Secure Multiple-Users Transmission Using Multi-Path Directional Modulation

Mohammed Hafez[1], Tamer Khattab[2], Tarek Elfouly[3], Hüseyin Arslan[1,4]
[1] Department of Electrical Engineering, University of South Florida, Tampa, Florida 33620
[2] Department of Electrical Engineering, Qatar University, Doha, Qatar
[3] Department of Computer Science and Computer Engineering, Qatar University, Doha, Qatar
[4]School of Engineering and Natural Sciences, Istanbul Medipol University, Beykoz, Istanbul 34810
Email: mhafez@mail.usf.edu, tkhattab@ieee.org, tarekfouly@qu.edu.qa, arslan@usf.edu

***Abstract*—This work introduces a physical-layer secure multiple-users communication scheme. Our scheme employs the multi-path nature of the wireless channel to provide a different secure communication link for each of the legitimate users. We show that the proposed scheme highly degrades the eavesdroppers channel even for the worst case scenarios. We also provide the secrecy capacity and secrecy outage probability for the proposed scheme. We analyze the effect of the number of users, channel paths, and antenna elements on the secrecy performance of the scheme.**

***Index Terms*—Directional modulation, Antenna arrays, Physical-layer security.**

I. Introduction

Limitations on the wireless communication resources (i.e., time and frequency) introduces the need for another domain that can help communication systems to match the increasing demand on high data transfer rates and quality of service (QoS). By using multiple antennas [1], either on the transmitter or the receiver side or both, the space domain was introduced as a new dimension that allows communications systems to reach higher rates. Based on their construction, multiple antennas can be considered as a single unit (i.e., antenna arrays) or separate uncorrelated units. The single unit structure introduce a flexible tool to transmit (receive) the wireless signal based on the spatial direction of interest, while the uncorrelated structure gives the opportunity to either improve the QoS, in terms of channel capacity and throughput, by exploiting the available diversity, or increasing the system rate by utilizing the space as a source for multiplexing (multiple access).

The widespread use of wireless technology and its ease of access makes the privacy of the information, transferred over the wireless network, questionable. Along with the drawback of the traditional ciphering algorithms, physical layer security rises as a solution for such problem.

Multiple-antennas systems offer more resources (i.e. degrees of freedom) which can be used to achieve secure communication [2], [3]. Some examples of these resources are the number of transmit antennas and the ability to have directive communication by using antenna arrays. One of the recently developed techniques, that make use of directive antenna-arrays to provide secrecy, is *Directional Modulation* (DM).

Many Algorithms were proposed, that make use of the properties of the MA systems, to provide a robust secure communication link [4]. These algorithms can be split over two main Categories, namely "*Precoding based*" and "*Array based*". there are some other algorithms that don't fall under these categories. Example of these algorithms are, transmit antenna selection [5], key generation using precoding matrix indices [6], and time-domain artificial noise generation [7].

For *Precoding based* schemes, the transmitter construct a precoding matrix, based on its knowledge about the channels' realizations, to make the signal able to be decoded only if it went through the channel of the legitimate user [8], [9]. Construction of such precoding matrix depends mainly on the channel state information that is available at the transmitter. If the transmitter has information about the eavesdropper channel, it uses either *Generalized Singular Value Decomposition* (GSVD) or *Zero-Forcing* (ZF). GSVD constructs a set of parallel independent sub-channels between the transmitter and the two receivers. This allows the transmitter to choose only the sub-channels in which the legitimate receiver has advantage over the eavesdropper, to be used for message transmission [10], [11]. on the other hand, ZF constructs a pre-coding matrix that would protect the confident messages from being transmitted towards the eaves dropper [12].

When there is no information available at the transmitter about the channel of the eavesdropper, the transmitter attempts to provide secrecy to the legitimate message by embedding a jamming signal (i.e. *Artificial Noise* (AN)) into the null-space of the legitimate channel [13], [14]. With the assumption of the independence between the legitimate and the eavesdropper channels, the transmitter assumes that the AN will leak into the received signal of the eavesdropper causing some degradation for it's performance.

