Achieving Physical Layer Security with Massive MIMO Beamforming

Elias Yaacoub*, Mohammed Al-Husseini†

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

† Beirut Research and Innovation Center, Beirut, Lebanon. Email: husseini@ieee.org

***Abstract*—Physical layer security allows secure communications between a source and destination without the need to resort to key-based encryption techniques. Its increasing importance stems from the difficulty of implementing advanced encryption techniques in certain networks, such as the internet of things (IoT). In this paper, physical layer security is implemented by using massive multiple input multiple output (MIMO) techniques. Specifically, beamforming with large cylindrical antenna arrays is investigated. 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. Simulation results show that high levels of secrecy capacity can be achieved with the proposed approach.**

***Index Terms*—Physical layer security, jamming, antenna arrays, beamforming, cylindrical arrays, massive MIMO.**

I. Introduction

Physical layer security is being considered as a potential solution for securing communications without relying on the overhead of traditional application layer encryption techniques. It relies on signal processing, channel coding, and other physical layer techniques [1], and thus could be considered more convenient for secure machine-to-machine (M2M) communications, internet of things (IoT), and device-to-device (D2D) communications [2]. It provides the possibility of hiding the signal in noise for a potential eavesdropper [1], while allowing the intended recipient to receive the message correctly.

Recent investigations in the literature have considered achieving physical layer security through cooperative relaying [3]. Under this approach, a set of relays can be selected to relay the signal from source to destination, while another set includes relays acting 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 [3]. Under such a system, the source and destination need to trust the relays, where a “friendly”relay would be entrusted not to transmit the message to the eavesdropper. In addition, to optimize performance, some computational overhead is still needed in order to determine the set of nodes acting as relays and the other set containing the jammers.

The approach proposed in this paper avoids the use of relays. It is based on using massive multiple input multiple output (MIMO) arrays at the legitimate source and/or destination in order to perform simultaneous transmission and jamming through antenna array beamforming techniques. With the advent of millimeter wave communications, Massive MIMO deployments are becoming practically feasible [4]. This would allow the placement of a large number of antennas in a relatively small area.

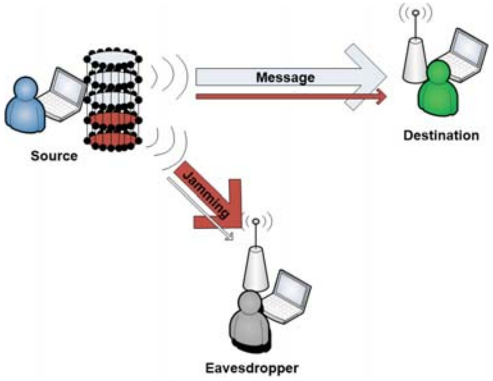

Fig. 1. System model with cylindrical array at the source.

The rest of this paper is organized as follows. Section II presents the system model. In Section III, simulation results are described and analyzed. Finally, Section IV concludes the paper and indicates directions for future research.

II. System Model

The system model is shown in Fig. 1. It consists of a source, equipped with a massive MIMO antenna array, sending a message to a destination. An eavesdropper attempts to intercept the unencrypted message. The destination and the eavesdropper are assumed to have omnidirectional antennas.

In Fig. 1, the antenna array disposition at the source is selected to be a cylindrical one. This array geometry was presented in [5], [6]. In [7], it was proposed for beamforming in a WCDMA/3G system. Cylindrical arrays allow obtaining 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 [8]. 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. 2. It was shown by the authors and others in [5] that the array factor of a cylindrical array is equivalent to the multiplication of the

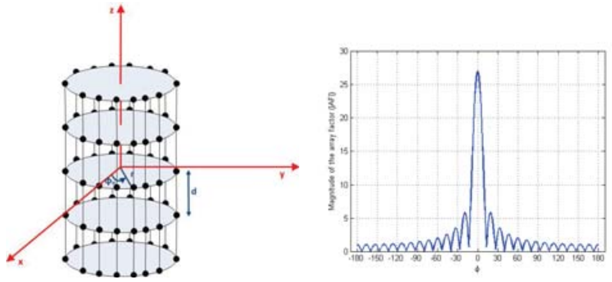

Fig. 2. Left: Cylindrical array. Right: Magnitude of the array factor of a cylindrical array in the $x-y$ plane, with $M = 8$ stacked circular arrays, each consisting of $N = 33$ isotropic elements with $ka = 10$. Vertical separation between elements is $d = 0.5\lambda$ (with λ being the wavelength).

array factor of a linear array on the z-axis by that of a circular array in the $x-y$ plane. A method that transforms a circular array to a virtual linear array was proposed in [9]. 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. For example, Fig. 2 shows the magnitude of the array factor of a 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 method proposed in this paper makes use of the cylindrical array in order to perform covert communication without the need for 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. 1, where three circular arrays form the cylindrical array are used for transmission whereas two circular arrays form the cylindrical array are 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.

