On the Use of Massive Cylindrical Antenna Arrays for Physical Layer Security

Elias Yaacoub
Faculty of Computer Studies, Arab Open University
Beirut, Lebanon
Email: eliasy@ieee.org

***Abstract*—The need for physical layer security techniques is increasing with the deployments of machine to machine (M2M), internet of things (IoT), and device to device (D2D) communications. An important aspect of physical layer security is to perform covert communications of a possibly unencrypted signal without allowing an eavesdropper to detect the signal. In this paper, cylindrical antenna arrays with a large number of elements are proposed in order to reach this objective. These arrays allow the transmission of both the useful signal to the destination and the jamming signal to the eavesdropper without resorting to the help of other nodes for relaying the signal and/or jamming the eavesdropper. In addition, these arrays can be used at the destination for enhancing the received signal level and/or jamming the eavesdropper simultaneously with the transmitter. Monte Carlo simulation results show that high levels of secrecy capacity can be achieved with the proposed approach.**

I. Introduction

With the advent of machine-to-machine (M2M) communications, internet of things (IoT), and device-to-device (D2D) communications, the overhead of traditional application layer encryption techniques is becoming a limiting factor in wireless networks [1]. Physical layer security, which relies on signal processing, channel coding, and other physical layer techniques is a potential solution to address this problem. In fact, it allows to hide the signal in noise as far as the eavesdropper is concerned [2], [3], while allowing the destination to receive it without relying on computationally intensive decryption methods.

A common approach to achieve this goal is to rely on cooperative relaying [4], [5], [6], where certain relays are used to relay the signal from source to destination, while others act as jammers to prevent the eavesdropper from detecting the message. This often requires the use of antenna beamforming techniques, in order to avoid significant leakage of the signal in the direction of the eavesdropper [6], [7]. The relays used should be considered “friendly”, i.e. they would not transmit the message to the eavesdropper. Furthermore, additional overhead is needed, in order to determine the set of cooperative nodes acting as relays and the set of nodes acting as jammers, while selecting the suitable transmit power for each node.

In this paper, simultaneous transmission (to the destination) and jamming (to the eavesdropper) are performed without resorting to relays. Instead, concepts of massive multiple input multiple output (MIMO) are used at the source and/or destination. Massive MIMO deployments are becoming practically feasible due to millimeter wave communications that are being investigated for 5G deployments [8]. This would allow the placement of a large number of antennas in a relatively small area. A particular antenna disposition to form cylindrical antenna arrays, first presented in [9], [10], [11], and proposed for beamforming in a WCDMA/3G system in [12], is studied in this paper and shown to lead to high secrecy capacity.

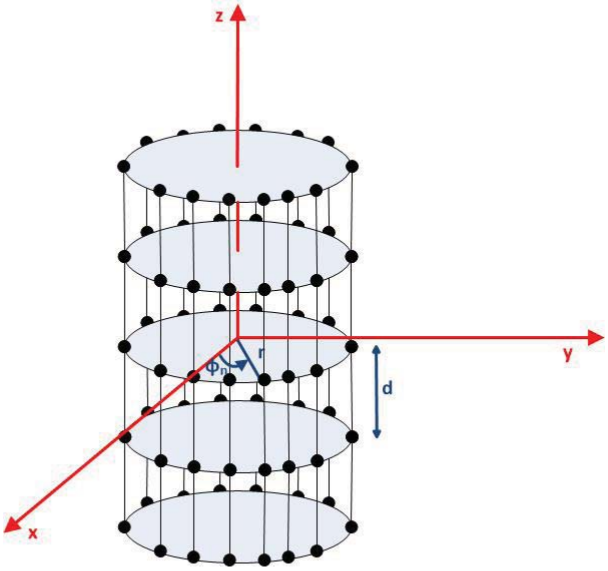

Fig. 1. Cylindrical array.

The rest of this paper is organized as follows. Section II presents an overview of cylindrical antenna arrays. The system model is presented in Section III. In Section IV, simulation results are described and analyzed. Finally, conclusions are drawn in Section V, and areas for future research are outlined.

II. Overview of Cylindrical Antenna Arrays

This section presents an overview of cylindrical arrays and of beamforming using these arrays as first introduced in [12]. The objective from using these arrays is to obtain highly directive beams that lead to high antenna gains in a desired direction while leading to low sidelobe levels in undesired directions. Antenna gain is closely related to the directivity of the antenna, which is calculated directly from the array factor [13].