In DM, the antenna pattern is recognized as a spatial complex constellation, but it's not used as a source of information. The antenna pattern complex value, at a certain desired direction, is set to have the same complex value of the symbol to be transmitted. This scheme also randomizes the signal in the undesired directions, thus, providing a source of directional security. Contrary to the regular beam-forming, which provides directional power scaling, DM technique is applied in the transmitter by projecting digitally encoded

978-1-4799-6664-6/16/$31.00 ©2016 IEEE

information signals into a pre-specified spatial direction while simultaneously distorting the constellation formats of the same signals in all other directions.

The idea was first considered as changing the stage where modulation takes place. The authors of [15] and [16] started to explain the idea of directional modulation using phased arrays, and demonstrated (synthesized) it in [17] and [18]. Based on their methodology, the modulation process needs to take place at the RF stage, instead of the regular base band modulation. Another algorithm for synthesizing DM is the antenna subset modulation (ASM) presented in [19]. In this technique, they only use few selected elements from the available antenna array to transmit. The elements used in transmission are randomly selected for each transmitted symbol to provide a randomized constellation pattern for the undesired direction. In [20], quadrature modulated I and Q data streams were separately encoded at the baseband, up-converted to radio frequency (RF) and then separately transmitted.When the two streams are combined in the far-field, the resultant IQ data is only detectable along the pre-specified spatial direction.

We can look at the difference between the conventional beam-forming and DM from another perspective. In the conventional beam-forming, the complex weights, which scale the antenna array, are changing based on the rate of change of the communication channel. Contrary, in the case of DM, the rate of change of the weights is related to the transmitted data rate [21]. In [22], a general analysis for DM using vector-domain is performed. The authors categorize DM algorithms into two groups. The first one they call it *"Static"* algorithms, where the generated antenna pattern does not change for any selected constellation point, i.e., if we choose to transmit one single point of the constellation, the generated pattern will always be the same. The second group is the *"Dynamic"* algorithms, where we can transmit the same constellation point with a different pattern each time, which makes it hard to track and decipher. Due to the lack of tools that can evaluate the performance of such system, some parameters based on BER, error-vector-magnitude (EVM), and secrecy rate were suggested in [23].

In our previous work [24], we introduced the Multi-Directional DM transmission scheme (MDDM). By using MDDM, we were able to provide multiple secure communication links for different directions. We showed that the scheme increases the transmission capacity of the system up to the number of the antenna elements. Also, the secrecy capacity increases with the increase of the number of transmitted streams. Moreover, MDDM has a low complexity structure compared to other DM implementations and it does not necessitate the implementation of special receiver algorithms.

Up till now, DM was only discussed from the algorithm construction perspective, and to the extent of the authors knowledge there has been no study of the employment of DM algorithms into the system level. Hereby, we propose a system level design that makes use of our proposed MDDM scheme. The new design utilizes the dispersive nature of the channel to provide a location-based secure communication link to each of the legitimate users. The scheme shows the ability to highly degrade the eavesdropper channel, even for the worst case scenarios. We also deduce the secrecy capacity and outage probability for the scheme. Besides, we compare the performance of this scheme to the performance of AN precoding, as they share the same assumption about the channel knowledge.

The rest of this paper is organized as follows: In section II, we review the multiple-directions transmission concept. Section III presents the proposed multi-path secure system. Section IV discusses the system performance. Finally. we conclude the paper in section V.

II. MDDM Transmission System design

Here, we consider that we have a broadcast channel with a single source (base-station) and L destinations; namely directions. Each direction has its own desired data stream $x_i(k)$, and has a different transmission angle with respect to the base-station θ_i, where $i = 1,2,\ldots,L$, and k is the time index. Different directions share the same resources of time slots, frequency bands, or codes simultaneously. All legitimate receivers and the eavesdropper are considered to have a single receiving antenna. The base-station uses a linear antenna array, with N elements, for transmission. Based on the idea of directional modulation, we need to set $W = [w_1(k), w_2(k), \ldots, w_N(k)]^T$, so that $f(\theta_i,k) = x_i(k)$, where W is the vector containing the complex weights for the antenna array and f is the value of the resulting complex antenna pattern at a time instant k by the receiver located at a certain direction θ, where

$$f(\theta,k) = h^*(\theta)W(k), \tag{1}$$

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

and $h^*(\theta)$ is the array steering vector for a receiver positioned at the direction θ.

