Secure Spatial Multiple Access Using Directional Modulation

Mohammed Hafez, *Student Member, IEEE*, Marwan Yusuf, Tamer Khattab, *Member, IEEE*,
Tarek Elfouly, *Senior Member, IEEE*, and Hüseyin Arslan, *Fellow, IEEE*

***Abstract*— In this paper, we introduce a secure multiple access scheme, which exploits the multipath structure of the channel to create a multi-user interference environment. The generated interference enables legitimate users to share time and frequency resources over spatially secure communication links. Utilizing directional modulation, we ensure secrecy for legitimate users against eavesdropping while preserving mutual confidentiality between the legitimate users themselves. Moreover, we introduce a complementary scheme for covering the non-selective channel case. The scheme uses directional modulation in coordinated multi-point transmission to provide location-specific secure communication to legitimate users. We characterize the achievable performance using a newly defined metric called vulnerable region. We provide analysis for the achievable secrecy rate, secrecy outage probability, and channel correlation effect on the secrecy performance for the proposed scheme. Furthermore, the effect of the channel spatial diversity, channel estimation error, and the number of legitimate users on the secrecy performance is studied.**

***Index Terms*— Antenna arrays, coordinated multi-point, directional modulation, physical-layer security.**

I. Introduction

TIME and frequency resources for wireless communications have proven to be inadequate for coping with the current high rate demand on wireless technology. The space domain has been introduced as a third resource allowing communication systems to reach higher rates. By implementing multiple antennas (MA) [1], either on the transmitter side, the receiver side or both, new resources (i.e. degrees of freedom) are introduced to wireless systems. Based on their construction, MA systems can be considered as a single unit (i.e., antenna arrays) or separate uncorrelated units. The single unit structure provides a flexible mechanism to transmit or receive wireless signals based on a spatial direction of interest, while the uncorrelated structure gives the opportunity to improve quality-of-service (QoS).

From another perspective, the widespread use of wireless technology and its broadcast nature raised a flag on the privacy of information transferred over the wireless network. Rising as a promising paradigm to the traditional ciphering algorithms, physical layer security provides another level of protection [2]–[4]. One way to ensure secrecy, at the physical layer level, is to utilize the random nature of the communication channel. This approach has been made more feasible through the extra resources provided by MA systems.

Many algorithms have been proposed to provide a robust secure communication link via utilizing the physical layer properties of the MA systems [5]. Most of the studied algorithms can be split into two main categories, namely "*precoding based*" and "*array based*", while a few others do not fall under these categories. Examples of these algorithms are key generation using precoding matrix indices [7] and time-domain artificial noise generation [8].

Lately, most of the literature focuses on *precoding based* schemes, where the transmitter constructs a precoding matrix, based on its knowledge about the channel realizations, to ensure the signal is decodable only through the channel of the legitimate user [9], [10]. Construction of such precoding matrix depends mainly on the amount of knowledge of the channel at the transmitter. If the transmitter has information about the eavesdropper's 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 receivers. The transmitter selects only the sub-channels where the legitimate receiver has advantage over the eavesdropper for message exchange [11], [12]. On the other side, ZF generates a precoding matrix that prevents confidential messages from being transmitted towards the eavesdropper [13]. When the transmitter does not have knowledge of the channel of the eavesdropper, it attempts to provide secrecy to the legitimate message by embedding a jamming signal (e.g. *artificial noise* (AN)) into the null-space of the legitimate channel [14], [15]. With the assumption of independence between the legitimate and the eavesdropper channels, the transmitter presumes that the AN

Manuscript received January 23, 2017; revised July 22, 2017 and October 16, 2017; accepted October 24, 2017. Date of publication November 3, 2017; date of current version January 8, 2018. This work was supported in part by the National Science Foundation under Grant ECCS-1247503 and in part by the Scientific and Technological Research Council of Turkey under Grant 114E244. The work of M. Hafez and T. Khattab was supported by the Qatar National Research Fund, QNRF (a member of the Qatar Foundation, QF) under Grant NPRP 7-923-2-344. Part of this paper was presented at the IEEE International Conference on Communications, May 2016 [37]. The associate editor coordinating the review of this paper and approving it for publication was A. Zaidi. *(Corresponding author: Mohammed Hafez.)*

M. Hafez and H. Arslan are with the Department of Electrical Engineering, University of South Florida, Tampa, FL 33620 USA (e-mail: mhafez@mail.usf.edu; arslan@usf.edu).

