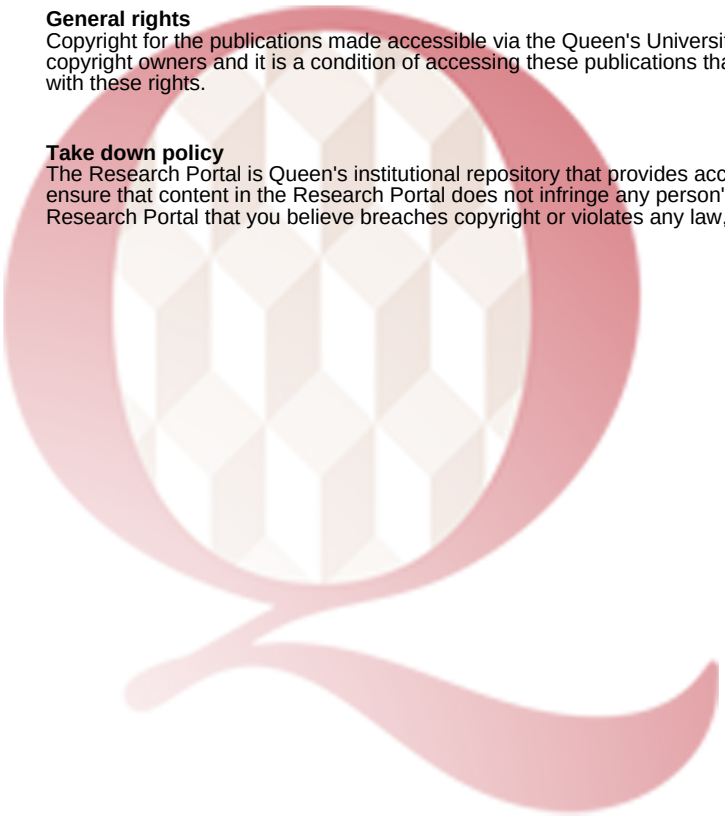
Investigation of secure wireless regions using configurable beamforming on WARP

Zhang, Y., Yin, B., Woods, R., Cavallaro, J., Marshall, A., & Ko, Y. (2014). Investigation of secure wireless regions using configurable beamforming on WARP. In 2014 Asilomar Conference on Signals, Systems, and Computers. (pp. 1979-1983). Pacific Grove, CA: IEEE Computer Society. DOI: 10.1109/ACSSC.2014.7094817

Published in:
2014 Asilomar Conference on Signals, Systems, and Computers

Document Version:
Early version, also known as pre-print

Queen's University Belfast - Research Portal:
Link to publication record in Queen's University Belfast Research Portal



Investigation of Secure Wireless Regions Using Configurable Beamforming on WARP

Yuanrui Zhang*, Bei Yin†, Roger Woods*, Joe Cavallaro†, Alan Marshall‡, Youngwook Ko*
* ECIT, Queen's University Belfast
Belfast, Northern Ireland, UK
Email: {yzhang31, r.woods, y.ko}@qub.ac.uk
† Department of Electrical and Computer Engineering Houston, Texas, USA
Email: {by2, cavallar}@rice.edu
‡ Electrical Engineering and Electronics, University of Liverpool
Liverpool, England, UK
Email: Alan.Marshall@liverpool.ac.uk

***Abstract*—In this paper, we examine a novel approach to network security against passive eavesdroppers in a ray-tracing model and implement it on a hardware platform. By configuring antenna array beam patterns to transmit the data to specific regions, it is possible to create defined regions of coverage for targeted users. By adapting the antenna configuration according to the intended user's channel state information, this allows the vulnerability of the physical regions to eavesdropping to be reduced. We present the application of our concept to 802.11n networks where an antenna array is employed at the access point. A range of antenna array configurations are examined by simulation and then realized using the Wireless Open-Access Research Platform(WARP).**

I. Introduction

Recent wireless communication systems require significantly high secrecy and privacy for transmission techniques as the connectivity between millions of user devices and access points increases. Whilst conventional security methods are designed to operate in layers other than the physical layer, extra physical layer security will be required to supplement conventional encryption methods.

