AN ATTACK ON ANTENNA SUBSET MODULATION FOR MILLIMETER WAVE COMMUNICATION

Cristian Rusu, Nuria González-Prelcic

Universidade de Vigo
Email: {crusu,nuria}@gts.uvigo.es

Robert W. Heath Jr.

The University of Texas at Austin
Email: rheath@utexas.edu

ABSTRACT

Antenna subset modulation (ASM) is a physical layer security technique that is well suited for millimeter wave communication systems. The key idea is to vary the radiation pattern at the symbol rate by selecting one from a subset of patterns with a similar main lobe and different side lobes. This paper shows that ASM is not robust to an eavesdropper that makes multiple simultaneous measurements at multiple angles. The measurements are combined and used to formulate an estimation problem to undo the effects of the side lobe randomization. Simulations show the performance of the estimation algorithms and how the eavesdropper can effectively recover the information if the signal-to-noise ratio exceeds a certain threshold. Using fewer active radio frequency chains makes it harder for the attacker to recover the transmit symbol, at the expense of more grating lobes.

Index Terms— Antenna subset modulation, millimeter wave communication, physical layer security, large antenna arrays.

1. INTRODUCTION

Communication at millimeter wave (mmWave) frequencies has applications in personal area, local area, and cellular networks [1]. A distinguishing feature of mmWave systems is that they use adaptive arrays at both the transmitter and receiver. As in lower frequency systems, security is also important for mmWave systems. One approach to enhance security is what is widely known as physical layer security [2, 3, 4, 5, 6]. The large antenna arrays in mmWave systems can be exploited by physical layer security techniques like antenna subset modulation (ASM) [7].

ASM combines the benefits of security and directional transmission. It artificially introduces randomness in the received constellation in directions different from the intended transmission angle. It also has the advantage of eliminating the need for conventional baseband circuitry, using only a limited number of radio frequency chains, while at the same time exploiting the large antenna arrays that will be used in mmWave systems. The original claims about the security of ASM made in [7] assumed that the eavesdropper made measurements only at a single angle. As we show in this paper, a smart adversary can attack the ASM system by making multiple simultaneous measurements at different angles and combining the results together. There are various techniques related to ASM. For example directional modulation (DM) also scramble the symbol constellation in the undesired directions [8, 9]. Another example is spatial keying (SK) transmission techniques [10, 11] such as spatial modulation (SM) and space shift keying (SSK) where the information is encoded in the subset selection of the transmit antennas from the large dimensional antenna arrays. SM and SSK were developed for lower frequency systems with different channel models. Further, the security enhancement in DM, SM, and SSK were not quantified. There are a number of physical layer security methods for multiple antenna systems [12, 13, 14, 15, 16] but these approaches are generally analyzed assuming rich scattering channels, which are not a good assumption for mmWave communication.

In this paper we show how compressive sensing techniques and standard estimation techniques can be used to formulate an effective attack on ASM. We design a receiver strategy that lets a sufficiently sensitive eavesdropper recover the information encoded in the ASM signal without knowledge of the time varying antenna selection pattern or the angular location of the target receiver. The key idea is to combine simultaneous measurements made at carefully chosen locations, so that the measurement matrix is full rank and the resulting system of equations has a unique solution. We suggest a way to enhance ASM by the use of smaller antenna subsets, with an increase in the sidelobes amplitudes.

2. PROBLEM STATEMENT

Consider the mmWave MISO communication system in Figure 1. Directional beamforming is used to provide array gain along an azimuth angle θ_{T}, the angular location of the target receiver. Elevation angle is not considered, since we assume that the array will be positioned in the x–y plane. In this paper we will consider an array with N total antennas. The transmitter uses a subset of only $M < N$ antennas in the array for the transmission of a given symbol, and this subset changes from one symbol to the next one, following the principles of Antenna Subset Modulation (ASM) described in [7]. This generates a changing radiation pattern which provides physical layer security, making more difficult for an eavesdropper to decode transmitted data, as explained in the next paragraphs. We assume a narrowband channel model dominated by the LoS component, perfect synchronization and symbol-rate sampling. In this case, the channel vector for a receiver located along the θ direction can be written as

$$\boldsymbol{h}^H(\theta) = \Big[\, e^{-j\left(\frac{N-1}{2}\right)\frac{2\pi d}{\lambda}\cos(\theta)},\ e^{-j\left(\frac{N-1}{2}-1\right)\frac{2\pi d}{\lambda}\cos(\theta)},\ \ldots,\ e^{j\left(\frac{N-1}{2}\right)\frac{2\pi d}{\lambda}\cos(\theta)}\Big]$$

with $d \leq \lambda/2$ and being λ the wavelength. The transmitter uses directional beamforming to orient its main beam along θ_{T} and antenna

This work was partially funded by the Spanish Government and the European Regional Development Fund (ERDF) under projects TACTICA and COMPASS (TEC2013-47020-C2-1-R), and by the Galician Regional Government and ERDF under AtlantTIC.