A. Cylindrical Arrays

Cylindrical antenna arrays are obtained by stacking circular arrays one above the other such that the elements form linear arrays in the vertical direction, as depicted in Fig. 1. It was shown by the author and others in [9] that the array factor of a cylindrical array is equivalent to the multiplication of the array factor of a linear array on the z-axis by that of a circular array in the $x - y$ plane.

Considering a circular array with radius a having N antenna elements, and denoting by I_n and α_n the excitation coefficients' magnitude and phase for element n, and by $\phi_n = 2\pi(n-1)/N$ the angle in the $x - y$ plane between the x-axis and element n, then the array factor of one circular array in the $x - y$ plane can be expressed as [13]:

$$\mathrm{AF}_{\text{circular}}(\theta,\phi) = \sum_{n=1}^{N} I_n e^{j\{ka[\sin\theta\cos(\phi-\phi_n)]+\alpha_n\}} \tag{1}$$

where k is the wave number.

Considering a linear array on the z axis with M antenna elements separated by inter-element spacing d, and denoting by b_m the excitation coefficient of element m, then the array factor of a linear array on the z-axis is given by [13]:

$$\mathrm{AF}_{\text{linear}}(\theta) = \sum_{m=1}^{M} b_m e^{jk(m-1)(kd\cos(\theta)+\beta)} \tag{2}$$

where $\beta = -kdcos\theta_0$, with θ_0 the direction of maximum radiation.

Hence, the array factor of a cylindrical antenna array is given by:

$$\mathrm{AF}(\theta,\phi) = \mathrm{AF}_{\text{linear}}(\theta) \times \mathrm{AF}_{\text{circular}}(\theta,\phi) \tag{3}$$

Replacing (1) and (2) in (3), we obtain:

$$\begin{aligned}\mathrm{AF}(\theta,\phi) = &\sum_{m=1}^{M} b_m e^{jk(m-1)(kd\cos(\theta)+\beta)} \\ &\times \sum_{n=1}^{N} I_n e^{j\alpha_n} e^{jka[\sin\theta\cos(\phi-\phi_n)]}\end{aligned} \tag{4}$$

From (4), it can be seen that the excitation currents of each element of a cylindrical array can be considered as the product of an excitation current of an element of a linear array ($b_m e^{j\beta}$) by that of an element of a circular array ($I_n e^{j\alpha_n}$). Setting the magnitudes of these coefficients to 1 for circular and linear arrays leads to uniform circular arrays (UCA) and uniform linear arrays (ULA), respectively.

B. UCA to ULA Transformation

A method that transforms a UCA to a virtual ULA was proposed in [14]. It allows to join the benefits of 360 degrees symmetry in circular arrays with the flexibility of adjusting the array factor through varying the excitation coefficients in linear arrays.

The approach of [14] was applied in [10] on the stacked circles forming cylindrical arrays to enhance the directivity in the direction of the desired elevation angle. This transformation needs a large number of elements on the circular array. It is defined as follows:

$$\mathbf{a}_{\mathrm{v}}(\theta,\phi) = \mathbf{JFa}(\theta,\phi) \tag{5}$$

Where **a** is the array response vector of the circular array, and $\mathbf{a}_{\mathrm{v}}$ is the array response vector of the virtual linear array. Moreover,

$$\mathrm{F} = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & \omega^{-h} & \omega^{-2h} & \cdots & \omega^{-(N-1)h} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \omega^{-1} & \omega^{-2} & \cdots & \omega^{-(N-1)} \\ 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^{1} & \omega^{2} & \cdots & \omega^{(N-1)} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \omega^{h} & \omega^{2h} & \cdots & \omega^{(N-1)h} \end{bmatrix}. \tag{6}$$

with $\omega = e^{j2\pi/N}$, N the number of elements of the circular array, and

$$\mathrm{J} = diag\{j^m\sqrt{N}J_m(ka\sin(\theta_0))^{-1}\};m=-h,...,0,...,h \tag{7}$$

In (7), J_m is the Bessel function of the first kind of order m and a is the radius of the circular array.

$$[\mathrm{a}(\theta,\phi)]_{\mathrm{i}} = e^{jka[\sin\theta\cos(\phi-\frac{2\pi(i-1)}{N})]};i\epsilon\{1,2,...,N\} \tag{8}$$

The number of elements of the virtual linear array is defined as:

$$\mathrm{N_v} = 2\mathrm{h}+1 \tag{9}$$

and h is chosen such that:

$$\max\left(\mathrm{h}||\mathrm{h} \leqslant \frac{N-1}{2}\text{and}\frac{|J_{h-N}(ka\sin(\theta_0))|}{|J_h(ka\sin(\theta_0))|} < \varepsilon\right) \tag{10}$$

This approximation is valid only for $N >> ka$.