The major issue in securing wireless networks is in ~~its~~ broadcast nature of radio transmissions which means that a message sent to a legitimate user will be exposed to any potential eavesdropper who is within range. For example in Fig. 1, Alice is the sender who wishes to send messages to the intended receiver Bob in the presence of a passive eavesdropper Eve. In the context of an 802.11n network, if we envisage that the access point (AP) equipped with an antenna array acts as Alice, then *beamforming* can be used to restrict the eavesdroppers' access to the signals [1]–[5]. In [1], a metric called exposure region (ER) was introduced to refer the area within which an eavesdropper can access and decode the signals being transmitted.

One challenge posed by passive eavesdroppers is that the AP does not have knowledge of Eve, or of her CSI, sometimes even her existence. Therefore, the ER should be minimized ~~so~~ that the possibility of Eve being within the ER is reduced. In [6], the problem has been formulated to minimizing the area of the ER according to Bob's location on the condition that Bob's received power must be guaranteed to be above a threshold

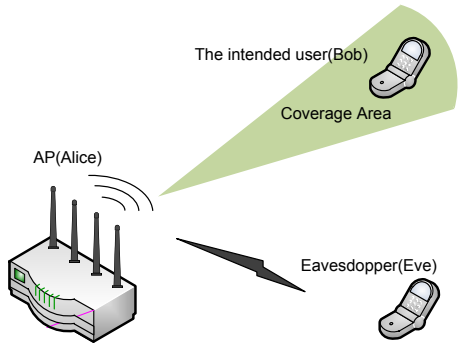


Fig. 1. A three-party communication model: Alice, Bob and Eve. The shadow area surrounding Bob illustrates the ER.

power. It has been shown that the area of ER is affected by the array configuration, i.e., the number of antenna elements and their spacing, and Bob's position. Based on the analysis of ER, configurable beamforming technique was proposed to match the array configuration and Bob's position. A look-up table is built to store the information and used to suggest the best choice based on Bob's position.

This work is an extension of configurable beamforming technique in [6]. ~~In [6],~~ we showed that configurable beamforming technique provides the array mode that gives the minimum ER based on Bob's location in free-space path loss model. However, the channel is more complex in real environments. In this paper, we will use a more realistic channel model, i.e., ray-tracing model, to study the performance of the configurable beamforming technique. Furthermore, we will explore the potential of realizing a configurable beamforming technique in a real set-up on WARP. The main contributions of the paper are:

- Direction of Emission (DoE) estimation is studied in a ray-tracing model. The estimated best angle indicates the beamforming angle for the configurable beamforming algorithm.
- Investigat~~ing~~ the applicability of configurable beamforming technique in a ray-tracing model. The results show that the look-up table generated in a free-space

TABLE I. ARRAY MODES FOR A 4-ELEMENT ARRAY

Mode	M1	M2	M3	M4	M5	M6
$(N, \Delta d/\lambda)$	(1,-)	(2,0.5)	(3,0.5)	(4,0.5)	(2,1.0)	(2,1.5)
Symbol	o - - -	o o - -	o o o -	o o o o	o - o -	o - - o

path loss model serves well as a good approximation in a ray-tracing model.

- Implementing the configurable beamformer on WARP hardware. The phase offsets induced by hardware are modeled and calibrated.
- Examining a number of beamforming configurations using the WARP hardware in an anechoic chamber. The results show that the active element pattern phenomenon and imperfect antenna pattern impact the effectiveness of the algorithm.

The rest of the paper is organized as follows. In Section II, the configurable beamforming technique is briefly reviewed. In Section III, the algorithm is examined in a ray-tracing model. Then, it is implemented on WARP in In Section IV. The conclusions and future work are given in Section V.

II. BACKGROUND

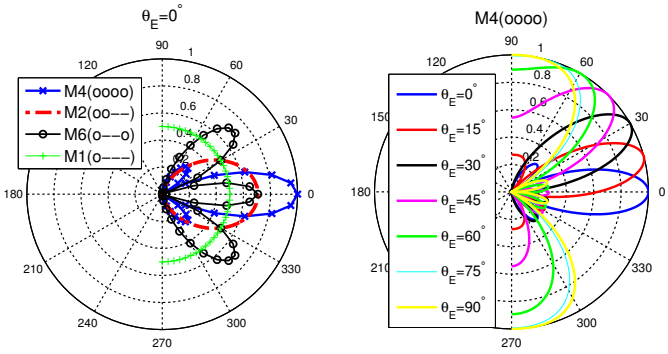
ER is actually a set of positions of which a user's received power is larger than threshold P_{th}. It is assumed that AP's total transmission power P_t is fixed, which is a normal setting in the current 802.11 wireless networks. There are two types of parameters that affect the size of ER, the array configuration (i.e., the number of elements N and their spacing Δd) and DoE angle θ_E. In the following, the impact of these parameters are studied and the configurable beamfomring technique is reviewed.