This material is based upon work supported in part by the National Science Foundation under Grant No. NSF-CCF-1319556.

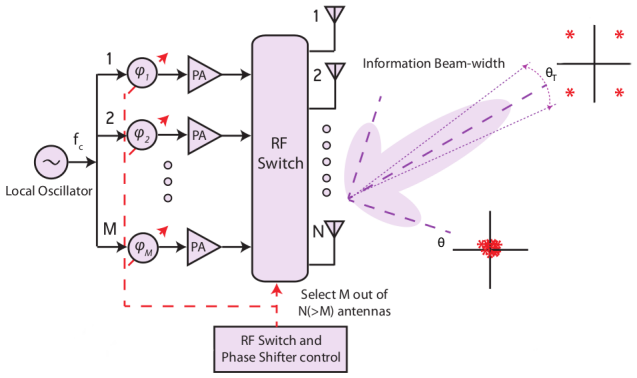

Fig. 1: An example of an ASM transmitter with QPSK modulation. We show how in the direction of θ_{T} the constelation is received unaltered while in any other direction θ the constelation is rotated and scaled, in different ways, with every symbol transmitted. The phase shifts $\varphi_1, \ldots, \varphi_M$ are the entries of the beamformer $\boldsymbol{w}(k)$.

subset selection at symbol k. Symbols are generated by introducing an additional data dependent phase offset in the active antennas. Thus, the beamforming vector $\boldsymbol{w}(k)$ represent the effects of complex phase modulation, beamforming and antenna subset selection at symbol k

$$\boldsymbol{w}(k) = \frac{1}{M}[\boldsymbol{b}(k) \odot \boldsymbol{h}(\theta_{\mathrm{T}})]\, e^{j\psi(k)} \tag{1}$$

where $\odot$ is the elementwise multiplication operation and $\psi(k)$ is the constant data-dependent phase offset introduced in addition to the progressive inter-antenna phase shifts, $\boldsymbol{b}(k) \in \mathcal{B}_N$ is an $N \times 1$ vector, where $\mathcal{B}_N$ denotes the set of all binary vectors of size N, and $\mathbf{1}^T\boldsymbol{b}(k) = M$ enforcing the constraint on the total number of active antennas. The binary vector $\boldsymbol{b}(k)$ thus encodes the M-antenna subset selected for transmitting the k^{th} symbol, i.e., the positions with ones indicate active antennas while zeros indicate unused antennas. The transmit signal can be written

$$\boldsymbol{x}(k) = \boldsymbol{w}(k)x(k) \tag{2}$$

$$= \frac{\sqrt{E_{\mathrm{s}}}e^{j\psi(k)}}{M}[\boldsymbol{b}(k) \odot \boldsymbol{h}(\theta_{\mathrm{T}})]. \tag{3}$$

It can be shown [7] that the noiseless received symbol is

$$y(k,\theta) = \boldsymbol{h}^H(\theta)\boldsymbol{x}(k) \tag{4}$$

$$= \underbrace{\frac{1}{M}\boldsymbol{h}^H(\theta)[\boldsymbol{b}(k) \odot \boldsymbol{h}(\theta_{\mathrm{T}})]}_{\substack{\text{complex scalar} \\ \text{dependent on } \theta \text{ and } \boldsymbol{b}(k)}} \underbrace{\sqrt{E_{\mathrm{s}}}e^{j\psi(k)}}_{\text{information symbol}} \tag{5}$$

$$= \rho(\theta, \boldsymbol{b}(k))\sqrt{E_{\mathrm{s}}}e^{j\psi(k)} \tag{6}$$

for some $\boldsymbol{b}(k)$. The scaling factor ρ that appears in (6) is in general complex for every $\theta \neq \theta_{\mathrm{T}}$ and changes with the symbol index k, while $\rho(\theta_{\mathrm{T}}, \boldsymbol{b}(k)) = 1,\ \forall\ \boldsymbol{b}(k) \in \mathcal{B}_N$. In this paper we assume the transmission is realized using complex phase modulation schemes such as QPSK.

