Queen's University
Belfast

Creating secure wireless regions using configurable beamforming

Document Version:
Peer reviewed version

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

Creating Secure Wireless Regions using Configurable Beamforming

Yuanrui Zhang*, Alan Marshall§, Roger Woods*, Youngwook Ko*

* ECIT, Queen's University Belfast
Belfast, UK
Email: {yzhang31, r.woods, y.ko}@qub.ac.uk
§ Electrical Engineering and Electronics, University of Liverpool
Liverpool, UK
Email: Alan.Marshall@liverpool.ac.uk

Abstract—We present a novel approach to network security against passive eavesdroppers by employing a configurable beamforming technique to create tightly defined regions of coverage for targeted users. In contrast to conventional encryption methods, our security scheme is developed at the physical layer by configuring antenna array beam patterns to transmit the data to specific regions. It is shown that this technique can effectively reduce vulnerability of the physical regions to eavesdropping by adapting the antenna configuration according to the intended user's channel state information. In this paper we present the application of our concept to 802.11n networks where an antenna array is employed at the access point, and consider the issue of minimizing the coverage area of the region surrounding the targeted user. A metric termed the exposure region is formally defined and used to evaluate the level of security offered by this technique. A range of antenna array configurations are examined through analysis and simulation, and these are subsequently used to obtain the optimum array configuration for a user traversing a coverage area.

Keywords—Beamforming, exposure region(ER), IEEE 802.11n, wireless security

I. INTRODUCTION

Recent wireless communication systems require significantly high secrecy and privacy for transmission techniques. The vast amount of connectivity between millions of user devices and access points, where sensitive data is exchanged, requires more protection than ever before. Conventional encryption-based security has many limitations when used in wireless networks. For example, current techniques used in the 802.11 protocols such as WEP and WPA, are vulnerable to many practical attacks [1]. As most conventional security methods are designed to operate in layers other than the physical layer, extra physical layer security will act as a complementary approach to conventional encryption methods. In this paper, we look at physical space security which is in the scope of physical layer security.

A key threat in securing wireless networks is based around the broadcast nature of radio transmissions. In a typical indoor environment, a message sent to a legitimate user will be exposed to any potential eavesdropper who is within range. The principle of physical space security is to hide the knowledge of the existence of the message from the eavesdropper rather than encrypting the contents of the message from the eavesdropper [2], [3].

In this context, *beamforming* can be used to restrict the eavesdroppers' access to the signals [2]–[6]. Beamforming is traditionally used to optimize the system performance such as data rate, reliability, range, etc. But here it is used to enhance the signal strength by steering beams in the direction of intended users, whilst suppressing the signal strength in other directions by placing nulls thereby limiting the eavesdroppers' signal strength.

In this paper, we develop a configurable beamforming technique to limit the eavesdropper's ability to access the signals, by adaptively changing the antenna configuration based on the intended user's channel state information (CSI). The CSI availability at the transmitter can be realized by a feedback channel through which the estimated channel information is sent back to the transmitter from the intended user. For indoor environments, channel conditions vary greatly for different scenarios. For a typical indoor environment, the human walking speed is very low, e.g. 1 m/s, resulting in a Doppler frequency shift of just a few Hz, which has been shown in [7]; thus the channel is assumed to be static during the packet transmission time [2]. In this paper, it is also assumed that the frequency-selective fading is solved by orthogonal frequency division multiplexing (OFDM) incorporated in the 802.11 protocols [2], [3]. Under these assumptions, the receiver's CSI mainly depends on the location. For example, in a log-distance channel model, the path loss depends on the distance between the transmitter and the receiver and other environment-related parameters. This allows the transmitter to adapt to the channel based on the location of the intended user per packet transmission. From now on, we assume that the transmitter is aware of the location of the intended user.