M. Yusuf is with the School of Engineering and Natural Sciences, Istanbul Medipol University Beykoz, 34810 Istanbul, Turkey (e-mail: marwan.med7at@gmail.com).

T. Khattab is with the Department of Electrical Engineering, Qatar University, Doha, Qatar (e-mail: tkhattab@ieee.org).

T. Elfouly is with the Department of Computer Science and Computer Engineering, Qatar University, Doha, Qatar (e-mail: tarekfouly@qu.edu.qa).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TWC.2017.2768419

will leak into the received signal of the eavesdropper causing some degradation in its performance.

Recently, the ongoing research for the 5G evolution suggests moving to a higher range of frequency bands (i.e., mm-wave range) [16]. The characteristics of the wireless communication channel change significantly at this range of frequencies. Sparse channel structure and high attenuation factors, render the integration of analog beam-forming algorithms to the system more feasible and highly recommended [17]. Consequently, *array based* secrecy algorithms are gaining momentum as an important topic of research.

Phased arrays have been used to increase the gain of the transmitted stream along one direction in space while reducing the gain for all other directions. Such approach can be used as a source to achieve secrecy at the physical layer while maintaining high power efficiency. Despite the achieved low gain in other spatial directions, an eavesdropper with a very sensitive receiver can retrieve the data. In order to avoid this issue, *directional modulation* (DM) was proposed [18].

In DM, the antenna pattern is treated as a spatial complex constellation. The magnitude and phase of the antenna pattern, at a certain desired direction, is set to have the same value of the data symbol. Contrary to the conventional beamforming, which provides directional power scaling, DM technique is simultaneously distorting the constellation of the same signals in all directions other than the desired one.

This technique was first introduced in [18] and [19], where it was proposed to move the modulation process from the baseband to the radio frequency (RF) stage. Afterwards, the same authors demonstrated this idea in [20] and [21]. In [22], quadrature modulated streams were separately encoded at the baseband. When the two streams combine in the far field, the received IQ data can be only detected along a predefined spatial direction. Later, using a limited number of the available antenna elements was proposed in [23]. The number and the position of the selected elements were changed randomly for each transmitted symbol. This random selection assures the distortion of the transmitted signal towards undesired directions.

We can consider some other perspectives to define the difference between conventional beamforming and DM. One of these perspectives is the rate of change of the complex weights of the antenna array. For conventional beamforming, the rate is based on the rate of change of the communication channel. In contrast, in the case of DM, the rate is related to the transmitted data rate [24]. In [25], the authors used vector-domain analysis to measure the performance of the DM technique. The authors defined two categories for the behavior of DM algorithms. The first category includes *"Static"* algorithms, where the generated antenna pattern does not change over time. This could be a threat to the system if the eavesdropper was able to identify the randomization pattern along its direction. The other category is *"Dynamic"* algorithms, where the same constellation point can be transmitted using a different pattern each time, making it hard to track and decipher. In order to evaluate the performance of such system, some parameters based on bit-error-rate (BER), error-vector-magnitude (EVM), and secrecy rate were suggested in [26]. A new approach for the synthesis of DM using singular value decomposition (SVD) was proposed in [27] based on identifying the similarities and differences between multiple-input-multiple-output (MIMO) and DM technologies.