A. Impact of Array Mode and DoE Angle on ER

The configurable beamforming is based on a selection of antenna array configurations. Take a 4-element array for instance, there are 6 different modes which are numbered from M1 to M6 as shown in Table I. For convenience, each mode is given a symbol using a series of 'o' and '-'.

The impact of array configuration $(N, \Delta d)$ and the DoE angle θ_E is shown in Fig. 2. In the left sub-figure, the DoE angle is fixed to 0°. Different array configurations produce different shapes and sizes of ER. In the right sub-figure, the array configuration is fixed to mode M4, ER is changed according to the DoE angle θ_E.

Combining the factors of array configuration $(N, \Delta d)$ and DoE angle θ_E, the area of ER A is plotted in Fig. 3. For $\theta_E \in [-90^\circ, 90^\circ]$, A is symmetric to $\theta_E = 0^\circ$. So θ_E is shown in the range from 0° to 90°. The ER area in mode M1, i.e., a single element transmitting is denoted by A_0. The area A is normalized to A_0 for convenience. Each dashed curve shows the ratio A/A_0 versus the DoE angle θ_E. The security level is measured by the ER area: the smaller the ER is, the more secure the transmission is. The goal is to minimize the ER by adapting array configuration to DoE angle. Configurable beamforming is a numerical solution to this problem.



(a) Different array mode (b) Different DoE angle

Fig. 2. Impact of array mode and DoE angle

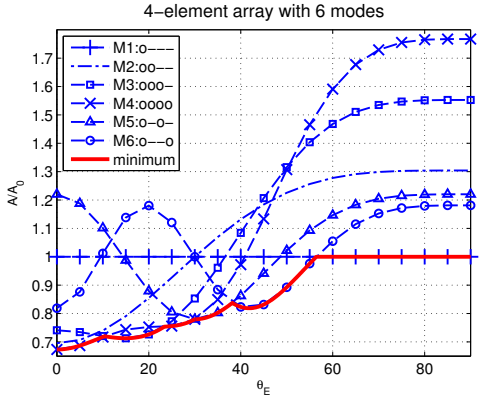


Fig. 3. ER area $A(N, \Delta d, \theta_E)$

B. Configurable Beamforming Technique

For each θ_E, there is at least one $(N, \Delta d)$ that gives the minimum A. For example, at $\theta_E = 50^\circ$, mode M5 gives minimum ER area. In Fig. 3, the minimum value of A/A_0 for each θ_E is shown by a solid curve. A look-up table, shown in Table II, is built based on this minimum line.

It can be observed in Table II that $N = 4$ does not always generate the smallest ER. In general, for small θ_E, array modes with more elements works better. For large θ_E, less number of elements works better.

III. INVESTIGATION OF THE ALGORITHM WITH RAY-TRACING MODEL

In Section II, the algorithm is examined under the assumption that channel is free-space path loss channel, which means there is only line-of-sight (LOS) path. In most real environments, the none-line-of-sight (NLOS) is unavoidable

TABLE II. LOOK-UP TABLE OF $(N, \Delta d)$ AND θ_E

θ_E	$(N, \Delta d/\lambda)$	θ_E	$(N, \Delta d/\lambda)$	θ_E	$(N, \Delta d/\lambda)$
0°	(4,0.5)	25°	(4,0.5)	50°	(2,1.5)
5°	(4,0.5)	30°	(4,0.5),(2,1)	55°	(2,1.5)
10°	(4,0.5)	35°	(2,1)	60°	(1,-)
15°	(3,0.5)	40°	(2,1.5)	65°-90°	(1,-)
20°	(3,0.5)	45°	(2,1.5)		