Given the signal in (6), our aim is to study under which conditions and available tools an eavesdropper is capable of recovering the transmitted symbol. In addition, we study different ways of increasing the robustness of the ASM technique to the attack we are able to design.

3. THE ATTACK

3.1. The setup of the attack

In this section we analyze how an eavesdropper could be able to recover information despite ASM being used by the transmitter. The undesired receiver will use multiple measurements (along different directions) and classical or sparse processing to recover the information.

Consider an eavesdropper which is capable of receiving the transmitted signal along several directions θ_ℓ, $\ell = 1, \ldots, L$, which do not coincide with the angle of the target receiver θ_{T}. The set of these reception angles is stored in the vector $\boldsymbol{\theta}$ of size $L \times 1$. The noisy symbol received along these different directions at discrete-time k is

$$\boldsymbol{y}(k,\boldsymbol{\theta}) = \boldsymbol{H}(k,\boldsymbol{\theta})\boldsymbol{x}(k) + \boldsymbol{v}(k) \tag{7}$$

where $\boldsymbol{v}(k) \sim \mathcal{CN}(0, N_0/2)$ and the $L \times N$ channel matrix $\boldsymbol{H}(k,\boldsymbol{\theta})$ is defined as

$$\boldsymbol{H}(k,\boldsymbol{\theta}) = \begin{bmatrix}\boldsymbol{h}(\theta_1) & \boldsymbol{h}(\theta_2) & \ldots & \boldsymbol{h}(\theta_L)\end{bmatrix}^H = \begin{bmatrix} e^{jz_1\pi\cos\theta_1} & e^{jz_2\pi\cos\theta_1} & \ldots & e^{jz_N\pi\cos\theta_1} \\ e^{jz_1\pi\cos\theta_2} & e^{jz_2\pi\cos\theta_2} & \ldots & e^{jz_N\pi\cos\theta_2} \\ \vdots & \vdots & \ldots & \vdots \\ e^{jz_1\pi\cos\theta_L} & e^{jz_2\pi\cos\theta_L} & \ldots & e^{jz_N\pi\cos\theta_L} \end{bmatrix}. \tag{8}$$

For simplicity of exposition we denote $z_i = (N-1)/2 - i$ with $i = 0, \ldots, N-1$, and we consider $d = \lambda/2$. We also assume that $L > N$. Our aim is to develop a strategy to undo the effect of randomizing the constellation along directions which do not correspond to the target receiver. This means removing the rotation effect over the received symbols, so that the received constellation is just a scaled version of the transmitted one.

To make more explicit the different parameters that need to be estimated in order to recover the transmitted symbol, we write (7) in the following way

$$\begin{aligned}\boldsymbol{y}(k,\boldsymbol{\theta}) &= \frac{1}{M}\boldsymbol{H}(k,\boldsymbol{\theta})\boldsymbol{B}(k)\boldsymbol{h}(\theta_{\mathrm{T}})\sqrt{E_{\mathrm{s}}}e^{j\psi(k)} \\ &= \frac{1}{M}\boldsymbol{H}(k,\boldsymbol{\theta})\boldsymbol{B}(k)\boldsymbol{h}(\theta_{\mathrm{T}})x(k)\end{aligned} \tag{9}$$

where $\boldsymbol{B}(k) = \mathrm{diag}(\boldsymbol{b}(k))$. From this equation it is clear that we have three unknowns: $\boldsymbol{b}(k)$ which represents the antenna selection pattern used by the transmitter at time k, θ_{T} the angle of the target receiver and the transmitted symbol $x(k)$. Their effect is combined in the unknown vector $\boldsymbol{x}(k)$. Thus, the first goal is to recover $\boldsymbol{x}(k)$ and then to estimate the three unknowns. Given the solution $\boldsymbol{x}(k)$, it is very easy to estimate the selection pattern $\boldsymbol{b}(k)$ just by checking the non-zero entries of $\boldsymbol{x}(k)$ while the estimation of the transmitted symbol $x(k)$ does necessitate knowledge of θ_{T}, which in turn needs to be estimated separately.