In our previous work [28], we introduced the multiple-directions-DM (MDDM) transmission scheme. 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 antenna elements. Also, the achievable secrecy rate increases when increasing the number of transmitted streams. Moreover, MDDM does not necessitate the implementation of any special algorithms at the receiver side.

A. Major Contributions

Up till now, DM was only discussed from the algorithm construction perspective, and to the extent of the author's knowledge, there has been no study of the employment of DM algorithms, into a multi-user system level. As a result of this, we propose the following,

- We introduce a system level design based on our previously 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.
- We also deduce the secrecy rate and outage probability for the proposed scheme. Besides, we compare the performance of this scheme with the performance of AN precoding, as they share the same assumptions about the channel knowledge.
- For open environments where scatterers are limited or line-of-sight dominates the communication, a coordinated multi-point (CoMP) transmission scheme is proposed. Using multiple geographically separated base stations to transmit the signal allows the data to be decodable only at the intersection of their information beams while being distorted at other locations.
- In this context, we define a metric called *vulnerable region* (VR) that refers to the area within which a receiver can access and decode the signal being transmitted to legitimate users.

B. Organization

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 while the CoMP scheme is introduced in Section IV. Section V discusses the system performance. Finally, we conclude the paper in Section VI.

C. Notation

Throughout this paper, vectors are represented using lowercase bold-face letters, matrices are uppercase bold-face letters, and non-bold letters are used for scalars. The superscripts $(.)^{\dagger}$, $(.)^{T}$, $(.)^{-1}$ stand for the conjugate-transpose, transpose, and inverse operations, respectively. $[.]^{+} = \max(., 0)$ and $\mathbb{C}$ represents the complex numbers domain.

II. MDDM Transmission System Design

We consider a broadcast channel with a single source (base station) and L destinations; namely, transmission directions. Each direction has its own independent digitally modulated data stream, $x_i(k)$, and 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. The base station uses a linear antenna array, with N elements, for transmission.

Based on the idea of directional modulation, we need to set $\mathbf{w} = [w_1(k), w_2(k), \ldots, w_N(k)]^T$, so that $f(\theta_i, k) = x_i(k)$, where $\mathbf{w}$ 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, which is received by the receiver located at a certain direction θ, where

$$f(\theta, k) = \mathbf{h}^\dagger(\theta)\mathbf{w}(k), \tag{1}$$

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

and $\mathbf{h}^\dagger(\theta)$ is the array steering vector for a receiver positioned at direction θ. Here, d represents the spacing between antenna elements, and λ is the carrier wave-length.

Let us define $\mathbf{f}$ as the column vector that contains the desired pattern values, for each of the desired transmission directions.

$$\mathbf{f} = [f(\theta_1, k), f(\theta_2, k), \ldots, f(\theta_L, k)]^T$$
$$= \mathbf{H}^\dagger\mathbf{w} = \begin{bmatrix} \mathbf{h}^\dagger(\theta_1) \\ \mathbf{h}^\dagger(\theta_2) \\ \vdots \\ \mathbf{h}^\dagger(\theta_L) \end{bmatrix} [w_1(k), w_2(k), \ldots, w_N(k)]^T, \tag{3}$$

where, $\mathbf{H} \in \mathbb{C}^{N\times L}$, 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 [29], we find that

$$\mathbf{w}_{\text{ln}} = \mathbf{H}\left(\mathbf{H}^\dagger\mathbf{H}\right)^{-1}\mathbf{f}. \tag{4}$$

By replacing $\mathbf{f}$ with $\mathbf{x} = [x_1(k), x_2(k), \ldots, x_L(k)]^T$, we can produce the required weights to modulate the resulting antenna pattern, so that the pattern takes the desired values at the desired directions. Based on this, the value of the received pattern can be rewritten as,[1]

$$f(\theta, k) = \mathbf{h}^\dagger(\theta)\mathbf{H}(\mathbf{H}^\dagger\mathbf{H})^{-1}\mathbf{x}(k) = \mathbf{h}^\dagger(\theta)\mathbf{D}\,\mathbf{x}(k). \tag{5}$$