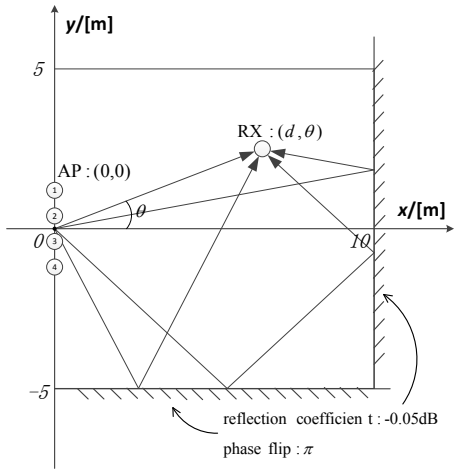


Fig. 4. Ray-tracing model

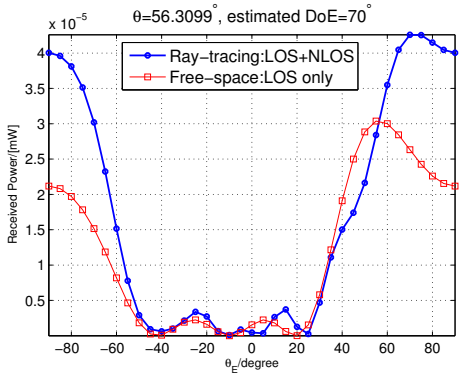


Fig. 5. Received power of Bob for DoE estimation

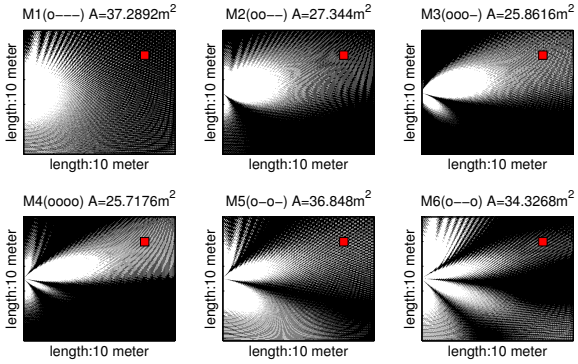


Fig. 6. Example 1: ER for 6 array modes

because of reflection and scattering of signals. In this section, we examine whether the look-up table generated in free-space still applies in a more complicated channel model, such as ray-tracing model which serves as a controllable multipath environment [7].

A. A Simple 2D Ray-Tracing Model

Imagine that two infinitely long metal walls are placed in free space, as shown in Fig 4. One is parallel to x-axis at $x = 10$ and the other to y-axis at $y = -5$. For this particular set-up, there are only three NLOS paths besides LOS path, of which two paths are one-reflection path and one path is two-reflection path. For the purpose of simulation, AP sits at the origin point. The antenna array lies along the y-axis. ~~User~~'s polar coordinate is (d, θ). The path loss obeys free-space path loss model. For LOS path, the distance is d. For NLOS paths, the distance is the total length of the path that a signal travels. At the reflection point, the signal suffers additional loss which is counted by reflection coefficient. In addition, there is a radian of π phase flip for each reflection.

B. DoE Estimation

In practice, ~~AP~~ needs to estimate the best DoE angle to decide an appropriate array mode based on the DoE angle. AP will form a beam using the 4-element array and sweeps the beam at every $5°$ in a range from $-90°$ to $90°$. For each θ_E, the received power of Bob is recorded. The DoE angle that corresponds to the largest received power is chosen as the best DoE angle. In a ray-racing model, the estimated best DoE angle θ_E normally is not ~~the~~ Bob's true angle. In Fig. 5, the received power of Bob during the DoE estimation stage is shown. Bob's coordinates are (2,3). The true angle θ_B is $56.3099°$. In this case, the estimated best DoE θ_E is $70°$.

C. Examples of ER in Ray-Tracing Model

DoE estimation is performed before AP transmits to Bob. Then Bob sends the best DoE angle θ_E back to AP via a feedback channel. AP will use θ_E to generate beamforming weights which are imposed on ~~date~~ streams. The received power is measured across the room for all array modes. The threshold of received power P_{th} which is chosen from the received power for mode M1, so that Bob is within the ER for most cases. The ERs are shown in Fig. 6.

In Fig. 6, the room has a 10×10 m^2 area. The total transmit power P_t is 0 dBm. We use the carrier frequency of 2.4GHz which corresponds to a wavelength of 0.125m. To make sure that the property of ER is fully revealed, we take a measurement every 0.02m. The white area shows the ER where the received power is above P_{th}; in the black area, the received power is below P_{th}. The red square marker indicates Bob's position. Bob's coordinates are $(8, 3)$. Its true angle is $\theta_B = 20.556°$ while the estimated best DoE is $\theta_E = 15°$. Based on the look-up table, mode M4 should give a minimum ER. In Fig. 6, the values of ER area are given for each array mode. The minimum area is 25.7176 m^2 which is given by mode M4. It means that the look-up table successfully gives the best array mode. In the following, we show a complete result where Bob is moved across the room to examine how configurable beamforming technique performs.