Note that given the structure of $\boldsymbol{b}(k)$, if $M \ll N$, the transmitted vector is sparse, since only some of its entries are nonzero. Therefore, recovering the transmitted symbol from $\boldsymbol{y}(k,\boldsymbol{\theta})$ in (7) without knowledge of the selected subset of antennas or θ_{T} can be seen as a compressed sensing (CS) problem. The channel matrix acts as the sensing matrix, while the received signal along multiple angles constitutes the available measurement. In addition to the full column rank condition, the coherence of the channel matrix has to be low enough if we want to solve the problem from a CS perspective, making use of ℓ_1 minimization techniques. If the condition $M \ll N$ is

not verified, we cannot leverage sparsity, and have to use standard estimation algorithms as Least Squares (LS) to solve the problem.

It is well known [17] that $\boldsymbol{x}(k)$ is the unique solution to (7) if $\boldsymbol{H}$ has Kruskal-rank equal to M (or equivalently, is full column rank). Also when considering sparse reconstruction algorithms we know that the mutual coherence of $\boldsymbol{H}$ plays an important role. In the next sections we develop conditions on the set of reception angles to be used by the eavesdropper receiver which guarantee that the channel matrix is full column rank, and also present the different approaches we use to solve the problem depending on the condition $M \ll N$ is verified.

3.2. Design of the set of reception angles

In the next paragpahs we study the properties of $\boldsymbol{H}(k, \boldsymbol{\theta})$ with a particular attention on full column rank conditions and the levels of the mutual coherence.

With $\omega_\ell = e^{j\pi\cos(\theta_\ell)}$ the channel matrix entries are $(\boldsymbol{H}(k,\boldsymbol{\theta}))_{\ell n} = \omega_\ell^{z_n}$. First, notice that the channel matrix has a row Vandermonde structure which guarantees full rank N as long as $\cos(\theta_{\ell_1}) \neq \cos(\theta_{\ell_2})$ for any $\ell_1 \neq \ell_2$ [18].

The mutual coherence is the maximum absolute value correlation between any two distinct columns of $\boldsymbol{H}(k,\boldsymbol{\theta})$ is $\mu(\boldsymbol{H}(k,\boldsymbol{\theta})) = \frac{1}{L}\max_{i\neq p} |\boldsymbol{h}_i^H \boldsymbol{h}_p|$. Expanding and simplifying the dot product

$$\boldsymbol{h}_i^H \boldsymbol{h}_p = \sum_{\ell=1}^{L} e^{j\pi(z_p - z_i)\cos(\theta_\ell)} = \sum_{\ell=0}^{L-1} e^{j\frac{\pi(z_p-z_i)\ell}{L-1}} = \sum_{\ell=0}^{L-1} \omega^\ell, \tag{10}$$

with $\omega = e^{j\frac{\pi(z_p-z_i)}{L-1}}$ and assuming that the angles θ_ℓ are selected such that $\phi_\ell = \cos(\theta_\ell)$ are uniformly distributed in $[0,1]$. Thus $\phi_\ell = \ell/(L-1)$ with $\ell = 0,\ldots,L-1$. The maximum is attained when $z_p - z_i = 1$ leading to the final simplification

$$\mu(\boldsymbol{H}(k,\boldsymbol{\theta})) = \frac{1}{L}\left|\frac{\sin(\pi/2)}{\sin(\pi/(2L-2))}\right|. \tag{11}$$

With this choice for the angles $\boldsymbol{\theta}$ the value of the mutual coherence depends exclusively on the number of measurements L and generally does not take values approaching the upper bound of 1.

3.3. Estimation of the transmitted symbol

As previously explained, the eavesdropper needs to estimate three different parameters contained in the received vector to be able to obtain the transmitted symbol. Therefore, we can split the estimation process in three different steps.

1. Estimation of the support of $\boldsymbol{x}(k)$. The first goal is to recover the support of the solution. Equipped with this estimation we can then proceed with the estimation of θ_{T} and ultimately of the symbol $x(k)$. We propose two ways to accomplish this:

- The least squares method. The direct obvious approach would be to solve

$$\underset{\boldsymbol{x}(k)}{\text{minimize}} \quad \|\boldsymbol{y}(k,\boldsymbol{\theta}) - \boldsymbol{H}(k,\boldsymbol{\theta})\boldsymbol{x}(k)\|_2. \tag{12}$$

  Since we do not assume a sparsity constraint, i.e. we do not have that $M \ll N$, this is a sensible approach.