The performance of the MDDM scheme is evaluated using the average achievable secrecy rate [2],

$$R_{\text{secrecy}} = R(\theta_{\text{l}}) - R(\theta_{\text{a}}), \tag{6}$$

where,

$$R(\theta) = \log_2(1 + \gamma(\theta)), \tag{7}$$

$$\gamma(\theta) = \frac{|\mathbf{h}^\dagger(\theta)\mathbf{d}_{\text{l}}|^2\,\sigma_{\text{l}}^2}{\sum_{j\neq l}|\mathbf{h}^\dagger(\theta)\mathbf{d}_j|^2\sigma_j^2 + \sigma_n^2}, \tag{8}$$

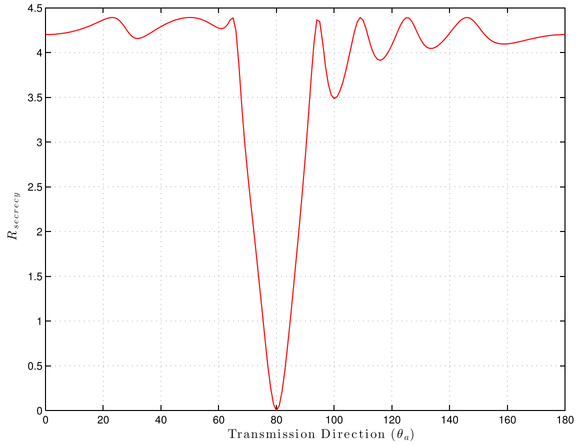

Fig. 1. Secrecy rate based on the SINR of the received symbols.

$\gamma(\theta)$ is the received signal-to-interference-plus-noise-ratio (SINR) at the direction θ, θ_{l} is the desired transmission direction, θ_{a} is any arbitrary direction, $\mathbf{d}_j$ is the j^{th} column of the precoding matrix $\mathbf{D}$ with $j \in \{1, 2, \ldots, L\}$, σ_j^2 is the power assigned to the j^{th} stream and σ_n^2 is the noise power at the receiver. It is assumed that the total transmission power is constrained to a maximum value, $\mathcal{P}$, (i.e., $\sum_{j=1}^{L}\sigma_j^2 \leq \mathcal{P}$).

Fig. 1 shows the secrecy performance in terms of the secrecy rate in (6). For the shown results, $N = 10$ with half wavelength separation, $L = 4$, $\theta_l = 80^\circ$, $\sigma_{\text{l}}^2/\sigma_n^2 = 10$, and the noise power at the eavesdropper $\sigma_{n_e}^2 = 0$ dB. The figure shows high secrecy gain outside the main lobe, which indicates that the data obtained at a non-intended direction can not be detected reliably. Moreover, it is shown that communication is not secure along the direction of the legitimate user. However, the multipath nature of the channel can be used to generate a pre-coding scheme that ensures secrecy for this direction; this will be discussed in a later section.

III. Secure Multiple Access

The problem discovered in the previous section is that, if the eavesdropper is aligned with one of the transmission directions, it will be able to receive a clear decodable constellation of the transmitted data. This will be mitigated by implementing the multipath nature of the channel into the generation of the MDDM signal. This section will show how the signal can be constructed at the base station to provide MDDM while achieving secrecy based on locations rather than just directions of the legitimate receiver. The section discusses the secrecy issues for different scenarios.

A. System Model

Consider a single base station equipped with an N elements linear antenna array. The base station is serving M legitimate users; each is equipped with a single antenna. We assume the existence of a passive eavesdropper, which is equipped with an arbitrary number of antennas N_E.

The signals transmitted by the M users are received through L different paths. Here, we assume space reciprocity, i.e., the

[1] Note that, the usage of any other antenna array structure is applicable, as long as the appropriate steering vector $\mathbf{h}^\dagger(\theta)$ is used for the generation of the weights $\mathbf{w}$.