D. Configurable Beamforming in Ray-Tracing Model

In theory the look-up table needs to change according to the room environment to give an accurate prediction. However, ~~it's~~ not ~~very~~ practical because the room environment may vary quite constantly. Preferably the look-up table generated in free-space path loss model can serve as an approximation to different environments. To study the applicability of the look-up table generated from a free-space path loss model to a ray-tracing model, Bob is moved to positions across the entire

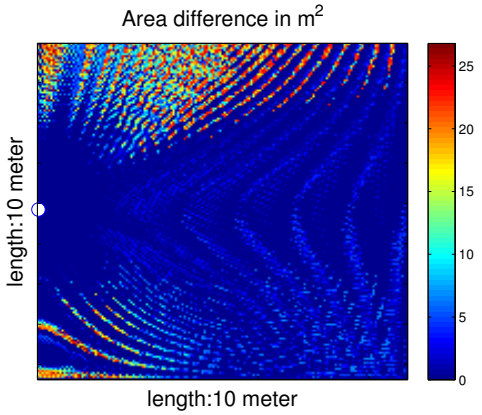


Fig. 7. Area difference ΔA across the room

room. The area difference given by the array mode suggested by the look-up table and the actually mode that gives the minimum ER is denoted by ΔA. As the wavelength is 0.125 m, we take samples of Bob's positions at every 0.06 m. The area difference ΔA is then measured and shown in Fig. 7. The value of the difference is shown by the color. The white circle represents AP's position.

The difference ΔA in a range from 0 to 26.80 m^2. However, for 86.06% of Bob's positions, the difference is less than 5 m^2, which means that the look-up table serves well as an approximation in the ray-tracing model.

IV. Investigation of the Algorithm on WARP

In this section, we will implement the configurable beamforming based on WARP for the purpose of simulating an 802.11n AP. WARP is a soft-defined radio platform based on FPGA [8]. One of its ~~designs~~ is WARPLab which is used to explore physical layer algorithm. The framework of WARPLab ~~is consisted of~~ WARP boards, MATLAB and Ethernet switch. WARP boards can transmit or receive data packets over the air with real-time transmission. The data packets can be downloaded/uploaded from/to MATLAB in PC via switch and processed offline.

In the WARP v3 board, up to 4 radio interfaces are supported. Each one is attached by an omni-directional antenna. The transmitter uses 4 antennas as an array to perform beamforming. Another WARP board, which only uses 1 antenna, serves as the receiver. For our purpose, the 2.4 GHz carrier is sent alone without modulation. Each carrier is weighted to form a beam as a whole in the array. The baseband processing is completed in MATLAB. Then four data streams are downloaded to the transmitter board. Baseband data is converted into RF analog signal in radio interface and sent via the antenna.

A. Transmitter Phase-Offset Calibration

The transmitter needs to be calibrated before beamforming because the phase offsets that are introduced in hardware will distort the carefully calculated beamforming weights, which in turn affects the beam formed over the air. In each radio interface, a MAXIM MAX2829 chip translates between baseband and RF. Although the four radio interfaces share a reference clock to generate the carrier, each phase-lock loop (PLL) unit settles at a slightly different time which cause a relative phase shift to each other. But these phase offsets will stay the same if the PLL is not re-tuned [9].

Taking RF1 as phase reference, the relative phase offsets on RF2, RF3 and RF4 are denoted by $\Delta\theta_1$ $\Delta\theta_2$ and $\Delta\theta_3$. The carrier frequency is denoted by w. Before transmitting any data, the phase offsets need to be calibrated. Then the estimated phase offsets are then compensated in the next transmission.

First, we use RF1 and RF2 as an example to show how to ~~calibration~~ between 2 radio interfaces. Imagine there is a receive antenna at the same distance away from RF1 and RF2. The reason for it is to avoid extra phase propagation delay when measuring $\Delta\theta_1$.