For a typical indoor scenario, Alice is the sender who wishes to send a message to the intended receiver Bob and Eve is a passive eavesdropper who listens to the channel and attempts to overhear the message. In the context of an 802.11n network, the access point (AP) equipped with an antenna array acts as Alice. The downlink transmission from Alice to Bob is to be protected, as shown in Fig. 1. Beamforming is used to create a secure space around Bob, thus preventing Eve from intercepting the signals if Eve is not inside the area. In [2], a metric called exposure region (ER) was introduced to refer the area within which an eavesdropper can access and decode the signals being transmitted. However, an approximation model to calculate the ER in [2] does not always reflect the true area,
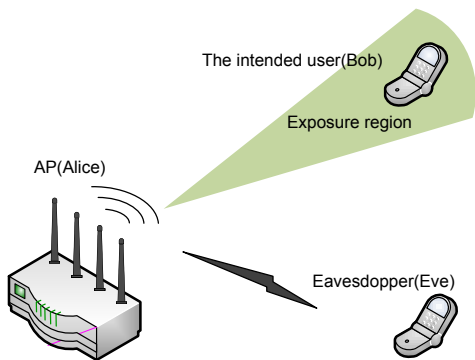
Fig. 1. A three-party communication model: Alice, Bob and Eve. The shadow area surrounding Bob illustrates the ER.

as will be shown in Section V.

In this paper, we aim to minimize the ER based on the received power that Bob can obtain being greater than or equal to a target level. The received power of Bob can be adjusted using beamforming with CSI at the transmitter. However, the AP does not have knowledge of Eve, or of her CSI, thus Eve could be located within the ER. In order to decrease the possibility of Eve being able to receive the signal correctly, the ER should be minimized. Our main contributions are:

- A more formal definition of ER with mathematical expression which provides insights of the impacts of related parameters including Bob's location and the array configuration.

- Formulation of the security problem about how to achieve the minimum ER given Bob's location.

- With analysis on the impacts of the parameters and knowledge of Bob's location, a configurable beam-forming technique is proposed which allows the AP to set the most appropriate configurations, i.e., number of antenna elements and their spacing, such that the ER is minimized in order to increase the level of security offered.

- A new metric called the *effective angle range* (EAR) within which the intended user can benefit from an antenna array achieving a smaller ER than an omni-directional antenna. By using the configurable beam-forming technique, the EAR is widened.

One benefit of this approach is that it can be realized using a single AP, thus it neither requires the coordination of multiple APs thus avoiding special placement of the APs [2], [3], [8] or synchronization of multiple APs across the network [4].

The rest of the paper is organized as follows. Related work on physical space security is discussed in Section II and the differences from our work are stated. Then a more formal definition of the ER is developed and the problem description based on the definition is given in Section III. In Section IV, the system model is introduced and a refinement of the problem formulation is brought up based on our system model. The analysis on the system parameters is given in Section V and the configurable beamforming technique is developed in Section VI. In Section VII, simulation shows

how the configurable beamforming technique works. Finally, the conclusions and future work are given in Section VIII.

II. RELATED WORK

The idea of isolating a physical secure region with beam-forming was first proposed in [4]. However, the concept of physical space security as well as the metric ER was first raised in [2], [3]. In [4], the eavesdroppers' ability to access the signals is limited by using multiple APs to transmit a complete packet in a time-division manner. In [2], [3] three strategies were proposed to reduce the ER with a group of arrays and a central controller is used to coordinate the group of arrays. Each array carries a different task, either beamforming or jamming for different strategies. In [6], a hybrid protocol with a public key encryption system was proposed based on the work presented in [3]. The work in [5] focuses on creating a fast-fading effect with a double-beam switching process on a single AP to minimize the coverage area.

Instead of using beamforming, directional antennas were utilized to achieve the spatial filtering effect of beamform-ing [8], [9]. In [8], the idea proposed in [4] is realized by deploying multiple APs to designated space sectors. The authors in [9] have used directional antennas on both the AP and the mobile user to obtain a minimum coverage area.

While the approaches in [2]–[4], [6], [8] focus on the collaboration of multiple antenna arrays, our approach uses beamforming on a single AP, which avoids a central controller or modifications to the 802.11 protocols. Furthermore, there are no special design requirements such as a public key encryp-tion system and a special deployment of arrays. Our approach minimizes the ER based on variable parameters including the intended user's location and the array configuration whereas in [5] the optimization of the predicted coverage area is investigated regardless of the intended user's various locations. In addition, while the calculation of the ER in [2], [3] is based on an approximate geometric model, a more formal definition in our paper by mathematical expression can provide better insights into the system.

III. PHYSICAL SPACE SECURITY PROBLEM DESCRIPTION

In the three-party communication model shown in Fig. 1, the AP intends to communicate with Bob in the presence of Eve. The AP is equipped with an antenna array, whilst it is assumed that mobile devices only have a single antenna which is the common setting in mobile phones. The downlink trans-missions from Alice to Bob and Eve experience a multiple-input-single-output (MISO) channel.