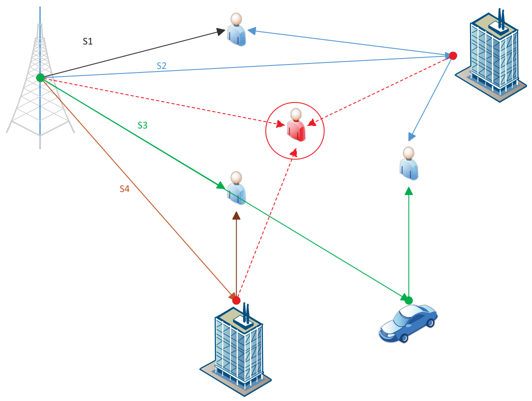

Fig. 2. A system illustration with 3 legitimate users (Blue) and one circled eavesdropper (Red). Legitimate users receive signals from 2 paths (Solid colored lines), and the eavesdropper receive it through 3 paths (Red dashed lines).

signal transmitted by the base station is also received by the users through the same L paths. Note that; L is the maximum number of independent paths in the system. [2]

Let us define α_{ml} as the gain coefficient of the l^{th} path that is delivered to the m^{th} user. We assume that all α_{ml}'s are available at the base station through feedback from all users. Each path is delivered with θ_l angle-of-departure (AoD), these AoD's are evaluated at the base station, which can be done using one of the methods according to [30].

The eavesdropper receives signals through P paths, we also define β_p as the gain coefficient of the p^{th} path to eavesdropper. We assume that all β_p's and α_{ml}'s are also available at the eavesdropper. This is considered as worst-case scenario where the eavesdropper has acquired the information about the channel state information (CSI) of the legitimate link through feedback channels.

Fig. 2 shows an example illustration for such system. Here, we are considering random small scale fading effect, which is modeled as a Rayleigh fading. Then, the gains are modeled as i.i.d Gaussian random variables.

The effect of the large scale fading (Path-loss and Shadowing) is not considered. This assumption is based on considering a noiseless channel for the eavesdropper. In such situation, for a certain eavesdropper location, the average path-loss affecting both the desired signal and interfering signals will almost have the same value, which means that the path-loss will not affect the value of the received signal-to-interference-ratio (SIR).

B. Construction of the Transmitted Signal

We define matrices $\mathbf{A} = \{\alpha_{ml}\}_{M\times L}$ and $\mathbf{H} = \{\mathbf{h}(\theta_l)\}_{1\times L}$. With the availability of $\mathbf{A}$ and $\mathbf{H}$ at the base station, the transmitted antenna pattern can be synthesized as

$$f(\theta,k) = \mathbf{h}^\dagger(\theta)\mathbf{H}[\mathbf{H}^\dagger\mathbf{H}]^{-1}\mathbf{A}^\dagger[\mathbf{A}\mathbf{A}^\dagger]^{-1}\mathbf{x}(k) = \mathbf{h}^\dagger(\theta)\mathbf{D}\,\mathbf{x}(k), \tag{9}$$

where $\mathbf{x} \in \mathbb{C}^{M\times 1}$ is a vector that contains the users data. Then, the SIR for the m^{th} transmitted signal $x_m(k)$ at any arbitrary direction θ can be calculated using (8), with $\mathbf{D} = \mathbf{H}[\mathbf{H}^\dagger\mathbf{H}]^{-1}\mathbf{A}^\dagger[\mathbf{A}\mathbf{A}^\dagger]^{-1}$.

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.