Let us define F as the column vector that contains the desired pattern values, for each of the desired transmission directions.

$$\begin{aligned} F &= [f(\theta_1,k), f(\theta_2,k), \ldots, f(\theta_L,k)]^T \\ &= H^H W = \begin{bmatrix} h^*(\theta_1) \\ h^*(\theta_2) \\ \vdots \\ h^*(\theta_L) \end{bmatrix} [w_1(k), w_2(k), \ldots, w_N(k)]^T, \end{aligned} \tag{3}$$

where, $H \in \mathbb{C}^{N\times L}$, and we consider that $L \leq N$, i.e., the number of desired transmission directions is less than the number of the antenna array elements. This makes (3) an under-determined set of linear equations. Using the least-norm solution [25], we find that

$$W_{ln} = H\left(H^H H\right)^{-1} F. \tag{4}$$

By replacing F with $X = [x_1(k), x_2(k), \ldots, x_L(k)]^T$, we can produce the required weights to modulate the resulting antenna pattern, so that the pattern takes the desired values at the

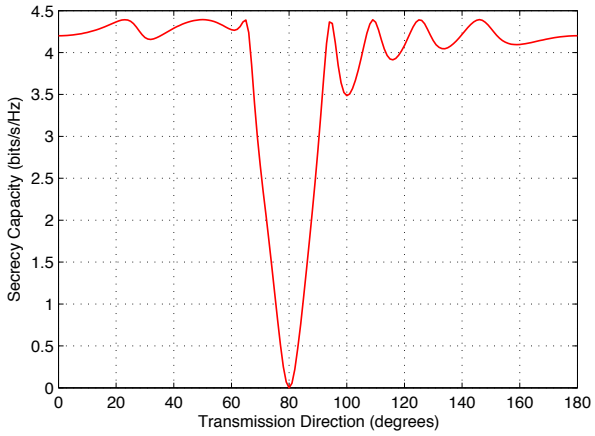

Fig. 1. Secrecy rate based on the SINR of the received symbols.

desired directions. Based on that, the value of the received pattern can be rewritten as,

$$f(\theta,k) = h^*(\theta)H(H^H H)^{-1}X(k). \quad (5)$$

Note that, the usage of any other antenna array structure is applicable, as long as the appropriate steering vector $h^*(\theta)$ is used for the generation of the weights W. Moreover, if we assume that the channel state information (CSI) for each of the users is available at the transmitter, we can enhance the secrecy performance of the system by multiplexing it within the generated weights.

$$W = \Gamma^H(\Gamma\Gamma^H)^{-1}X \quad (6)$$

where, $\Gamma = \Delta H^H$, and Δ is the $(L \times L)$ diagonal matrix containing the CSI of each of the users.

Figure 1 shows the secrecy performance in terms of the secrecy rate,

$$R_{Secrecy} = R(\theta_d) - R(\theta) \quad (7)$$

$$R(\theta) = log_2(1+\rho(\theta)), \quad (8)$$

where $R(\theta_d)$ is the achievable rate at the desired direction θ_d, $\rho(\theta)$ is the received SINR at any direction θ, and the SNR for the desired direction at 80^o is 10 dB. The figure shows high secrecy gain outside the main lobe, which indicates that the data obtained by non-intended directions will not be detected reliably. The figure also shows that communication is not secure in the direction of the legitimate user, however, the multi-path nature of the channel can be used to generate a precoding scheme that ensures secrecy for this direction as discussed in the next section.

III. Multi-Path Based Secure Communication

The problem here is that, if the eavesdropper is aligned with one of the transmission directions, it will be able to receive the clear constellation of the transmitted data. This will be mitigated by the introduction of the following scenario. Consider that the M users are assigned to a single base-station, which is equipped with an antenna-array of N elements for down-link transmission. The M users are receiving the BS signal through L different directions $(L > M)$. The base-station is assumed to have a full knowledge about the channel of each user (i.e., the delay profile and the angle of arrival of each path), which can be estimated using one of the methods according to [26].