At the time when the UCA to ULA transform was proposed, and when it was considered for cylindrical arrays, the number of antenna elements required to implement it was too large for practical systems. However, with the advent of 5G millimeter wave communications, stacking very large numbers of small antenna elements to form huge arrays with reasonable dimensions gained practical viability and increasing research interest, as demonstrated by the exceptional interest in massive MIMO systems, e.g., [8]. This paper uses these concepts in a physical layer security framework, where the cylindrical arrays can be used to transmit the message to the destination while jamming the eavesdropper, without resorting to relays, as described in Section III. The UCA to ULA transform allows these arrays to have highly directive narrow beams with low sidelobes while preserving 360 degrees symmetry.

III. System Model

The system model, shown in Fig. 2, consists of a source sending a message to a destination, in the presence of an eavesdropper. A cylindrical antenna array is assumed to be used at the source, whereas the destination and the eavesdropper are assumed to have omnidirectional antennas. Furthermore, the

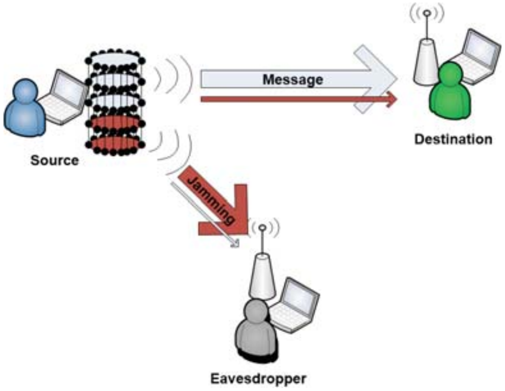

Fig. 2. System model with cylindrical array at the source.

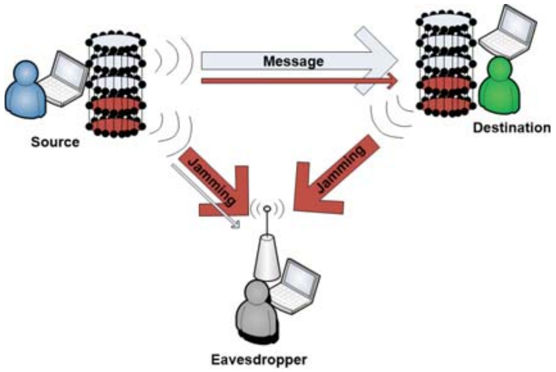

Fig. 3. System model with cylindrical arrays at the source and destination.

cylindrical array can be used to perform covert communication without resorting to the help of relays. In fact, a cylindrical array with several stacked circular arrays can be split into two arrays: one used to transmit the useful signal to the source, while the other is used to transmit a jamming signal to the eavesdropper. With appropriate beamforming, the main beam of the array transmitting the useful signal will be directed towards the destination (with very little leakage towards the eavesdropper through the antenna's sidelobes), whereas the main beam of the array transmitting the jamming signal will be pointed towards the eavesdropper (with very little leakage of the jamming signal towards the destination through the antenna's sidelobes).

This scenario is shown in Fig. 2, where three circular arrays form the cylindrical array used for transmission whereas two circular arrays form the cylindrical array used for jamming. Signal processing techniques at the transmitter would allow it to dynamically configure the number of elements used for transmission and those used for jamming. This can be done through the right excitation coefficients, as described in Section II, and by routing the desired signal (message or jamming signal) to each antenna element.