C. Eavesdropper with a Single Antenna

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

$$r(k) = \mathbf{e}\,\tilde{\mathbf{H}}^\dagger\,\mathbf{D}\,\mathbf{x}(k) = \mathbf{v}\times\mathbf{x}(k), \tag{10}$$

where $\mathbf{e} = \{\epsilon_q\}_{1\times Q}$, ϵ_q is the complex gain of the q^{th} received path, and Q is the total number of received paths. $\tilde{\mathbf{H}} = \{\mathbf{h}(\theta_q)\}_{1\times Q}$ is the steering matrix corresponding to the transmission directions θ_q with $q \in \{1,2,\ldots,Q\}$. Then, considering the decoding of the m^{th} message, the received SINR can be calculated as

$$\gamma^m = \frac{|\upsilon_m|^2\,\sigma_m^2}{\sum_{j\neq m}|\upsilon_j|^2\sigma_j^2 + \sigma_{n_m}^2}, \tag{11}$$

where υ_j is the j^{th} element of $\mathbf{v}$, which represents a coefficient affecting the data of the j^{th} user.

For the m^{th} legitimate user $\{\mathbf{e}\equiv\mathbf{a}_m, \tilde{\mathbf{H}}\equiv\mathbf{H}\}$, where $\mathbf{a}_m$ is the m^{th} row of $\mathbf{A}$ representing the channel of the m^{th} user. This will result in,

$$\begin{aligned}\mathbf{v} &= \mathbf{a}_m\mathbf{H}^\dagger\mathbf{D},\\ &= \mathbf{a}_m\mathbf{H}^\dagger\mathbf{H}[\mathbf{H}^\dagger\mathbf{H}]^{-1}\mathbf{A}^\dagger[\mathbf{A}\mathbf{A}^\dagger]^{-1},\\ &= \mathbf{a}_m\mathbf{A}^\dagger[\mathbf{A}\mathbf{A}^\dagger]^{-1},\end{aligned} \tag{12}$$

This leaves us with,

$$\begin{aligned}\upsilon_m &= 1,\\ \upsilon_{j\neq m} &= 0,\\ \gamma^m_{\text{Legit}} &= \sigma_m^2/\sigma_{n_m}^2,\end{aligned} \tag{13}$$

where γ^m_{Legit} is the SINR at the m^{th} legitimate user.

Otherwise, if there is a mismatch between the channel used at the transmitter and the actual channel, the legitimate receiver will experience some multi-user interference. The effect of multi-user interference on the secrecy performance will be discussed in Subsection E.

In the case of an eavesdropper $\{\mathbf{e}\equiv\mathbf{b}, \mathbf{v} = \mathbf{b}\tilde{\mathbf{H}}^\dagger\mathbf{D}\}$, where $\mathbf{b} = \{\beta_p\}_{1\times P}$. The received SINR for this case would be,

$$\gamma^m_{\text{Eaves}} = \frac{|\mathbf{b}\tilde{\mathbf{H}}^\dagger\mathbf{d}_m|^2\sigma_m^2}{|\mathbf{b}\tilde{\mathbf{H}}^\dagger\mathbf{D}_m|^2\sigma_{int}^2 + \sigma_{n_e}^2} \tag{14}$$

where $\mathbf{d}_m$ is the m^{th} column of $\mathbf{D}$, representing the precoding vector for the m^{th} data stream. $\mathbf{D}_m$ is the rest of the precoding matrix $\mathbf{D}$ after removing $\mathbf{d}_m$. σ_{int}^2 is the transmission power associated with the $M-1$ interfering streams, and $\sigma_{n_e}^2$ is the noise power at the eavesdropper side.

[2] In a practical system, some of the users may experience less diverse channel. For these situations, the gain coefficients corresponding to the non-utilized paths by a user will be considered as zeros.

In order to consider the minimum guaranteed secrecy, we assume that the eavesdropper has a noiseless channel (i.e., $\sigma_e^2 = 0$).[3] Then, the achievable secrecy rate can be defined as,

$$\begin{aligned} R_s &= R_l - R_e, \\ &= \left[\log_2(1+\gamma_{\text{Legit}}^m) - \log_2(1+\gamma_{\text{Eaves}}^m)\right]^+. \end{aligned} \tag{15}$$

The performance of the system in terms of average achievable secrecy rate and secrecy outage probability will be investigated in the next section. Consider Theorem 1 for the distribution of γ_{Eaves}^m and R_e.