According to work in [2], [3], we define the ER as an area where a general receiver has a received power above a certain threshold power denoted by P_{th}. Here, we treat Eve as a general receiver, because the AP is not aware of Eve's location. P_{th} can represent the level of the receiver sensitivity, above which the receiver can correctly decode the signal being transmitted. Let P_{rB} and P_r denote the received power of Bob and Eve, respectively. Then, the ER can be defined as

$$E = \{p | P_r \geq P_{th}\}, \qquad (1)$$

where p denotes the location information of Eve. The security level of the system can be evaluated by the area of the ER,
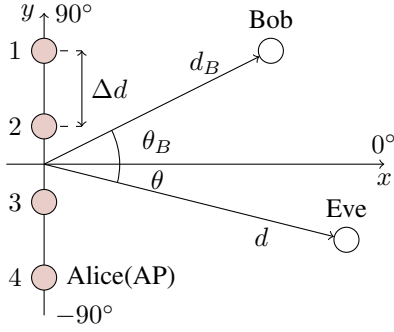
Fig. 2. System model: an AP with a ULA on Y-axis with $N = 4$ elements and Δd spacing, Bob's and Eve's coordinates are (d_B, θ_B) and (d, θ), respectively

which is denoted by $A = area(E)$. With Bob's location p_B known at the AP, beamforming is used to focus the energy on Bob. Thus, the area A is affected by Bob's location p_B.

However, it is not feasible to suppress the transmitted energy at Eve's location as Eve can be randomly located. To lower the chance that Eve is inside the ER, the ER should be minimized. The goal is to minimize the area of the ER A according to Bob's location p_B on the condition that Bob's received power P_{rB} must be guaranteed to be above the threshold power P_{th}. Thus, the problem can be posed as follows.

$$\min A(p_B)$$
$$\text{s.t. } P_{rB}(p_B) \geq P_{th} \qquad (2)$$

IV. SYSTEM MODEL

The system model is shown in Fig. 2. We use a uniform linear array (ULA) that contains a line of N antenna elements with an equal spacing of Δd. The elements of ULA as well as the receive antennas are assumed to be omni-directional. It is of interest to study the beamforming in a 2-D plane. Let Bob's location be denoted by $p_B = (d_B, \theta_B)$ and Eve's location be $p = (d, \theta)$; the values d_B and d are the distances from the AP to Bob and Eve, respectively; θ_B and θ are the angles for Bob and Eve. In order to match the angles with polar coordinates, the ULA is placed on the Y-axis with its middle point at the origin point. As the AP is normally mounted on a wall, we therefore study the angle range from $-90°$ to $90°$.

A. Channel Model

The pass loss models used in the ITU indoor propagation model [10] and the TGn channel model [11] are based on the log-distance path loss model. Since log-distance path loss models are based on the free-space path loss model, we begin with the free-space path loss model to demonstrate the effect of the configurable beamforming technique for simpler mathematical modeling. The free-space path loss (dB) is given by

$$PL(d) = 20\log(4\pi d/\lambda). \qquad (3)$$

where λ is the wavelength of the carrier signal. For example, in 802.11n standard, a carrier with a frequency of 2.4 GHz has a wavelength of 0.125 m.

For a $N \times 1$ MISO channel, the channel gain vectors for Bob and Eve are denoted by $\mathbf{h} = [h_1, h_2, \ldots, h_N]$ and $\mathbf{g} = [g_1, g_2, \ldots, g_N]$, of which each element is a channel gain denoted by h_i or g_i, $i \in [1, 2, \ldots, N]$ and is composed of two parts, an amplitude attenuation and a phase shift due to the propagation delay. Since the path loss in (3) is the power attenuation in logarithm scale, so the amplitude is $L(d) = 10^{-PL(d)/20}$. For example, g_i can be written as

$$g_i = L(d_i)e^{j\phi_i} = \frac{\lambda}{4\pi d_i}e^{j\phi_i}, \qquad (4)$$

where d_i is the distance between the ith antenna element and the receiver's antenna and ϕ_i is the phase shift. h_i can be given in a similar way.