We define the matrix $A = \{\alpha_{ij}\}_{M\times L}$, where α_{ij} is the gain coefficient of the j^{th} path that is delivered to the i^{th} user. Based on that, the transmitted antenna pattern will be synthesized as

$$f(\theta,k) = h(\theta)H[H^H H]^{-1}A^H[AA^H]^{-1}S(k) = C(\theta)S(k), \quad (9)$$

where $H \in \mathbb{C}^{N\times L}$ is the steering matrix, $S \in \mathbb{C}^{M\times 1}$ vector that contain the users data. Then the SIR of the signal of the m^{th} transmitted signal $s_m(k)$ at any direction θ would be calculated as

$$SIR_m(\theta) = \frac{|c_m(\theta)|^2}{\sum_{\forall j\neq m}|c_j(\theta)|^2}. \quad (10)$$

We can see from (9), that the transmitted pattern at any direction θ is a linear combination of all M data streams. Then, if an eavesdropper is trying to decode the m^{th} message based on the reception of a single direction, it will suffer from a high interference level due to the other $M-1$ streams. We will show later that the received SIR value has a high probability of being low.

Based on this model, the received signal at any receiver in the network is given as

$$r(k) = B \times \mathbf{C} \times S(k) = V \times S(k), \quad (11)$$

where $B = \{\beta_p\}_{1\times P}$ is the gain coefficient of the p^{th} received path by any user, and $\mathbf{C} = [C(\theta_1);C(\theta_2);\ldots;C(\theta_P)]$. Again, considering the decoding of the m^{th} message, the received SIR can be calculated as

$$SIR_m^r = \frac{|v_m|^2}{\sum_{\forall j\neq m}|v_j|^2}. \quad (12)$$

For the m^{th} legitimate user $\{v_m = 1, v_{\forall j\neq m} = 0\}$, which eliminates the effect of other streams on its message. Otherwise, if the received signal is not completely aligned to the legitimate user channel, it will still suffer from such interference as shown by later results. The exact distribution of SIR_m^r with relation to N, L, and M is out of the scope of this study, but it is considered in an extension of the current work.

Based on (12), and by assuming the worst case analysis where the eavesdropper does not suffer from any noise effect, we can define the achievable secrecy rate as

$$\begin{aligned} R_s &= R_l - R_e, \\ &= [\log(1+\gamma_l) - log(1+SIR_m^r)]^+, \end{aligned} \quad (13)$$

where γ_l is the SNR received by the legitimate user, and $[.]^+ = \max(.,0)$ indicates that only positive values are considered otherwise $R_s = 0$. The average achievable rate and the probability of its existence (i.e., $P(R_s > 0)$) will be numerically investigated in the next section.

Also, as we consider the case where the eavesdropper is totally passive and the information about its channel is not

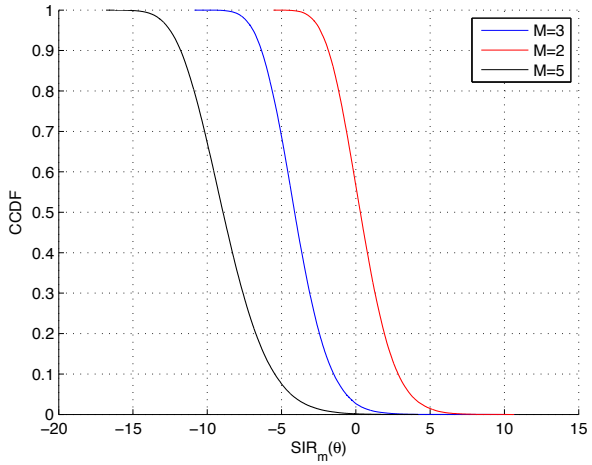

Fig. 2. CCDF of the received SIR from a single path at any random transmission direction θ.

