBSET_SELECTION (M, N)
2: Initialize(b₀, T₀, iter_count) ▷ bᵢ is the thinning pattern rep. as a binary vector
3: for i = 1 to iter_count do
4:   Tᵢ = βTᵢ₋₁ ensure β < 1 ▷ Exponential cooling schedule
5:   bᵢ = swap(bᵢ₋₁) ▷ Perturb bᵢ₋₁ by swapping the loc. of a 0 and 1 at random
6:   ∆E = E(b*) − E(bᵢ₋₁) ▷ Compute the change in cost ∆E
7:   if ∆E < 0 or exp(−∆E/Tᵢ) > rand[0, 1]² then
8:     bᵢ = b* ▷ Probabilistically accept the new solution if ∆E ≥ 0
9:   else
10:    bᵢ = bᵢ₋₁ ▷ Try another perturbation
11: end if
12: end for
13: end procedure

The performance of any simulated annealing algorithm depends heavily on the choice of the cost function and cooling schedule. For this work, an exponential cooling schedule produced the best results. The algorithm seeks to minimize the cost function

\[ E = \max_{\text{SLL}} |SLL|_{\text{dB}} \]

\[ = \max_{\theta \in \Omega} 20 \log_{10} |F(\theta)| \]

where SLL stands for the sidelobe level. 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 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 \( B \) from which the transmitter draws antenna subsets for each symbol.

Reducing the sidelobe levels has benefits in terms of security. While the magnitude of the received symbols in undesired directions is now lower, the randomization in phase caused by antenna subset selection is preserved by the use of a large enough codebook. Therefore, the resulting symbol distribution in undesired directions has a mean closer to zero and is hence more susceptible to errors.

\( ^2 \text{rand}[0,1] \) generates a number uniformly distributed on the interval[0,1].
We hasten to emphasize that, for a given array configuration, the codebook is constructed only once and is independent of the target direction. This keeps the antenna subset selection procedure simple.

VI. SIMULATION RESULTS

In this section, we present numerical examples illustrating constellation synthesis, array performance and transmission security of ASM. Linear arrays with isotropic antennas are considered. The parameters for each simulation are overlaid on the corresponding plots. In some of the results that follow, the performance of ASM is compared against a conventional array with array size equal to the number of active elements in the ASM array.

A. Constellation Synthesis Results

First, we show the constellation synthesized by ASM when using the proposed antenna subset selection techniques (cf. Sections IV and V) to transmit a QPSK signal. As is evident in Fig. 7, the constellation produced by ASM along the target direction is undistorted while, along an undesired transmit direction, the received symbols appear randomized. Notice how the received symbol cluster has a lower magnitude when using optimized antenna subset selection compared to RASS. Also shown in Fig. 7 is the constellation produced by conventional array transmission in these directions, which is still crisp enough for a sensitive eavesdropper to demodulate.

B. Array Performance Results

Fig. 8 depicts the radiation patterns of a randomly thinned array and of an array synthesized using simulated annealing. The optimized array exhibits a lower sidelobe level, as expected, at the expense of a small increase in the mainlobe width. However, both arrays feature a narrower mainlobe width compared to a conventional array (with the same number of active antennas).

Histograms of the resulting sidelobe levels are shown in Fig. 9. The sidelobe behavior of the optimized array is superior to that of a conventional array, which has a sidelobe level of $-13.5$ dB when steered to broadside [30].

C. Transmission Security Results

In this section, we demonstrate that ASM can achieve a low SER around the target angle while enforcing a high SER in undesired directions. The setup consists of $N = 35$ antennas of which only $M = 20$ are active at a given time. The array beamforms along $\theta_T = 36^\circ$. Simulated annealing is used to
Fig. 7. Comparison of the constellation produced by ASM and by a conventional array along target and undesired directions.