The distances d_B and d are normally regarded as far larger than the array spacing, e.g. $\Delta d = 0.5\lambda$. So the distances between different antenna elements and the receiver's antenna can be considered as the same. In this case, the absolute phase shift of each channel gain does not matter. The relative phase shift $(-2\pi\Delta d \sin\theta/\lambda)$ between adjacent elements will decide how different waves are added at an angle of θ [12]. Let the first element in the array be the reference element as labeled in Fig. 2. The channel gains h_i and g_i are written as follows.

$$h_i = \frac{\lambda}{4\pi d_B}e^{-j2\pi(i-1)\Delta d\sin\theta_B/\lambda} \qquad (5)$$

$$g_i = \frac{\lambda}{4\pi d}e^{-j2\pi(i-1)\Delta d\sin\theta/\lambda} \qquad (6)$$

B. Refinement on Problem Formulation

The transmitted signal vector $\mathbf{s} = \mathbf{w} \cdot x$, where x is the modulated symbol with unit power and $\mathbf{w}$ is the beamforming weight vector. The AP performs transmit beamforming, so $\mathbf{w} = \mathbf{h}^\dagger/||\mathbf{h}||$. $\mathbf{h}^\dagger$ denotes the conjugate transpose of $\mathbf{h}$ and $||\mathbf{h}||$ is the norm of $\mathbf{h}$. Let P_t be the transmit power that is assumed to be constant and set to an appropriate value according to specific network plannings. Let n be the zero-mean additive white Gaussian noise. The noise variance is given according to room environment. In order to guarantee a minimum received SNR, P_{th} is set according to the noise n.

The received signals of Bob and Eve are

$$r_B = \sqrt{P_t}(\mathbf{h} \cdot \mathbf{w})x + n = \sqrt{P_t}||\mathbf{h}||x + n, \qquad (7)$$

$$r = \sqrt{P_t}(\mathbf{g} \cdot \mathbf{w})x + n = \sqrt{P_t}(\mathbf{g}\mathbf{h}^\dagger/||\mathbf{h}||)x + n. \qquad (8)$$

The received signal power of Bob and Eve are

$$P_{rB} = P_t||\mathbf{h}||^2 = NP_t\left(\frac{\lambda}{4\pi d_B}\right)^2, \qquad (9)$$

$$P_r = P_t|\mathbf{g}\mathbf{h}^\dagger|^2/||\mathbf{h}||^2 = P_t\left(\frac{\lambda}{4\pi d}\right)^2\frac{1 - \cos(N\phi)}{N(1 - \cos\phi)}, \qquad (10)$$

where $\phi = 2\pi\Delta d(\sin\theta_B - \sin\theta)/\lambda$.

It was demonstrated in Fig. 2 as well as the mathematical expressions in (9) and (10) that there are two types of parameters, Bob's location (d_B, θ_B) and the array configuration $(N, \Delta d)$. In our system, Bob's location is known at the AP, therefore, only the array configuration $(N, \Delta d)$ is adjustable. In addition, according to (9), P_{rB} does not depend on θ_B

and Δd; according to (10), P_r does not depend on d_B. In other words, the ER is determined by $(\theta_B, N, \Delta d)$ and P_{rB} is determined by (d_B, N).

It is worth noting that N should not exceed the maximum number of antenna elements N_{max}. Although there is no restraint on Δd, it is normally no less than 0.5λ and takes an integer multiple of 0.5λ. Therefore, the problem can be re-formulated as follows from (2).

$$\min_{N,\Delta d} A(\theta_B, N, \Delta d)$$

$$\text{s.t.} \quad \frac{P_{th}}{P_t}\left(\frac{4\pi d_B}{\lambda}\right)^2 \leq N \leq N_{max}$$

$$\text{and} \quad \frac{1}{2}\lambda \leq \Delta d \leq \frac{N_{max}-1}{2}\lambda \quad (11)$$

V. ER ANALYSIS

In this section, we study the impacts of the parameters mentioned in (11). To begin with, P_r in the ER expression in (1) is substituted by (10).

$$E(\theta_B, N, \Delta d) =$$
$$\left\{(d,\theta)|P_t\left(\frac{\lambda}{4\pi d}\right)^2 \frac{1-\cos[N\phi(\theta,\theta_B,\Delta d)]}{N[1-\cos\phi(\theta,\theta_B,\Delta d)]} > P_{th}\right\}, \quad (12)$$

where $\phi(\theta, \theta_B, \Delta d) = 2\pi\Delta d(\sin\theta_B - \sin\theta)/\lambda$.