The model in Fig. 2 assumed the existence of a cylindrical array only at the source. In the results of Section IV, this scenario is referred to as the "Source only" case. However, the destination can also be equipped with a cylindrical array. The main beam of the cylindrical array can be pointed towards the source in order to enhance the reception quality of the signal at the destination. In addition, if the destination is equipped with appropriate circuitry to transmit and receive at the same time, it could split its cylindrical array into two: one used to enhance the reception of the signal from the source, whereas the second can be used to transmit an additional jamming signal in the direction of the eavesdropper, as shown in Fig. 3. The number of circular arrays used for reception or for jamming at the destination can be set to optimize performance in coordination with the source. We denote by M_s and M_d the number of circular arrays forming the cylindrical arrays at the source and destination, respectively. Then, $M_{s,t}$ and $M_{s,j}$ are the number of arrays used for transmission and jamming, respectively, at the source. In addition, $M_{d,r}$ and $M_{d,j}$ are the number of arrays used for reception and jamming, respectively, at the destination. In this paper, two scenarios are considered, both assuming $M_s = M_d = M$. The first one consists of using the same configuration at the source and the destination; i.e., the number of circular arrays used for transmission at the source is equal to the number of circular arrays used for reception at the destination, and the rest are used for jamming. Hence, $M_{s,t} = M_{d,r}$ and $M_{s,j} = M_{d,j}$. This scenario is referred to as the "Same configuration" case in the results of Section IV, and it is shown in Fig. 3. The second scenario consists of setting $M_{d,r} = M - M_{s,t}$ and $M_{d,j} = M - M_{s,j}$, or, equivalently, $M_{d,r} = M_{s,j}$ and $M_{d,j} = M_{s,t}$. This scenario is referred to as the "Complementary configuration" case in the results of Section IV. In Fig. 3, it would consist of using three circular arrays for transmission and two for jamming at the source, while using two circular arrays for reception and three for jamming at the destination.

A. Capacity Calculations

The main contribution of this paper is the use of cylindrical arrays to achieve physical layer security. Therefore, we calculate the communication capacity between the source and destination on one hand, and between the source and eavesdropper on the other hand, in the presence of jamming signals while using the proposed cylindrical arrays. The parameters used in the equations below are listed in Table I.

The channel gain on the link between entities i and j (where the term "entity" is used here to refer to any of the source, destination, or eavesdropper) is given by:

$$H_{i,j,\text{dB}} = (-\kappa - \upsilon \log_{10} d_{i,j}) - \xi_{i,j} + 10 \log_{10} F_{i,j} \qquad (11)$$

In (11), the first factor captures propagation loss, with κ the pathloss constant, $d_{i,j}$ the distance in km between entities i and j, and υ the path loss exponent. The second factor, $\xi_{i,j}$, captures log-normal shadowing with zero-mean and a standard

TABLE I
DEFINITIONS.

Variable	Description
$P_{\mathrm{s,d}}$	Transmit power from source to destination
$P_{\mathrm{s,e}}$	Jamming power transmitted from source in the direction of the eavesdropper
$P_{\mathrm{d,e}}$	Jamming power transmitted from the destination in the direction of the eavesdropper
$H_{\mathrm{s,d}}$	Channel gain between source and destination
$H_{\mathrm{s,e}}$	Channel gain between source and eavesdropper
$H_{\mathrm{d,e}}$	Channel gain between destination and eavesdropper
$G_{\mathrm{s,d}}$	Antenna gain of the array used for transmission from source to destination, with its main beam steered in the direction of the destination (ϕ_d, θ_d)
$G_{\mathrm{d,s}}$	Antenna gain of the array used for reception at the destination from the source, with its main beam steered in the direction of the source (ϕ_s, θ_s)
$G_{\mathrm{s,e}}$	Antenna gain of the array used for jamming from source to eavesdropper, with its main beam steered in the direction of the eavesdropper (ϕ_e, θ_e)
$G_{\mathrm{d,e}}$	Antenna gain of the array used for jamming from destination to eavesdropper, with its main beam steered in the direction of the eavesdropper (ϕ_e, θ_e)
σ^2	Noise power

deviation σ_ξ, whereas the last factor, $F_{i,j}$, corresponds to Rayleigh fading with a Rayleigh parameter b (usually selected such that $E[b^2] = 1$).