In the model in Fig. 1 the existence of a cylindrical array is assumed only at the source. This scenario is referred to as the "Source only" case. In the event where the destination is also equipped with a cylindrical array, the main beam of that array can be directed 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. 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. 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.

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

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:

$$H_{i,j,\mathrm{dB}} = (-\kappa - \upsilon \log_{10} d_{i,j}) - \xi_{i,j} + 10 \log_{10} F_{i,j} \qquad (1)$$

In (1), 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 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:

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

In (2), $I_{\mathrm{s,d}}$ is the jamming signal power received at the destination due to the sidelobes of the cylindrical antenna array used for jamming the eavesdropper. It is given by:

$$I_{\mathrm{s,d}} = P_{\mathrm{s,e}} H_{\mathrm{s,d}} G_{\mathrm{s,e}}(\phi_d, \theta_d) G_{\mathrm{d,s}}(\phi_s, \theta_s) \quad (3)$$

It should be noted that in (2), 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 (3), 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 (3). When an omindirectional antenna is used at the destination, $G_{\mathrm{d,s}}$ is set to one in all directions in (2) and (3).

The capacity between the source and eavesdropper is given by:

$$C_{\mathrm{s,e}} = \log_2\left(1 + \frac{P_{\mathrm{s,d}} H_{\mathrm{s,e}} G_{\mathrm{s,d}}(\phi_e, \theta_e)}{I_{\mathrm{s,e}} + I_{\mathrm{d,e}} + \sigma^2}\right) \quad (4)$$

In (4), $I_{\mathrm{s,e}}$ 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:

$$I_{\mathrm{s,e}} = P_{\mathrm{s,e}} H_{\mathrm{s,e}} G_{\mathrm{s,e}}(\phi_e, \theta_e) \quad (5)$$

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, when it exists ($I_{\mathrm{d,e}} = 0$ in the scenario of Fig. 1). It is given by:

$$I_{\mathrm{d,e}} = P_{\mathrm{d,e}} H_{\mathrm{d,e}} G_{\mathrm{d,e}}(\phi_e, \theta_e) \quad (6)$$

It should be noted that in (4), 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 (5), 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 [10]:

$$C_{\mathrm{sec}} = \max_x I(x, y) - I(x, z) \quad (7)$$

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 (7) is approximated by the following expression:

$$C_{\mathrm{sec}} = C_{\mathrm{s,d}} - C_{\mathrm{s,e}} \quad (8)$$

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 III.

III. Simulation Results

A. Simulation Model

We consider a source-destination pair, with an eavesdropper located such that the source-eavesdropper line forms a 30 degrees angle with the source-destination line (scenario similar to Fig. 1). $M = 5$ 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 $ka = 10$ (k being the wave number and a the radius of the circular array).

The total transmit power is set to $P_{\mathrm{tot}} = 1$ 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 $P_{\mathrm{s,d}} = P_{\mathrm{tot}} \cdot M_{s,t}/M$ and $P_{\mathrm{s,e}} = P_{\mathrm{tot}} \cdot M_{s,j}/M$. 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., $P_{\mathrm{d,e}} = P_{\mathrm{tot}}$.

Channel gain is assumed to include pathloss, lognormal shadowing, and fast Rayleigh fading. 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.

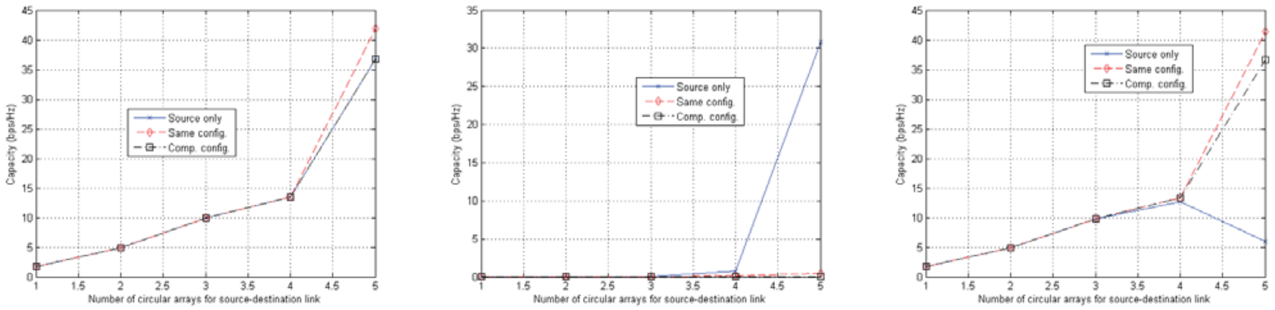

Fig. 3. Capacity measures. Left: $C_{\rm s,d}$; Middle: $C_{\rm s,e}$; Right: $C_{\rm sec}$.