- The ℓ_1 optimization method. To explicitly impose the binary structure to the selection pattern in $\boldsymbol{b}(k)$ we propose to solve the regularized problem

$$\underset{\boldsymbol{x}(k)}{\text{minimize}} \quad \|\boldsymbol{x}(k)\|_1 + \lambda\|\boldsymbol{y}(k,\boldsymbol{\theta}) - \boldsymbol{H}(k,\boldsymbol{\theta})\boldsymbol{x}(k)\|_2. \tag{13}$$

  Because of the sparsity constraint we expect this approach to work better if $M \ll N$.

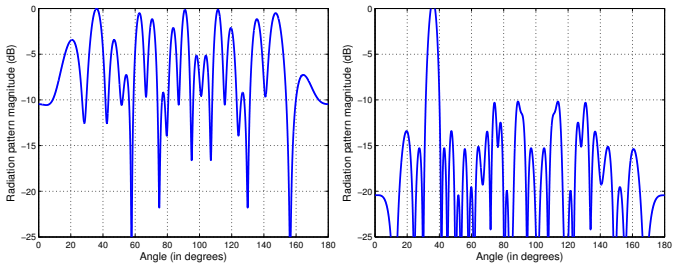

Fig. 2: The radiation patterns for a random sparse antenna subset with $M = 3$ (left) and for a random dense antenna subset with $M = 20$ (right). We set $N = 35$ and $\theta_{\mathrm{T}} = 36^\circ$.

We denote the solutions to the previous problem by $\tilde{\boldsymbol{x}}(k)$. We will denote the estimated antenna selection patterns $\tilde{\boldsymbol{b}}(k) = \mathbb{1}_{\tilde{\boldsymbol{x}}(k)}$, where the right hand side is the indicator function that takes values of 1 for a non-zero entry and 0 otherwise.

The way problems (12) and (13) are formulated there is no need for prior knowledge of the number of selected antennas M. If this information is available, the two problems need to be slightly modified as to accommodate for the explicit linear constraint $\mathbf{1}^T\boldsymbol{b}(k) = M$.

2. Given the angular direction θ_T of the target receiver, estimate the symbol $x(k)$.

With the antenna selection patterns estimated from the previous step and assuming we have access to the correct value of θ_{T} we have $\boldsymbol{z} = \tilde{\boldsymbol{x}}(k) \oslash \boldsymbol{h}(\theta_{\mathrm{T}})$, where $\oslash$ denotes the elementwise division. The vector $\boldsymbol{z}$ contains copies of the symbol $x(k)$, with different amplitudes, in all positions where it is not null. Thus a normalized vector would result in $\boldsymbol{z}_n = \boldsymbol{z} \oslash |\boldsymbol{z}|$. Assuming we are dealing with a QPSK constellation, a good way to estimate the symbol $x(k)$ from $\boldsymbol{z}_n$ is be to inspect the signs of the real and imaginary parts of $\boldsymbol{z}_n$, i.e., $\Re(\boldsymbol{z}_n)$ and $\Im(\boldsymbol{z}_n)$.

3. Estimation of the angular location of target receiver θ_{T}.

If θ_{T} is known, finding the transmitted symbol is easy due to the previous observations. But generally the attacker does not know this preferred angle. To estimate it we will use $\tilde{\boldsymbol{x}}(k)$ and the fact that in the direction of θ_{T} the symbol constellation is not rotated, only scaled, irrespective of the antenna subset picked. To estimate θ_{T} we employ the following 1D search procedure:

- Compute all $\boldsymbol{z}_i = \tilde{\boldsymbol{x}}(k) \oslash \boldsymbol{h}(\theta_i)$ where the angles θ_i belong to a fine grid of Q points equally spaced in the interval $[0,\pi]$.
- Solve by checking

$$\tilde{\theta}_{\mathrm{T}} = \underset{\theta_i}{\arg\max} \left|\sum \mathrm{sgn}(\Re(\boldsymbol{z}_i))\right| + \left|\sum \mathrm{sgn}(\Im(\boldsymbol{z}_i))\right|, \tag{14}$$

  where sgn is the signum function.

Following this searching procedure we notice that the maximum value $(2M)$ is attained for several angles near the true preferred angle θ_{T}. This is because when using ASM the constellation is unaltered inside a narrow solid cone centered on the target radial to θ_{T}. In such a situation we choose the center of the interval. Since the ASM technique allows for one direction where the constellations does not suffer rotational transformations we can be sure that if the estimation of the support $\tilde{\boldsymbol{b}}(k)$ was exact then θ_{T} belongs to this interval.