Fig. 8. Radiation pattern for arrays synthesized by the proposed antenna subset selection techniques. The sidelobe level of the randomly thinned array and optimized array are -10.4 dB and -14.7 dB, respectively.

construct an optimized codebook of 500 thinned array subsets. For this study, $10^7$ QPSK symbols were transmitted for each angle (in 0.5° increments). The SER was calculated assuming ML detection. Fig.
Fig. 9. Empirical histogram of the peak sidelobe level for the two proposed antenna subset selection techniques in ASM.

10 illustrates the SER performance of ASM under the two subset selection techniques.

Fig. 10. Comparison of the SER with ASM and with conventional array transmission for $\theta_T = 36^\circ$.

To further compare the SER performance of ASM with that of conventional array transmission, we consider a uniform linear array with number of antennas equal to the active set size of the ASM array.
The exact SER for $K$-ary PSK then equals [52]

$$P_s(\theta) = F \left( 1, \sqrt{\frac{2E_s}{N_0}}, \cot \frac{\pi}{K} \right)$$  \hspace{1cm} (89)$$

where $F$ is the cumulative distribution function of the noncentral $t$-distribution. The SER for conventional array transmission is thus computed and also shown in Fig. 10. ASM under both antenna subset selection techniques achieves a higher SER compared to conventional array transmission in unwanted directions. Moreover, ASM produces a narrow information beamwidth around the target angle. Also, optimized antenna subset selection is shown to exhibit better transmission security compared to RASS. Along with the average SER curves from simulation, the theoretical SER for RASS is plotted in Fig. 10 using (77). The theoretical SER based on the proposed statistical model closely matches the simulation for angles $\theta \in \Omega$. It is important to note that ASM provides these security benefits without additional transmit power, unlike other DM techniques [14], [15] that trade-off security for some increase in transmission power.

Next, in Fig 11, we present results on the SER of ASM for an eavesdropper and compare it against conventional array transmission. A 12-antenna array with 9 active antennas is considered and RASS is employed in ASM. With the target receiver located along $\theta_T = 45^\circ$, two angular locations are 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) illustrates a situation where the eavesdropper is angularly close to the target while, in scenario (b) the eavesdropper is far from the target angle. In both situations, ASM under RASS outperforms conventional array transmission. Even as the SNR increases, ASM maintains a high SER while, for a conventional array, the SER falls off rapidly with SNR.

Finally, Fig. 12 shows the improved secrecy capacity of ASM. Eqs. (82), (83) and (86) were applied with QPSK. ASM achieves better secrecy capacity compared to conventional array transmission, where in multiple transmit angles the secrecy capacity is rather low. Another desirable characteristic of ASM, which is evident in the figure, is its ability to create a 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 nonzero even as $\text{SNR} \to \infty$ because of its inherent irreducible artificial noise.

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 radiation pattern of the array is modulated at the symbol
Fig. 11. Average SER versus SNR for an eavesdropper when using ASM and conventional array transmission for two scenarios with $\theta_T = 45^\circ$. Scenario (a) eavesdropper is close to the target angle, along $\theta_a = 55^\circ$. Scenario (b) eavesdropper is far off the target angle, along $\theta_b = 167^\circ$.

Fig. 12. Secrecy capacity for different eavesdropper angles when using ASM and conventional array transmission. The crosses are the interpolated values of the secrecy capacity of ASM for $\theta$ near the target angle $\theta_T$.

rate to achieve direction-dependent data transmission. Unlike other directional modulation techniques, which scramble the desired constellation in unwanted directions, ASM provides security by 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-antenna 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 based on simulated annealing. Simulation examples were used to validate the security benefits of ASM against conventional array transmission. It was concluded that ASM achieves a narrow beamwidth in the desired direction and a high SER in undesired directions under both subset selection techniques. The optimized antenna subset selection was found to provide higher security benefits.

Future work will involve an extension of the analysis to multidimensional periodic arrays. Incorporating multidirectional transmission capabilities to ASM using array partitioning techniques is also an interesting research problem that merits further study.
REFERENCES


[37] “GaAs beamlead PIN diode,” *Data sheet of MA4GP905 in M/A-COM Technology Solutions*. 