The capacity, in bits per second per hertz (bps/Hz), between the source and destination, is given by:

$$C_{\mathrm{s,d}} = \log_2 \left(1 + \frac{P_{\mathrm{s,d}} H_{\mathrm{s,d}} G_{\mathrm{s,d}}(\phi_d, \theta_d) G_{\mathrm{d,s}}(\phi_s, \theta_s)}{I_{\mathrm{s,d}} + \sigma^2} \right) \quad (12)$$

In (12), $I_{\mathrm{s,d}}$ is the jamming signal power received at the destination due to the sidelobes of the cylindrical antenna array. It is given by:

$$I_{\mathrm{s,d}} = P_{\mathrm{s,e}} H_{\mathrm{s,d}} G_{\mathrm{s,e}}(\phi_d, \theta_d) G_{\mathrm{d,s}}(\phi_s, \theta_s) \quad (13)$$

It should be noted that in (12), the maximum of the directivity $G_{\mathrm{s,d}}$ is in the direction of the destination (ϕ_d, θ_d), which leads to a high received useful signal power. In (13), the maximum of the directivity $G_{\mathrm{s,e}}$ is in the direction of the eavesdropper (ϕ_e, θ_e), whereas the direction of the destination (ϕ_d, θ_d) will fall under the sidelobes (and possibly nulls) of the jamming array directed towards the eavesdropper. Therefore, the capacity $C_{\mathrm{s,d}}$ will be high due to high received signal power and low jamming power leaked from the source. When a cylindrical array is available at the destination, $G_{\mathrm{d,s}}$ will be in its maximum in the direction of the source (ϕ_s, θ_s), and will enhance the received signal power, but will also lead to boosting the received jamming power as expressed in (13). When an omindirectional antenna is used at the destination, $G_{\mathrm{d,s}}$ is set to one in all directions in (12) and (13).

The capacity between the source and eavesdropper is given by:

$$C_{\mathrm{s,e}} = \log_2 \left(1 + \frac{P_{\mathrm{s,d}} H_{\mathrm{s,e}} G_{\mathrm{s,d}}(\phi_e, \theta_e)}{I_{\mathrm{s,e}} + I_{\mathrm{d,e}} + \sigma^2} \right) \quad (14)$$

In (14), $I_{\mathrm{s,e}}$ is the jamming signal power received at the eavesdropper due to the main beam of the cylindrical antenna array used for jamming at the source. It is given by:

$$I_{\mathrm{s,e}} = P_{\mathrm{s,e}} H_{\mathrm{s,e}} G_{\mathrm{s,e}}(\phi_e, \theta_e) \quad (15)$$

In addition, $I_{\mathrm{d,e}}$ is the jamming signal power received at the eavesdropper due to the main beam of the cylindrical antenna array used for jamming at the destination, in case the scenario of Fig. 3 is used ($I_{\mathrm{d,e}} = 0$ in the scenario of Fig. 2). It is given by:

$$I_{\mathrm{d,e}} = P_{\mathrm{d,e}} H_{\mathrm{d,e}} G_{\mathrm{d,e}}(\phi_e, \theta_e) \quad (16)$$

It should be noted that in (14), the maximum of the directivity $G_{\mathrm{s,d}}$ is in the direction of the destination (ϕ_d, θ_d), whereas the direction of the eavesdropper (ϕ_e, θ_e) will fall under the sidelobes and nulls of the cylindrical array used for transmitting the useful signal to the destination. In (15), the maximum of the directivity $G_{\mathrm{s,e}}$ is in the direction of the eavesdropper (ϕ_e, θ_e), which leads to a high received jamming power at the eavesdropper. Therefore, the capacity $C_{\mathrm{s,e}}$ will be low due to low useful signal power and high jamming power received at the eavesdropper. When a cylindrical array is available at the destination, $G_{\mathrm{d,e}}$ will be in its maximum in the direction of the eavesdropper (ϕ_e, θ_e), which will lead to even higher jamming power received at the eavesdropper.

B. Secrecy Capacity

Denoting by $I(x, y)$ the mutual information between the transmitted signal x at the source and the received signal y at the destination, and by $I(x, z)$ the mutual information between the transmitted signal x at the source and the overheard signal z at the eavesdropper, the secrecy capacity is given by [5], [15]:

$$C_{\mathrm{sec}} = \max_x I(x, y) - I(x, z) \quad (17)$$

where the maximization is carried over the distribution of x.

In this paper, since by definition the capacity is the maximization of mutual information, the secrecy capacity of (17) is approximated by the following expression:

$$C_{\mathrm{sec}} = C_{\mathrm{s,d}} - C_{\mathrm{s,e}} \quad (18)$$

The use of cylindrical arrays with large number of elements over their constituent circular arrays will lead to highly directive beams in the direction of interest (direction of the destination for the useful signal and direction of the eavesdropper for the jamming signal). In addition, it will lead to low sidelobe levels in the other directions, which is expected to lead to high values of $C_{\mathrm{s,d}}$ and low values of $C_{\mathrm{s,e}}$, as confirmed by the simulation results in Section IV.