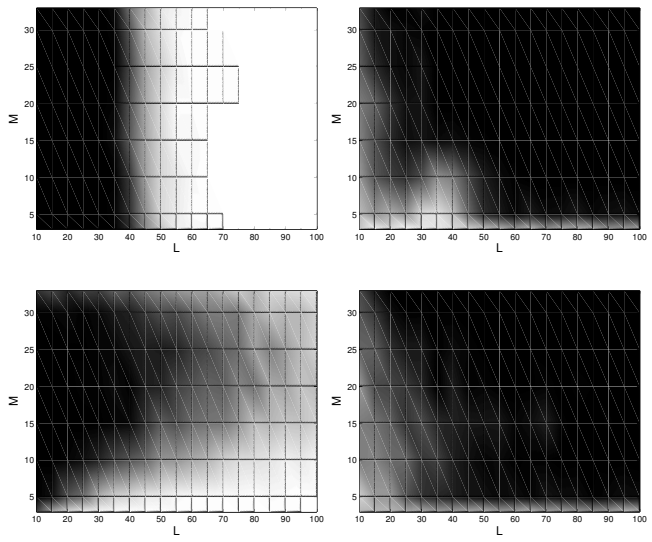

Fig. 3: Phase transitions for the least squares (top) and ℓ_1 (bottom) approaches for the recovery of the antenna subset (left) and for the recovery error of the preferred angle θ_{T} (right). In the case of the antenna subset recovery lighter is better (higher perfect recovery rate) while for the angle recovery darker is better (lower estimation error).

We treat the computation of $\tilde{\theta}_{\mathrm{T}}$ separately because this angle does not change with the transmission of every symbol, it remains the same during a transmission session. Still, its computation can be done at each time k in order to improve the quality of the estimate.

In the following sections we move to show how the proposed attack works various simulated scenarios and we discuss variations of ASM that are potentially robust to the proposed attack.

4. AN ASM TECHNIQUE ROBUST TO THE ATTACK

In Figure 2 we show the difficulty of estimating the preferred angle θ_{T} in an ASM architecture with $N = 35$ and $M \in \{3, 20\}$. The estimation of θ_{T} presented in the previous section is based on the fact that the constellation does not suffer rotational transformations in this direction and that there is only *one* such direction. When $M \ll N$ there are several angles at which the radiation pattern achieves the maximum value thus making impossible the distinction and identification of the correct transmitted symbol in these cases without knowing of the true angle of transmission θ_{T}.

A clear disadvantage in the case $M = 3$ is the high level of the side lobes. A future goal is to design radiation patterns that allow multiple peaks but also minimize the side lobe levels using a small number of antennas M. This involves searching for an antenna subset between the total $\binom{N}{M}$ possible subsets that obeys some design requierements. As applied in [7], a heuristic search procedure can be used to find near-optimal solutions.

5. SIMULATION RESULTS

We now move to show experimentally the efficacy of the proposed attack against the ASM. We show how each estimation step described in Section 3.3 can be realized.

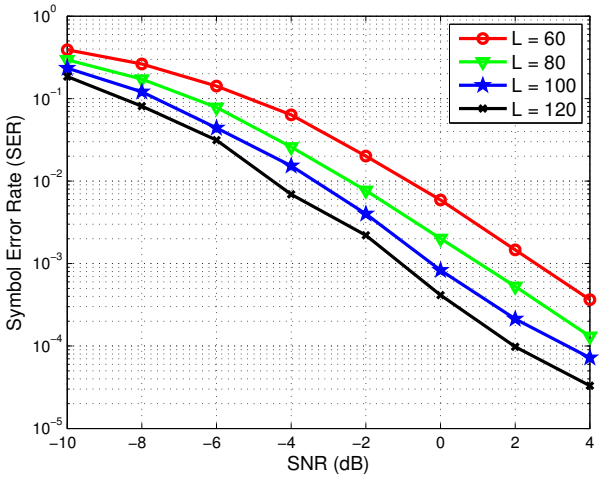

Fig. 4: Symbol Error Rate for different SNR and attacker angles L for an ASM architecture with $N = 35, M = 20$. Recovery is done using the ℓ_1 approach.