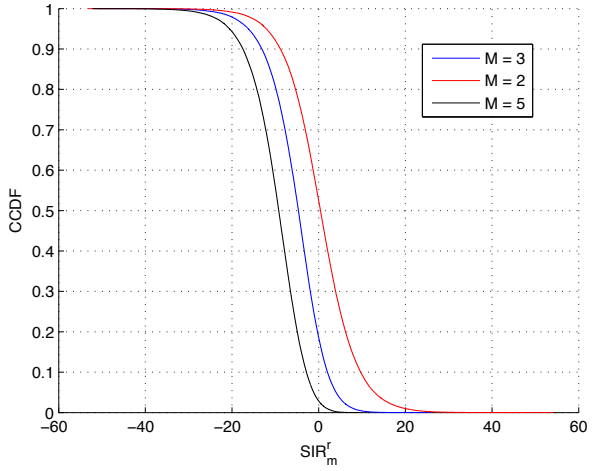

Fig. 3. CCDF of the received SIR by the eavesdropper.

available, we will compare the performance of this scheme to the secrecy performance of MIMO precoding with Artificial Noise (AN) [13].

IV. Secrecy Performance

In this analysis, we consider a system with three users ($M = 3$) receiving their signals through six paths ($L = 6$) and the base-station is equipped with a single antenna array of ten elements ($N = 10$). Also, we assume that the fading coefficients of the eavesdropper's channel and the legitimate user's channel are uncorrelated. The analysis shown here is based on numerical system simulation, as there is no closed mathematical form for the relation between the SIR and the system parameters yet.

Figure 2 shows the Complementary Cumulative Distribution Function (CCDF) of $SIR_m(\theta)$ from (10). We can see that, with probability 95%, the power of the interfering streams will be much larger than the power of the desired stream (i.e., $P\{SIR_m(\theta) < 0 \text{ dB}\} = 0.95$). These results induce that the eavesdropper's channel has lower capacity than the legitimate user's channel. Notice that the effect of the noise is not considered in these results. The figure also shows the case where the system only has two users, where we have $P\{SIR_m(\theta) < 0 \text{ dB}\} = 0.5$. Moreover, when the number of users reaches 5, the received SIR drops dramatically.

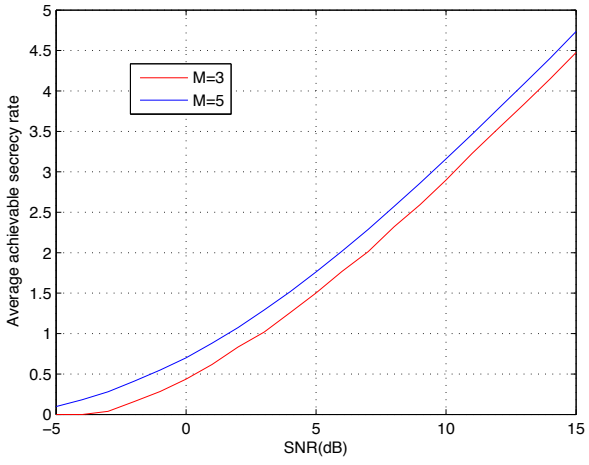

Fig. 4. The change of the average achievable secrecy rate R_s with the SNR of the legitimate user's channel γ_l.

The same analysis is carried for the received SIR at the eavesdropper, SIR^r_m, expressed by (12). In Figure 3, we consider the worst case scenario, where the eavesdropper is aligned with the legitimate user (i.e., both are receiving the same number of paths and from the same directions). We can see from the figure that the eavesdropper's channel suffers from high degradation with a high probability. Here, we refer to the degradation of the channel as the decrease happens to the value of the received SINR.

Figure 4 shows the change of the average achievable secrecy rate expressed by (13), with the change of γ_l. It is clear that we still can achieve a positive secrecy rate even with a very noisy channel on the legitimate user side.

On the other hand, Figure 5 compares the probability of achieving positive secrecy rates in the case of using DM, with the AN scheme from [13]. We can see that even with low number of users $M = 3$, the probability of having a positive secrecy rate is comparable to the AN scheme. Also, just by increasing the number of users ($M = 5$), DM outperforms AN scheme. Besides, we can see that after a certain number of transmit antennas N_a, the enhancement of the performance of the AN scheme is no much significant.