Theorem 1: The achievable rate at the eavesdropper follows a Logistic distribution, Logistic$(\log(\frac{\varphi}{\sigma_{int}^2}), \frac{1}{M})$*, hence, the received SINR follows a Shifted-Log-Logistic distribution.*

Proof: The proof is conducted in Appendix A. ■

Here, the eavesdropper is considered entirely passive, and the information about its channel is not available to any of the legitimate users. As part of the performance evaluation, it will be compared to the performance of MIMO precoding with AN, while considering the optimal power distribution between data and AN [14].

D. Eavesdropper with an Arbitrary Number of Antennas N_E

The case of an eavesdropper with multiple receiving antennas can be thought of as equivalent to a network with multiple eavesdroppers. It represents the worst-case scenario of the multiple-eavesdroppers case, where all the eavesdroppers have perfect cooperation channel. On the other hand, it must be noted that the scenarios studied in the sequel do not consider the cases of active eavesdroppers.

Considering the AN system, and due to the aforementioned assumption of the availability of **A** at the eavesdropper, the eavesdropper can reconstruct the pre-coding matrix on its side. For the case where $\{N_E < N_A\}$, the eavesdropper will not be able to separate the legitimate data from the noise components. When $\{N_E \geq N_A\}$ and assuming knowledge of the pre-coding matrix, the eavesdropper has enough information to be able to extract the legitimate data from the noise imposed over it [31]. Here, N_A represents the number of antennas at the transmitter of the AN scheme, which corresponds to M in our proposed scheme.

Redefine the received signal at the eavesdropper as,

$$\mathbf{r}_e(k) = \mathbf{B}\,\tilde{\mathbf{H}}^\dagger\,\mathbf{D}\,\mathbf{s}(k), \tag{16}$$

where $\mathbf{B} = \{\beta_{np}\}_{N_E \times P}$ and β_{np} represents the gain coefficient of the p^{th} path received by the n^{th} antenna.

For the AN case, the pre-coding matrix **D** is constructed using only statistical information of the channel. This information is fed back to the transmitter, which makes it vulnerable to the eavesdropper. In such case, as stated earlier, the eavesdropper can reconstruct **D** and acquire the transmitted data if it has enough receiving antennas.

For the proposed scheme, and based on equation (9), the transmission directions, embedded in **H**, goes into the construction of the precoding matrix **D**. **H** is assumed to be exclusively known at the base station.[4] Due to the lack of knowledge of **H** at the eavesdropper side, it will not be able to perfectly reconstruct **D** and extract the legitimate data, even for the case where $\{N_E \geq M\}$. Later, we will also show that random generation of **H** will not be beneficial to correctly extract the legitimate data.

E. Multiple Access Secrecy Rate

Another concern, for the multiple access systems, is the secrecy sum-rate. The secrecy sum-rate is calculated based on the amount of data leaked from one user to the other users in the system. The achievable secrecy sum-rate is obtained by considering the worst-case scenario, where for each legitimate user m the remaining $M-1$ users are considered as collaborative eavesdroppers [32]. This case is equivalent to a multi-input, single-output, multi-eavesdropper (MISOME) wiretap channel [33]. The achievable secrecy sum-rate R_{sum} is given by,

$$R_{sum} = \sum_{m=1}^{M} \left[\log_2(1+\gamma_m) - \log_2(1+\gamma_{\hat{m}})\right]^+. \tag{17}$$

Replacing **b** with $\mathbf{a_m}$ in equation (14) and based on [32], we can define,

$$\gamma_m = \frac{|\mathbf{a}_m \mathbf{H}^\dagger\,\mathbf{d}_m|^2}{\sum_{j\neq m} |\mathbf{a}_m \mathbf{H}^\dagger\,\mathbf{d}_j|^2 + \sigma_{n_m}^2}, \tag{18}$$

$$\gamma_{\hat{m}} = ||\mathbf{A}_m \mathbf{H}^\dagger\,\mathbf{d}_m||^2 \tag{19}$$

where $\mathbf{A}_m$ is the rest of **A** after removing $\mathbf{a}_m$, and $\mathbf{d}_j$ is the part of the pre-coder related to the j^{th} user data.