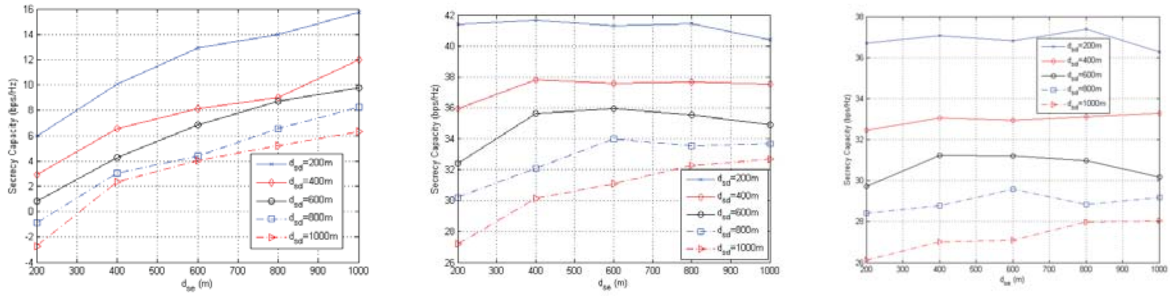

Fig. 4. Secrecy capacity between source and destination. Left: "Source Only"; Middle: "Same Configuration"; Right: "Complementary Configuration".

B. Results with Fixed Locations

In this section, the destination and eavesdropper are assumed to be located at the same distance from the source, set to 500 m. As mentioned in Section III-A, the source-eavesdropper line forms a 30 degrees angle with the source-destination line. Fig. 3 shows the results for $C_{\rm s,d}$, $C_{\rm s,e}$, and $C_{\rm sec}$. These capacities are plotted versus $M_{s,t}$.

Fig. 3 shows that $C_{\rm s,e}$ 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, $C_{\rm s,e}$ is generally low but increases by more than an order of magnitude when the number of transmit circular arrays moves from $M_{s,t} = 4$ to $M_{s,t} = 5$. 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 $M_{s,t} = 5$ (in order to distinguish this scenario from the "Source Only" case). Even this simple jamming scheme leads to an important reduction in $C_{\rm s,e}$, although outperformed by the "Complementary Configuration" case. Nevertheless, the "Same Configuration" case leads to the best performance in terms of $C_{\rm s,d}$, 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 (2).

When the results of $C_{\rm s,d}$ and $C_{\rm s,e}$ are used to generate the results of $C_{\rm sec}$ in Fig. 3, 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 $C_{\rm s,e}$ while maintaining a relatively high secrecy capacity $C_{\rm sec}$.

Fig. 3 shows an interesting behavior with the "Source Only" case: When the number of antennas used for transmission increases, $C_{\rm sec}$ 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 $C_{\rm s,d}$, due to the larger increase in $C_{\rm s,e}$. 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.

C. Results with Variable Locations

In this section, the distances between the destination and source on one hand, and the eavesdropper and source on the other hand, are varied. The source-eavesdropper line is still considered to form a 30 degrees angle with the source-destination line. Due to the high directive gains of the antennas, results do not vary much with distance when $M_{s,t} < 5$, i.e., when there is at least one circular array used at the transmitter for jamming the eavesdropper. Hence, they are not shown here due to space limitations. The results presented in this section correspond to $M_{s,t} = 5$, i.e. the case where all the antennas at the transmitter are used for transmission.

Fig. 4 shows the results for the secrecy capacity C_{sec} in the "Source Only", "Same Configuration", and "Complementary Configuration" scenario.

In the "Source Only" case, a large decrease in the secrecy capacity is shown when the eavesdropper becomes closer to the source. When the destination is relatively far and the eavesdropper is too close, in the absence of jamming, C_{sec} becomes negative. This means that the signal received at the eavesdropper is better than the one received at the legitimate destination, despite the beamforming performed in the direction of the destination. Hence, due to the large distance, the signal radiated through the sidelobes reaches the eavesdropper with higher power than the signal radiated through the main lobe reaches the destination. In the "Same Configuration" case, a massive MIMO array at the destination enhances considerably the situation, even if jamming is performed from the destination to the eavesdropper using an omnidirectional antenna. Interestingly, this performance slightly outperforms the case of "Complementary Configuration", where the destination receives with an omnidirectional antenna and jams the eavesdropper with a cylindrical array.

IV. Conclusions and Future Research Directions

An application of beamforming with massive MIMO arrays for physical layer security was investigated. The proposed method consists of using simultaneous jamming to an eavesdropper and transmission to a legitimate destination. 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. In the absence of jamming, simulation results showed that the secrecy capacity deteriorates dramatically when the eavesdropper is located closer to the transmitter. However, results showed that high secrecy capacities can be achieved between the source and destination, with low intercept capacities at the eavesdropper, when simultaneous transmission and jamming are performed. The use of massive MIMO arrays at the destination in addition to the source helped enhance the performance further by receiving a better signal quality from the source and contributing to increased jamming to the eavesdropper.

Future enhancements of this work include the investigation of random positions of the jammer and destination with respect to the transmitter in a given area. Another enhancement consists of investigating 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). Furthermore, it would be interesting to investigate the impact of inaccuracies in determining the locations of the destination and/or eavesdropper, which would affect the beam steering process.

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

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

[9] 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.

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