In this section we assume an ASM architecture with $N = 35$ and the transmit, preferred, angle of $\theta_{\mathrm{T}} = 36^{\circ}$. The first goal is to recover the binary vector $\boldsymbol{b}(k)$ that encodes the M–antenna subset selected when transmitting the k^{th} symbol. For various values of M and number of attacker angles L which are chosen uniformly at random in $[0, \pi]$ we show in Figure 3 phase transitions for the perfect recovery of $\boldsymbol{b}(k)$ and the phase transitions for the transmission angle estimation $|\theta_{\mathrm{T}} - \tilde{\theta}_{\mathrm{T}}|$. Results are averaged over 1000 runs, each time the L attacker angles $\boldsymbol{\theta}$ are chosen uniformly at random from $[0, \pi]$. The noiseless case is assumed. As expected, more measurements leads to better estimation of the support and transmission angle and, in the noiseless case, least squares provides better estimation.

Finally we want to show the proposed attack as it unfolds during a transmission session of various symbols in the presence of noise. Figure 4 shows the average Symbol Error Rates (SER) achieved when sending $N_{\mathrm{s}} = 10^6$ symbols assuming various values for the number of available measurements to the attacker. The recovery of the estimate $\tilde{\boldsymbol{x}}(k)$ is done using the ℓ_1 minimization approach (13) since this is robust to the addition of noise. In low, or even moderate, SNR levels the least squares approach performs poorly. Thus, for brevity, we do not show the results of the least squares method.

6. CONCLUSION

In this paper we proposed an attack on antenna subset modulation for millimeter wave communication. The attack is based on the key idea of using multiple simultaneous measurements at multiple reception angles. We derived conditions on the reception angles that guarantee that the problem of estimating the transmitted symbol from multiple measurements has a unique solution. We also analyzed the relationships between the different parameters in ASM and the number of measurements to be used by an eavesdropper to decode transmitted data. Simulation examples demonstrate how the proposed attack can decode information at moderately low SNR levels. An open problem is to analyze the secrecy capacity of ASM when the received signal consists of multiple measurements along different directions.

7. REFERENCES

[1] T. Rappaport, R. W. Heath Jr., R. Daniels, and J. Murdock, *Millimeter wave wireless communications*. Prentice Hall, 2014.

[2] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 716–721, 2008.

[3] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4–5, 2009.

[4] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*. Springer, 2010.

[5] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, UK: Cambridge University Press, 2011.

[6] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. USA: CRC Press, 2013.

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

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

[9] ——, "Beamsteering in pattern reconfigurable arrays using directional modulation," *IEEE Trans. Antennas Propag.*, vol. 58, no. 7, pp. 2259–2265, July 2010.

[10] J. Jeganathan, A. Ghrayeb, L. Szczecinski, and A. Ceron, "Space shift keying modulation for MIMO channels," *IEEE Trans. Wireless Commun*, vol. 8, no. 7, pp. 3692–3703, July 2009.

[11] J. Jeganathan, A. Ghrayeb, and L. Szczecinski, "Generalized space shift keying modulation for MIMO channels," in *Proc., IEEE Intl. Symposium on Pers., Indoor and Mobile Radio Commun. (PIMRC)*, Sep. 2008, pp. 1–5.

[12] R. Liu, T. Liu, P. H. V., and S. I. Shamai, "Multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4215–4227, Sep. 2010.

[13] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961–4972, August 2011.

[14] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in mimo wiretap channels with imperfect cs," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[15] E. Ekrem and S. Ulukus, "Capacity-equivocation region of the Gaussian MIMO wiretap channel," *IEEE Transactions on Information Theory*, vol. 58, no. 9, pp. 5699–5710, Sep. 2012.

[16] X. Zhang, X. Zhou, M. R. McKay, and R. W. Heath Jr., "Artificial-noise-aided secure multi-antenna transmission in slow fading channels with limited feedback," in *Proc., IEEE Intl. Conf. on Acoust., Speech, Signal Process. (ICASSP)*, 2014, pp. 3968 – 3972.

[17] M. Mishali and Y. C. Eldar, "From theory to practice: Sub-nyquist sampling of sparse wideband analog signals," *IEEE J. Sel. Topics Signal Process.*, vol. 4, pp. 375–391, April 2010.

[18] B. Alexeev, J. Cahill, and D. G. Mixon, "Full spark frames," *Journal of Fourier Analysis and Applications*, vol. 18, no. 6, pp. 1167–1194, June 2012.