IV. SIMULATION RESULTS

An area of 1×1 km^2 is considered, with random uniformly distributed locations for the source, destination, and eavesdropper. $M = 8$ circular arrays are stacked to form a cylindrical array, with vertical separation $d = 0.5\lambda$ between elements (with λ being the wavelength). Each circular array consists of $N = 33$ isotropic elements with $ka = 10$. Fig. 4 shows the

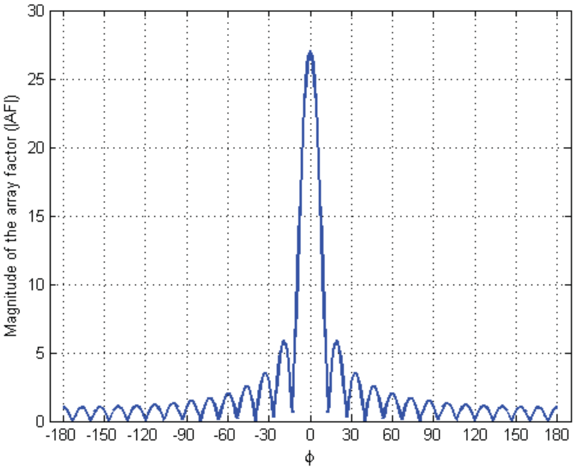

Fig. 4. Magnitude of the array factor of the cylindrical array in the $x - y$ plane.

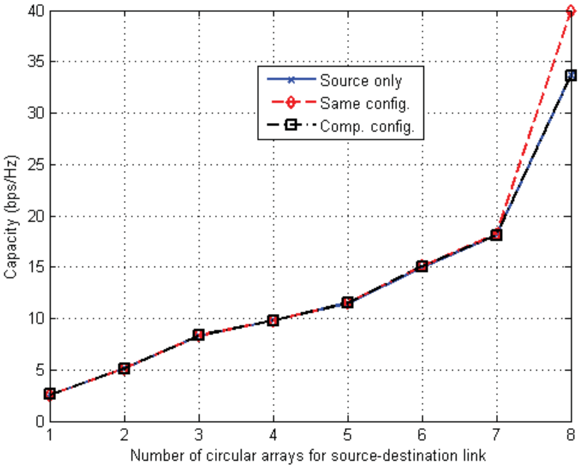

Fig. 5. Capacity between source and destination.

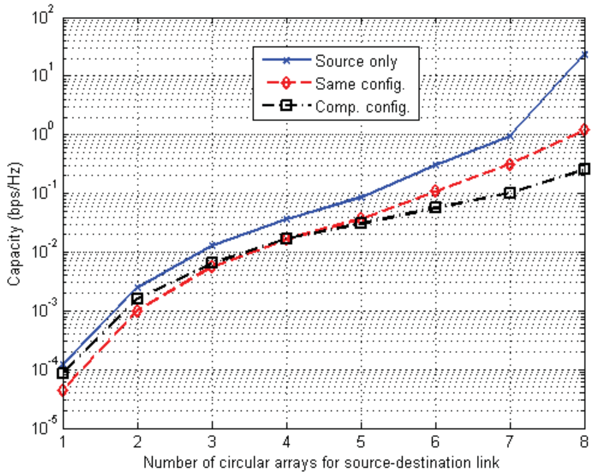

Fig. 6. Capacity between source and eavesdropper.

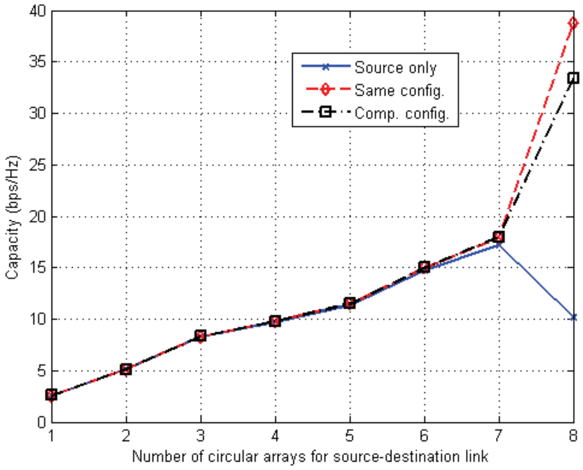

Fig. 7. Secrecy capacity between source and destination.

magnitude of the array factor of this cylindrical array in the $x - y$ plane ($\theta = 90$ degrees). The figure clearly shows the highly directive main beam and the low sidelobe levels.