The ER of an antenna array is similar to the array pattern, except that path loss is incorporated in the ER. It is enclosed by a boundary $D(\theta, \theta_B, N, \Delta d)$. From the inequality in (12), we can derive

$$D(\theta, \theta_B, N, \Delta d) = \sqrt{\left(\frac{\lambda}{4\pi}\right)^2 \frac{P_t}{P_{th}} \frac{1-\cos[N\phi(\theta,\theta_B,\Delta d)]}{N[1-\cos\phi(\theta,\theta_B,\Delta d)]}}. \quad (13)$$

The area of a circular sector with a radius of a and a central angle of Θ is $\frac{1}{2}a^2\Theta$. The ER can be divided into an infinite number of infinitely narrow sectors. Thus, the area A can be calculated by the following integral.

$$A(\theta_B, N, \Delta d) = \int_{-\pi/2}^{\pi/2} \frac{1}{2} D(\theta, \theta_B, N, \Delta d)^2 \, d\theta$$

$$= \frac{1}{2}\left(\frac{\lambda}{4\pi}\right)^2 \frac{P_t}{P_{th}} \int_{-\pi/2}^{\pi/2} \frac{1-\cos[N\phi(\theta,\theta_B,\Delta d)]}{N[1-\cos\phi(\theta,\theta_B,\Delta d)]} \, d\theta \quad (14)$$

Whilst there is no analytical solution for this integral, it can be calculated numerically. It is easy to obtain that d_B does not affect A from (14) and that the lower bound of N is proportional to d_B^2 from (11). In the following, we will only investigate the impacts of θ_B and $(N, \Delta d)$ on A.

A. Impact of θ_B

In order to study the impact of θ_B, the other parameters are fixed. Examples of the ER are plotted for $\theta_B = 0°, 30°, 60°$ in Fig. 3. The transmit power is $P_t = 10\,\text{dBm}$, which is set according to commonly used commercial products and the threshold power is $P_{th} = -80\,\text{dBm}$. For example, if the noise variance is $-100\,\text{dBm}$, the minimum signal-to-noise ratio in
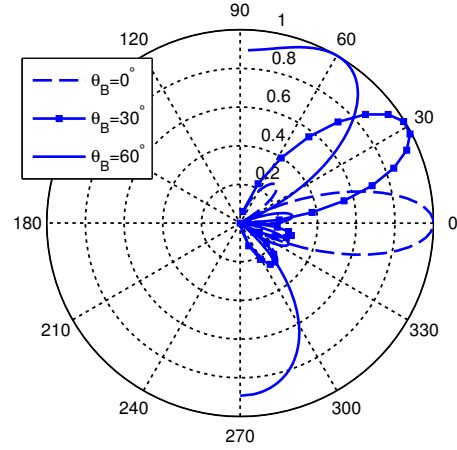

Fig. 3. ERs for different θ_B. Other parameters are $P_t = 10\,\text{dBm}$, $P_{th} = -80\,\text{dBm}$, $N = 4$ and $\Delta d = 0.5\lambda$

the ER is 20 dB. $(N = 4, \Delta d = 0.5\lambda)$ is used for the antenna configuration. In Fig. 3, the maximum coverage distance is normalized to one. Similar to the array pattern, the shape of the ER varies as θ_B increases from $0°$ to $90°$. For example, when θ_B is $60°$, the side lobe is too large to be ignored. Thus, the approximation used in [2], [3] does not always reflect the true area.

In this paper, A is normalized to A_0 for the purpose of comparing the antenna array with an omni-directional antenna in terms of security. A_0 is the area of the ER when only one element in the array is transmitting. For a fair comparison, other parameters are the same for calculating A and A_0. Moreover, A_0 is fixed if P_t is a fixed value. Due to the symmetry of the antenna array, we only show the results for θ_B from $0°$ to $90°$. The ratio for the entire range from $0°$ to $360°$ can be obtained in the same way.

The curve in Fig. 4 shows two things. First, the area A changes as Bob moves around. Second, when $\theta_B > 41°$, the ER of an antenna array is larger than that of an omni-directional antenna. The EAR is defined as the angle range where the ratio is less than one, which indicates where the antenna array outperforms an omni-directional antenna in terms of security. In Fig. 4, the EAR is from $0°$ to $41°$.