Note that, increasing the number of transmit antennas for AN adds hardware and processing complexity. While, for DM, increasing the number of users M adds processing complexity only, and keeps the hardware unchanged.

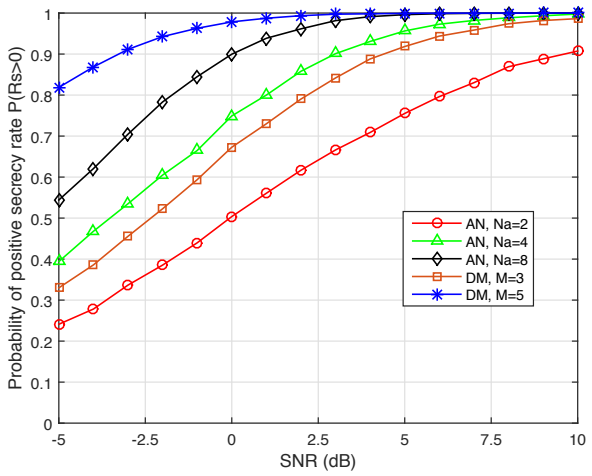

Fig. 5. The probability of achieving a positive secrecy rate $P(R_s > 0)$.

V. Conclusion

Here, we introduce a multi-user access system level design that uses MDDM as a transmission technique. The proposed system design exploits the dispersive nature of the wireless channel to create a position-based secure communication link. The proposed system is able to degrade the eavesdropper channels, even if the eavesdropper does not experience any noise. The amount of degradation increases with the increase of the number of users in the system. Moreover, the secrecy analysis shows that the proposed system is always able to achieve a positive secrecy rate with a high probability. We also show that the DM scheme outperforms the ordinary AN scheme.

Acknowledgment

The research work of Mohammed Hafez and Tamer Khattab was made possible by a grant from Qatar National Research Fund, QNRF, (a member of Qatar Foundation, QF) under the National Priorities Research Program, NPRP, grant number NPRP 6-1326-2-532. The statements made herein are the sole responsibilities of the authors.

References

[1] J. Mietzner, R. Schober, L. Lampe, W. H. Gerstacker, P. A. Hoeher, "Multiple-antenna techniques for wireless communications - a comprehensive literature survey," *IEEE Communications Surveys and Tutorials*, vol. 11, no. 2, pp. 87–105, June 2009.

[2] A.D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[3] C. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 29, pp. 656–715, 1949.

[4] M. F. Hanif, L. Tran, M. Juntti, and S. Glisic, "On Linear Precoding Strategies for Secrecy Rate Maximization in Multiuser Multi-antenna Wireless Networks," *IEEE Transactions on Signal Processing*, vol. 62, no. 14, pp. 3536–3551, July 2014.

[5] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit Antenna Selection for Security Enhancement in MIMO Wiretap Channels," *IEEE Transactions on Communications*, vol. 61, no. 1, pp. 144–153, January 2013.

[6] C. Wu, P. Lan, P. Yeh, C. Lee, and C. Cheng, "Practical Physical Layer Security Schemes for MIMO-OFDM Systems Using Precoding Matrix Indices," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1687–1700, September 2013.

[7] T. Akitaya, S. Asano, and T. Saba, "Time-domain Artificial Noise Generation Technique Using Time-domain and Frequency-domain Processing for Physical Layer Security in MIMO-OFDM Systems," *IEEE International Conference on Communications (ICC)*, pp. 807 – 812, June 2014.

[8] J. Tang, H. H. Song, F. Pan, H. Wen, B. Wu, Y. Jiang, X. Guo, and Z. Chen, "A MIMO Cross-layer Precoding Security Communication System," *IEEE Conference on Communications and Network Security (CNS)*, CA, USA, pp. 500 –501, October 2014.

[9] G. Geraci, J. Yuan, and I. B. Collings, "Large System Analysis of the Secrecy Sum-Rates with Regularized Channel Inversion Precoding," *IEEE Wireless Communications and Networking conference (WCNC)*, Paris, France, pp. 533 –537, April 2012.