We introduce a phase sweeping function $\phi(t) = 2\pi\frac{t}{T}, t \in [0, T]$ to RF2 data stream, where T is one packet duration. Then the transmitted signals from RF1 and RF2 are

$$x_1(t) = e^{jwt},\ x_2(t) = e^{jwt+\Delta\theta_1+\phi(t)}. \tag{1}$$

Assume that the receiver's carrier signal is $e^{-j(wt-\Delta\theta_R)}$. Then the received signal is

$$y(t) = x_1(t) + x_2(t) = e^{j\Delta\theta_R}(1 + e^{j(\Delta\theta_1+\phi(t))}) \tag{2}$$

Regardless of the term $e^{j\Delta\theta_R}$, when $\Delta\theta_1 + \phi(t_0) = \pi$, $|y(t)|$ has the minimum value. Thus, we solve t_0 that gives $|y(t)|$ the minimum value first, then solve $\Delta\theta_1 = \pi - \phi(t_0)$.

For a 4-element linear array, we divide the antennas into 3 groups. For the above method to work, a receive antenna of the same distance away from the 2 transmit antennas is needed. Therefore, we ~~make RF1 and RF3 in one group~~ and use RF2 as receiver to calibrate $\Delta\theta_2$. Similarly, RF2 and RF4 are ~~in a group~~ and RF3 is used to calibrate $\Delta\theta_3 - \Delta\theta_1$. It is more difficult to calibrate $\Delta\theta_3$ between RF1 and RF4 because neither RF2 nor RF3 fits the requirement of the receiver.

When RF2 (or RF3) receives from RF1 and RF4, there is an additional phase offset $\Delta\theta_p$ between the received signals from RF1 and RF4 due to unequal propagation distance. The transmitted signals from RF1 and RF4 are

$$x_1(t) = e^{jwt},\ x_4(t) = e^{jwt+\Delta\theta_3+\phi(t)}. \tag{3}$$

The received signals are

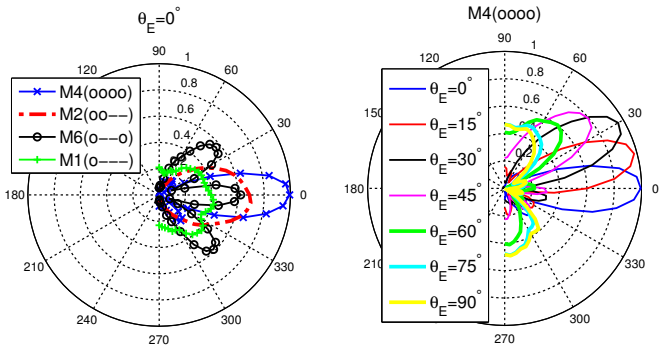
$$y_2(t) = x_1(t)e^{-j\Delta\theta_p} + x_2(t) \tag{4}$$

$$y_3(t) = x_1(t) + x_2(t)e^{-j\Delta\theta_p} \tag{5}$$

Two unknowns $\Delta\theta_3$ and $\Delta\theta_p$ can be solved in a similar way by combining $y_2(t)$ and $y_3(t)$.

B. Measurements of Array Pattern in Anechoic Chamber

Anechoic chamber ~~simulates~~ a free space environment. After transmitter calibration, array patterns of different array modes shown in Table I are then measured. The total transmit power is set to a fixed value by giving the same values of amplifier gains on WARP board. The received power is measured in mW. The measurements are taken every 5° from -90° to 90°. Then the array patterns are plotted in Fig. 8. For



(a) Different array mode (b) Different DoE angle

Fig. 8. Impact of array mode and DoE angle in experiment

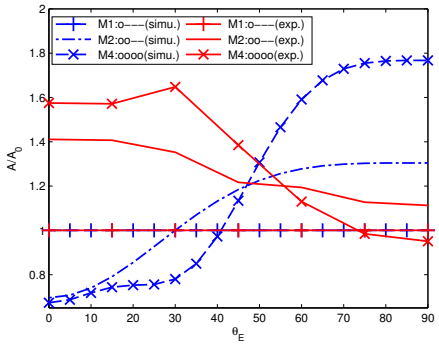


Fig. 9. Array patterns of different array modes in simulation and experiment

all measurements, the maximum received power is normalized to one.