B. Impact of $(N, \Delta d)$

For fixed $(N, \Delta d)$, A changes with θ_B according to Section V-A. For a fixed θ_B, A also changes with different $(N, \Delta d)$ combinations as shown in Fig. 5. The parameters used are $\theta_B = 0°$, $P_t = 10\,\text{dBm}$, and $P_{th} = -80\,\text{dBm}$. The maximum coverage distance is normalized to one. By comparing different N for the same Δd or comparing different Δd for the same N, the variations in the ER over a range of these parameters can be obtained. However, there is no obvious solution in deciding which $(N, \Delta d)$ is optimal. In Section VI, we will propose an algorithm to deal with this problem.

VI. THE CONFIGURABLE BEAMFORMING TECHNIQUE

For an array with a maximum number N_{max} of elements and Δd_{min} spacing, there are many possible $(N, \Delta d)$ com-
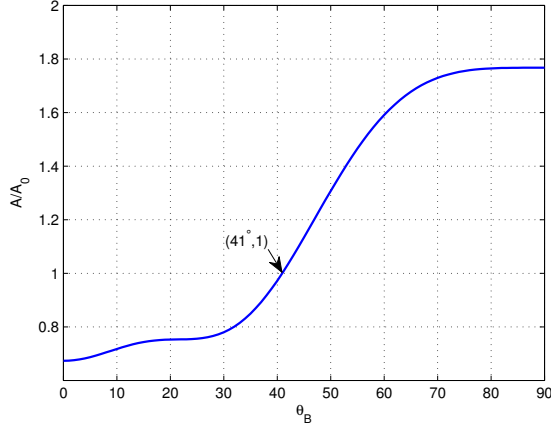
Fig. 4. Impact of θ_B on A/A_0. Other parameters are $P_t = 10\,\text{dBm}$, $P_{th} = -80\,\text{dBm}$, $N = 4$ and $\Delta d = 0.5\lambda$
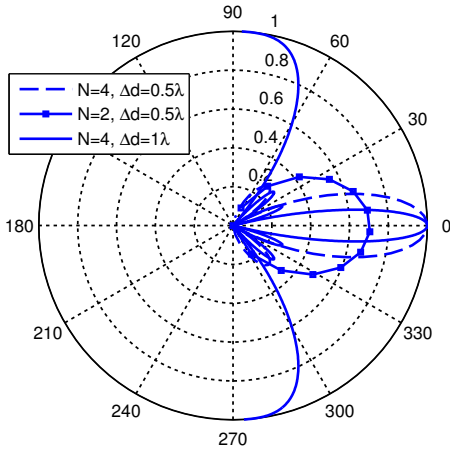

Fig. 5. ERs for different $(N, \Delta d)$. Other parameters are $\theta_B = 0°$, $P_t = 10\,\text{dBm}$, $P_{th} = -80\,\text{dBm}$

binations. There must exist at least one $(N, \Delta d)$ combination for given (d_B, θ_B), which gives the optimal solution for (11). In order to find the optimum $(N, \Delta d)$, we will build a look-up table T based on (d_B, θ_B) for practical use rather than obtaining the best solution by taking the derivative of $A(\theta_B, N, \Delta d)$. The algorithm is shown below. First, a table T_0 containing all possible $(N, \Delta d)$ is required. Then we need to divide the space into sectors by choosing an appropriate angle resolution of α (line 1-2) and find the optimum $(N, \Delta d)$ for each sector (line 3-21). We consider scenarios such as when P_t is not large enough or Bob is too far away. In these cases, AP may need more than one antenna to increase P_{rB} (line 7-11). However, we assume that Bob is within the coverage range of the AP, i.e., the AP can always cover Bob's location by using an appropriate array configuration.

Require: A configuration table T_0 with L possible $(N, \Delta d)$
1: Assign a valid value in radian to α
2: $M \leftarrow \lceil \frac{\pi}{2\alpha} \rceil$
3: Create an empty table T with $2\times(2M+1)$ cells
4: **for** $i = -M$ **to** M **do**
5:      **if** $-\frac{\pi}{2} \leq i\alpha \leq \frac{\pi}{2}$ **then**

TABLE I.   A CONFIGURATION TABLE T_0 FOR A 4-ELEMENT ANTENNA ARRAY WITH 0.5λ SPACING.