[10] S. A. A. Fakoorian and A. L. Swindlehurst, "Dirty Paper Coding Versus Linear GSVD-Based Precoding in MIMO Broadcast Channel with Confidential Messages," *IEEE Global Communications Conference (GLOBECOM)*, TX, USA, pp. 1–5, December 2011.

[11] S. A. A. Fakoorian and A. L. Swindlehurst, "Optimal Power Allocation for GSVD-Based Beamforming in the MIMO Gaussian Wiretap Channel," *IEEE International Symposium on Information theory (ISIT)*, MA, USA, pp. 2321–2325, July 2012.

[12] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust Beamforming for Secure Communication in Systems With Wireless Information and Power Transfer," *IEEE Transactions on Wireless Communications*, vol. 13, no. 8, pp. 4599–4615, August 2014.

[13] N. R. Zurita, M. Ghogho, and D. McLernon, "Outage Probability Based Power Distribution Between Data and Artificial Noise for Physical Layer Security" *IEEE Signal Processing Letters*, vol. 19, no. 2, pp. 71–74, February, 2013.

[14] N. Yang, M. Elkashlan, T. Q. Duong, J. Yuan, and R. Malaney, "Optimal Transmission with Artificial Noise in MISOME Wiretap Channels" *IEEE Transactions on Vehicular Technology*, Early Access, April, 2015.

[15] M. Daly and J. T. Bernhard, "Directional Modulation Technique for Phased Arrays," *IEEE Transactions on Antennas and Propagation*, vol. 57, no. 9, pp. 2633–2640, September 2009.

[16] M. Daly and J. T. Bernhard, "Directional Modulation and Coding in Arrays," *IEEE International Symposium on Antennas and Propagation (APSURSI)*, Spokane, WA, USA, pp. 1984 –1987, July 2011.

[17] M. Daly, E. L. Daly , and J. T. Bernhard, "Demonstration of Directional Modulation Using a Phased Array," *IEEE Transactions on Antennas and Propagation*, vol. 58, no. 5, pp. 1545–1550, May 2010.

[18] M. Daly and J. T. Bernhard, "Beam-steering in Pattern Reconfigurable Arrays Using Directional Modulation," *IEEE Transactions on Antennas and Propagation*, vol. 58, no. 7, pp. 2259–2265, July 2010.

[19] N. Valliappan, A. Lozano, and R. W. Heath, "Antenna Subset Modulation for Secure Millimeter-Wave Wireless Communication," *IEEE Transactions on Communications*, vol. 61, no. 8, pp. 3231–3245, August 2013.

[20] T. Hong, M. Z. Song, and Y. Liu, "Dual-Beam Directional Modulation Technique for Physical-Layer Secure Communication," *IEEE Transactions on Antennas and Propagation*, vol. 10, pp. 1417–1420, December 2011.

[21] O. N. Alrabadi and G. F. Pedersen, "Directional Space-Time Modulation: A Novel Approach for Secured Wireless Communication," *IEEE International Conference on Communications (ICC)*, pp. 3554 – 3558, June 2012.

[22] Y. Ding and V. F. Fusco, "A Vector Approach for the Analysis and Synthesis of Directional Modulation Transmitters," *IEEE Transactions on Antennas and Propagation*, vol. 62, no. 1, pp. 361–370, January 2014.

[23] Y. Ding and V. F. Fusco, "Establishing Metrics for Assessing the Performance of Directional Modulation Sysytems," *IEEE Transactions on Antennas and Propagation*, vol. 62, no. 5, pp. 2745–2755, May 2014.

[24] M. Hafez and H. Arslan, "On Directional Modulation: An Analysis of Transmission Scheme with Multiple Directions," *IEEE International Conference on Communications (ICC)*, London, UK, pp. 459–463, June 2015.

[25] S. Boyd and L. Vandenberghe, *"Convex Optimization"*, Cambridge University Press, 2004.

[26] T. Hayashi, M. Nakano, and A. Yamaguchi, "Novel AoA Estimation Method Using Delay Profile in Downlink" *International Workshop on Antenna Technology (iWAT)* pp. 35–38, Karlsruhe, Germany, 4–6 March, 2013.