In comparison to Fig. 2, Fig. 8 shows array patterns for different array modes and DoE angles measured in the experiment. For the left sub-figure, the DoE angle is $0°$. The yellow line with plus sign marker shows the pattern of a single element in the array when 3 other elements are silent. It can be seen that the pattern is not circle. The received power at $0°$ is about 0.4, which is almost twice than the received power at $90°$ which is roughly 0.2. This is caused by active element pattern phenomenon which is basically coupling between close antennas (here reference). In addition, the imperfection of the omni-directional antenna causes the fluctuations to the circle.

Due to active element pattern phenomenon and antenna imperfection, the array patterns shown in Fig. 8 are affected to a different extent. In the left ~~sub-~~figure, it can be seen that array mode with less number of antennas ~~are~~ affected more. Antenna pattern of mode M4 looks more symmetric and closer to the simulated pattern. In the right sub-figure, it can be seen that the directivity and gain become worse as θ_E get closer to $90°$, while for $\theta_E < 30°$, the beam has a good directivity.

C. ER Analysis

For all 6 array modes, the DoE angle in a range from $0°$ to $90°$ at every $15°$ are measured. Based on the measurements, the coverage area for each mode with a certain DoE angle can be calculated numerically. The results are plotted in Fig. 9.

Compare the experiment result with simulation result in Fig. 9, it can be seen that in general, as θ_E gets further away from $0°$, ER area A decreases instead of increasing. At $\theta_E = 0°$, $N = 4$ gives the largest area because less number of antennas suffer bigger loss of coverage area In all, active element pattern and imperfect antenna impact the effectiveness of the configurable beamforming Technique.

V. Conclusions

In this work, configurable beamforming technique has been investigated using a ray tracing model in simulation and a real implementation using WARP in an anechoic chamber. The look-up table created in free-space environment works well in a ray-tracing model. For the WARP implementation, there is a clear impact of active element pattern and antenna imperfection. There is still good directivity with angles less then $\pm 30°$, while there is considerable distortion outside this range. Furthermore, the impact is less for large number of antennas.

For future work, it is possible to use multiple arrays to overcome the insufficiency of the current implementation. Furthermore, ~~with the fact~~ that large number antenna array is less impacted, the algorithm has a potentially better performance in ~~M~~assive MIMO system.

Acknowledgment

The authors gratefully acknowledge support from the US-Ireland R&D Partnership USI033 'WiPhyLoc8' grant involving Rice University (USA), University College Dublin (Ireland) and Queens University Belfast (N. Ireland).

References

[1] S. Lakshmanan, C. Tsao, R. Sivakumar, and K. Sundaresan, "Securing wireless data networks against eavesdropping using smart antennas," in *Proc. of The 28th International Conference on Distributed Computing Systems(ICDCS)*, Beijing, China, Jun. 2008, pp. 19–27.

[2] S. Lakshmanan, C. Tsao, and R. Sivakumar, "Aegis: Physical space security for wireless networks with smart antennas," *IEEE/ACM Trans. Netw.*, vol. 18, pp. 1105–1118, Aug. 2010.

[3] J. Carey and D. Grunwald, "Enhancing wlan security with smart antennas: a physical layer response for information assurance," in *Proc. of IEEE 60th Vehicular Technology Conference(VTC)*, Los Angeles, CA, USA, Sep. 2004, pp. 318–320.

[4] T. Wang and Y. Yang, "Enhancing wireless communication privacy with artificial fading," in *Proc. of IEEE 9th International Conference on Mobile Adhoc and Sensor Systems(MASS)*, Las Vegas, Nevada, USA, Oct. 2012, pp. 173–181.

[5] N. Darmian, H. Oskoei, and B. Vazirnezhad, "Proposing a hybrid protocol for secure wireless networks based on signcryption scheme," in *Proc. of World Congress on Computer and Information Technology(WCCIT)*, Sousse, Tunisia, Jun. 2013, pp. 1–6.

[6] Y. Zhang, A. Marshall, R. Woods, and Y. Ko, "Creating secure wireless regions using configurable beamforming," in *Proc. of IEEE 25th International Symposium on Personal, Indoor and Mobile Radio Communications(PIMRC)*, Washington, USA, Sep. 2014.

[7] R. Valenzuela, "A ray tracing approach to predicting indoor wireless transmission," in *Proc. of IEEE 43rd Vehicular Technology Conference(VTC)*, Secaucus, New Jersey, May 1993, pp. 214–218.

[8] "WARP project." http://warpproject.org

[9] P. Murphy, "Design, implementation and characterization of a cooperative communications system," Ph.D. dissertation, Rice University, 2010.