No.	1	2	3	4	5	6
$(N, \Delta d/\lambda)$	(1,-)	(2,0.5)	(3,0.5)	(4,0.5)	(2,1)	(2,1.5)

6:          Create an index vector $\mathbf{u} = [1, 2, \ldots, L]$
7:          **for** $j = 1$ **to** L **do**
8:              **if** $P_{rB}(d_B, T_0(j)) < P_{th}$ **then**
9:                  Delete the jth element from $\mathbf{u}$
10:             **end if**
11:         **end for**
12:         $K \leftarrow$ No. of elements of $\mathbf{u}$
13:         Create an all-zero vector $\mathbf{v}$ with a length of K
14:         **for** $k = 1$ **to** K **do**
15:             $\mathbf{v}(k) \leftarrow A(i\alpha, T_0(\mathbf{u}(k)))$
16:         **end for**
17:         Find idx that corresponds to $\min \mathbf{v}$
18:         $T(1, i) \leftarrow i\alpha$
19:         $T(2, i) \leftarrow T_0(\mathbf{u}(idx))$
20:     **end if**
21: **end for**

For a given (d_B, θ_B), the AP chooses the most closely matched cell in T and uses the corresponding $(N, \Delta d)$. The chosen N elements are used and the rest remain silent. In practice, the AP could scan the room and update the look-up table to adapt to Bob's location. A smaller α will give more accurate result, but require more measurements, which will increase the implementation complexity in the AP as well as the processing time.

VII. SIMULATIONS

In this section, we present simulation results to illustrate how the configurable beamforming technique in Section VI works. In order to show all $(N, \Delta d)$ combinations, we consider a scenario where Bob is inside the coverage range of the AP even when the AP uses an omni-directional antenna. Therefore, N can take any integer value between 1 and N_{max} in (11).

The AP is equipped with a 4-element antenna array ($N_{max} = 4$) with an equal spacing of 0.5λ ($\Delta d_{min} = 0.5\lambda$). Possible combinations are listed in the configuration table T_0, as shown in Table I. There are two types of combinations. One is to increase N from 2 to 4 while keeping $\Delta d = 0.5\lambda$. The other kind is to increase Δd from 0.5λ to 1.5λ while keeping $N = 2$. For N_{max} is 4, there exists no intermediate combinations such as ($N = 3$, $\Delta d = 1\lambda$). However, when N_{max} is increased, various combinations will appear. In addition, there is one cell in T_0 for the omni-directional antenna case.

For this simulation, the carrier frequency is $2.4\,\text{GHz}$, so the wavelength λ is $0.125\,\text{m}$. The transmit power is $P_t = 10\,\text{dBm}$ and the threshold power is $P_{th} = -80\,\text{dBm}$. The area of the ER when the AP transmits with only one antenna is denoted by A_0. Because P_t is fixed, A_0 is constant. For a comparison with an omni-directional antenna, the ratio of A to A_0 is used.

Fig. 6 shows the ratio of A to A_0 for six $(N, \Delta d)$ combinations that correspond to T_0. Each dashed curve corresponds to one particular antenna configuration. For different antenna configuration $(N, \Delta d)$, the ratio A/A_0 varies with θ_B differently.
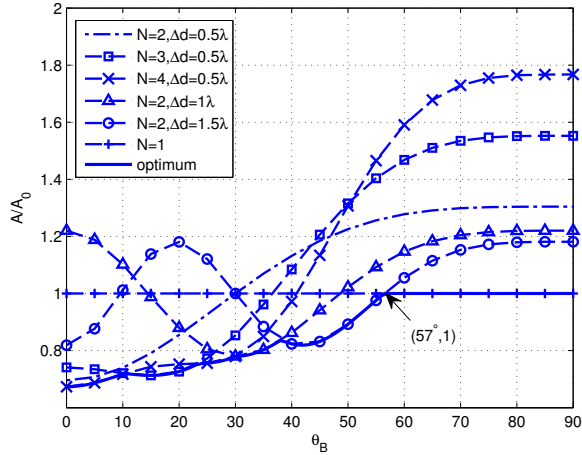
Fig. 6. A versus θ_W for different $(N, \Delta d)$ combinations.