The total transmit power is set to $P_{\text{tot}} = 1$ W, subdivided equally among the circular arrays. Hence, if $M_{s,t}$ circular arrays are used to form the cylindrical array transmitting the useful signal, then $P_{\text{s,d}} = P_{\text{tot}} \cdot M_{s,t}/M$ and $P_{\text{s,e}} = P_{\text{tot}} \cdot M_{s,j}/M$. In case of a cylindrical array at the destination, all the power can be used to transmit the jamming signal in the direction of the eavesdropper, i.e., $P_{\text{d,e}} = P_{\text{tot}}$.

Lognormal shadowing is considered to have a zero mean and an 8 dB standard deviation. Pathloss parameters are set to $\kappa = -128.1$ dB and $\upsilon = 3.76$. The results are averaged over 10000 iterations.

Figures 5, 6, and 7 show the results for $C_{\text{s,d}}$, $C_{\text{s,e}}$, and C_{sec}, respectively. These capacities are plotted versus $M_{s,t}$. A log scale is used in Fig. 6 due to the low value of $C_{\text{s,e}}$ when jamming is performed on the eavesdropper using the proposed cylindrical arrays with beam steering. $C_{\text{s,e}}$ has the highest values when jamming is performed from the source only, and decreases significantly when the jamming is performed jointly from source and destination. In addition, even when jamming is performed only from the source, $C_{\text{s,e}}$ is generally low but increases by more than an order of magnitude when the number of transmit circular arrays moves from $M_{s,t} = 7$ to $M_{s,t} = 8$. In fact, in the latter case, all the antenna elements at the source are used for transmission and none is used for jamming. This means that the eavesdropper is receiving part of the signal from the sidelobes of the antenna array, although the array becomes more directive with a narrower beam when all the antenna elements are used as a single transmit array. When jamming is also performed from the destination side, the situation becomes better. It should be noted that in the "Same Configuration" case, it is assumed that the destination jams the eavesdropper with a simple isotropic antenna (radiating equally in all directions) when $M_{s,t} = 8$ (in order to distinguish this scenario from the "Source Only" case). Even this simple jamming scheme leads to an important reduction in $C_{\mathrm{s,e}}$, although outperformed by the "Complementary Configuration" case. Nevertheless, the "Same Configuration" case leads to the best performance in terms of $C_{\mathrm{s,d}}$, with the other two scenarios having comparable performance. This is due to pointing two directive antennas in face of each other (one at the source and the other at the destination), which increases the signal to jamming and noise ratio in (12).

When the results of Figs. 5 and 6 are used to generate Fig. 7, the "Same Configuration" case is shown to still have the best performance in terms of secrecy capacity, followed by the "Complementary Configuration" case. However, if minimizing the useful signal leakage to the eavesdropper is the primary objective, then the "Complementary Configuration" scenario can be considered better, since it leads to the lowest $C_{\mathrm{s,e}}$ while maintaining a relatively high secrecy capacity C_{sec}.

Fig. 7 shows an interesting behavior with the "Source Only" case: When the number of antennas used for transmission increases, C_{sec} keeps increasing as long as there is at least one of the circular arrays used for jamming the eavesdropper. When all the antennas are used for transmission, the secrecy capacity drops dramatically despite the increase in $C_{\mathrm{s,d}}$, due to the larger increase in $C_{\mathrm{s,e}}$. This performance indicates the importance of physical layer security through joint transmission and jamming. The use of antenna arrays with large number of elements makes the simultaneous jamming/transmission operations possible, especially with the increasing popularity of massive MIMO techniques.

V. Conclusions and Future Research Directions

Physical layer security using simultaneous jamming and transmission was investigated. Cylindrical antenna arrays with large number of elements were used in order to increase the source-destination signal quality with high directive beams. At the same time, the arrays were used to transmit a jamming signal in the direction of an eavesdropper. Simulation results showed that high capacities can be achieved between the source and destination, with low intercept capacities at the eavesdropper, when simultaneous transmission and jamming are performed. Using cylindrical arrays at the destination in addition to the source helped enhance the performance further.