TABLE II.   A LOOK-UP TABLE T

θ_B	$(N, \Delta d/\lambda)$	θ_B	$(N, \Delta d/\lambda)$	θ_B	$(N, \Delta d/\lambda)$
0°	(4,0.5)	35°	(2,1)	70°	(1,-)
5°	(4,0.5)	40°	(2,1.5)	75°	(1,-)
10°	(4,0.5)	45°	(2,1.5)	80°	(1,-)
15°	(3,0.5)	50°	(2,1.5)	85°	(1,-)
20°	(3,0.5)	55°	(2,1.5)	90°	(1,-)
25°	(4,0.5)	60°	(1,-)		
30°	(4,0.5),(2,1)	65°	(1,-)		

The angle resolution α is set to $5°$. The calculations are to be done for $\theta_B \in [0°, 5°, 10°, \ldots, 90°]$. For each angle, there are six values of A/A_0. The minimum value is chosen and the corresponding $(N, \Delta d)$ is recorded in the look-up table T in Table II. The optimum solution is shown by the solid curve in Fig. 6. Based on Bob's angle, the most closely matched cell in T is chosen, which will give a minimum ER. The chosen antenna elements are used to transmit signals while the others stay silent. For example, when Bob's angle is $18.5°$, the best match is $20°$ and the optimum combination is $(N = 3, \Delta d = 0.5\lambda)$.

As shown in Fig. 6, the EAR is from $0°$ to $57°$. To achieve the minimum ER, the AP uses multiple antennas when Bob's angle is within the EAR, whereas the AP uses an omnidirectional antenna when Bob's angle is outside the EAR. Based on the observation of T, it can be inferred that as θ_B increases, the best solution uses a fewer number of elements and a larger spacing except for $\theta_B = 25°$.

By using the configurable beamforming technique, the EAR is increased up to $57°$, compared with the EAR for a certain $(N, \Delta d)$. For example, the EAR for $(N = 4, \Delta d = 0.5\lambda)$ is from $0°$ to $41°$. Therefore, the configurable beamforming technique not only minimizes the ER for a given location of Bob but also increases the EAR.

VIII. Conclusions

This paper presents a new approach to physical space security in wireless networks that is obtained by the creation of specific regions of wireless reception around targeted users.

The objective is to minimize the size of the ER. A novel solution using a configurable beamforming technique has been developed which only needs to be applied to a single AP. To this end, the mathematical expression for the ER was derived based on our system model. Through analysis and simulations, it is shown that the proposed technique is successful at optimizing the array configuration, i.e. the number of elements and their spacing, based on the intended user's location to achieve a minimum ER and increasing the EAR.

For future work, we intend to implement the system on hardware and test it in the real environment to substantiate the expected results. Furthermore, we plan to investigate approaches by which the transmitter can acquire the channel knowledge and evaluate the impact of the estimation errors of channel information.

References

[1] E. Tews and M. Beck, "Practical attacks against WEP and WPA," in *Proc. of the Second ACM Conference on Wireless Network Security (WiSec)*, Zurich, Switzerland, Mar. 2009, pp. 79–86.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] T. Paul and T. Ogunfunmi, "Wireless LAN comes of age: Understanding the IEEE 802.11n amendment," *IEEE Circuits Syst. Mag.*, vol. 8, no. 1, pp. 28–54, First Quarter 2008.

[8] P. Kannan, R. Swaminathan, and V. Palanisamy, "Enhancing WLAN security with sectored antennas," in *Proc. of International Conference on Ultra Modern Telecommunications & Workshops (ICUMT)*, St.-Petersburg, Russia, Oct. 2009, pp. 1–5.

[9] Z. Sun, J. Lu, and D. Ireland, "Increased security level using space-division approach in wireless computing network," in *Proc. of The 17th Asia-Pacific Microwave Conference (APMC)*, Suzhou, China, Dec. 2005.

[10] ITU-R Recommendation M.1225, "Guidelines for evaluation of radio transmission technologies for IMT-2000," *International Telecommunication Union*, vol. 69, 1997.

[11] V. Erceg *et al.*, "TGn channel models," *IEEE 802.11-03/940r4*, May 2004.

[12] F. Gross, *Smart Antennas for Wireless Communications: with MATLAB*. New York: McGraw-Hill, 2005.