Future enhancements of this work include the dynamic optimization of the transmit power for both the useful and jamming signals, along with dynamic configuration of the antenna arrays (number of elements used for transmission and those used for jamming). Another interesting research direction would be to investigate scenarios with more than one eavesdropper, and the need for using relays (with or without cylindrical arrays) to enhance performance in this case. In addition, another extension of this work would be the study of scenarios where the eavesdropper is itself equipped with a directive antenna, steered in the direction of the source. Last but not least, it would be interesting to investigate efficient eavesdropper localization techniques, and the impact of inaccuracies in determining the locations of the destination and/or eavesdropper, which would affect the beam steering process.

References

[1] T.-Y. Liu, P.-H. Lin, S.-C. Lin, Y.-W. P. Hong, and E. A. Jorswieck, "To Avoid or Not to Avoid CSI Leakage in Physical Layer Secret Communication Systems", *IEEE Communications Magazine*, vol. 53, no. 12, pp. 19–25, December 2015.

[2] P. H. Che, M. Bakshi, and S. Jaggi, "Reliable Deniable Communication: Hiding Messages in Noise", *Proc. IEEE Int'l. Symp. Info. Theory*, Instanbul, Turkey, pp. 2945–2949, July 2013.

[3] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, "Hiding Information in Noise: Fundamental Limits of Covert Wireless Communication", *IEEE Communications Magazine*, vol. 53, no. 12, pp. 26–31, December 2015.

[4] K. Park, T. Wang, and M. Alouini, "On the Jamming Power Allocation for Secure Amplify-and-Forward Relaying via Cooperative Jamming", *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1741–1750, September 2013.

[5] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical Layer Security in Wireless Cooperative Relay Networks: State of the Art and Beyond", *IEEE Communications Magazine*, vol. 53, no. 12, pp. 32–39, December 2015.

[6] X. Chen, L. Lei, H. Zhang, and C. Yuen, "On the Secrecy Outage Capacity of Physical Layer Security in Large-Scale MIMO Relaying Systems with Imperfect CSI", *Proc. IEEE ICC*, Sydney, Australia, pp. 2052–2057, June 2014.

[7] X. Chen, C. Zhong, C. Yuen, and H.-H. Chen, "Multi-Antenna Relay Aided Wireless Physical Layer Security", *IEEE Communications Magazine*, vol. 53, no. 12, pp. 40–46, December 2015.

[8] Z. Gao, L. Dai, D. Mi, Z. Wang, M. A. Imran, and M. Z. Shakir, "MmWave Massive-MIMO-based Wireless Backhaul for the 5G Ultra-Dense Network", *IEEE Wireless Communications*, vol. 22, no. 5, pp. 13–21, October 2015.

[9] E. Yaacoub, M. Al Husseini, A. Chehab, A. El Hajj, K. Y. Kabalan, "Hybrid Linear and Circular Antenna Arrays", *Iranian Journal of Electrical and Computer Engineering*, vol. 6, no. 1, pp. 48–54, Winter-Spring 2007.

[10] E. Yaacoub, M. Al Husseini, A. Chehab, K. Y. Kabalan, A. El Hajj, "Pattern Synthesis with Cylindrical Arrays", *WSEAS Transactions on Communications*, vol. 5, no. 12, pp. 2198–2207, December 2006.

[11] A. A. L. Neyestanak, M. Ghiamy, M. Naser-Moghaddasi, and R. A. Saadeghzadeh, "Investigation of Hybrid Elliptical Antenna Arrays", *IET Microwaves, Antennas and Propagation*, vol. 2, no. 1, pp. 28–34, February 2008.

[12] E. Yaacoub, K. Kabalan, A. El-Hajj, and A. Chehab, "Cylindrical Antenna Arrays for WCDMA Downlink Capacity Enhancement",*IEEE International Conference on Communications (ICC 2006)*, pp. 4912–4917, Istanbul, Turkey, June 2006.

[13] C. A. Balanis, *"Antenna Theory, Analysis and Design"*, 4th edition, John Wiley and Sons, 2016.

[14] B. K. Lau and Y. H. Leung, "A Dolph-Chebyshev Approach to the Synthesis of Array Patterns for Uniform Circular Arrays", *IEEE International Symposium on Circuits and Systems*, Geneva, Switzerland, May 28-31, 2000.

[15] A. D. Wyner, "The Wire-Tap Channel", *Bell Systems Technical Journal*, vol. 54, pp. 1355-1387, October 1975.