Basically, γ_m represents the power of the m^{th} legitimate message at the m^{th} user compared to the interference imposed on it from the other $M-1$ messages. While $\gamma_{\hat{m}}$ represents the leakage of the m^{th} message received by the remaining $M-1$ users.

In the proposed system, the pre-coder zero-forces the M legitimate messages with respect to each other. This means that in the event of perfect knowledge of the users CSI's, the sum rate would be infinite. For more realistic assumption, in the next section, we will consider the case of imperfect CSI knowledge and study its effect on the achievable secrecy sum-rate.

F. Power Allocation

The work in this paper focuses on studying performance evaluation and simulation under equal power allocation, where all transmitted streams are allocated the same power. While this strategy might not result in the optimal system performance, it enables simplicity in terms of practical system implementation as well as tractability in terms of mathematical analysis. The results obtained here can be thought of as a lower bound on the optimal system performance. The system can

[3] The assumption of noiseless eavesdropper channel corresponds to calculating a lower bound on performance.

[4] The estimation process of the directions used for transmission and the generation of the steering vectors are exclusively done at the base-station. This information is not shared at any point during the communication process. This makes it not possible for the eavesdropper to acquire such information.

be further extended to incorporate different power allocations for different directions which will require further studies into different power allocation strategies. This is left as a future expansion of this work.

Here, we are discussing some of the other applicable power allocation strategies. Since the secrecy aspects are the main drive for this work, the focus should be on utility functions such as secrecy rate and secrecy outage probability. Then, the optimization problems can be formulated as follows,

$$\begin{aligned}\{\sigma_1^2, \sigma_2^2, \ldots, \sigma_M^2\} &= \arg \max_{\sigma_1^2,\sigma_2^2,\ldots,\sigma_M^2} R_{sum}\\ \{\sigma_1^2, \sigma_2^2, \ldots, \sigma_M^2\} &= \arg \max_{\sigma_1^2,\sigma_2^2,\ldots,\sigma_M^2} \bar{R}_s\\ \{\sigma_1^2, \sigma_2^2, \ldots, \sigma_M^2\} &= \arg \min_{\sigma_1^2,\sigma_2^2,\ldots,\sigma_M^2} P(\bar{R}_s < \gamma_{th}) \qquad (20)\end{aligned}$$

where $\bar{R}_s = \frac{1}{M}\sum_{i=1}^{M} R_i$ is the average achievable secrecy rate per user. Besides, based on the desired application, various constrains can be imposed on the system. Exemplary constraints may include, but not limited to, total power ($\sum_{m=1}^{M} \sigma_m^2 \leq \mathcal{P}$), average power, average received SINR per user, or enhancing the overall fairness between users.

IV. Coordinated Multi-Point Transmission

CoMP refers to a wide range of techniques that enable dynamic coordination or transmission with multiple geographically separated base stations to enhance the end-user service quality even at cell edges [34], [35]. One of the major categories for CoMP downlink transmission is the joint processing and transmission scheme where data is transmitted simultaneously from all base stations to improve the received signal quality or to cancel interference from other users. To that end, highly detailed feedback is required on the channel properties in a fast manner. Another requirement is the need for very close coordination between the base stations to facilitate combination of data as well as fast switching of the cells.

Here, we assume the lack of knowledge of CSI of all users at all base stations. Each base station only knows the relative direction of each desired user to its location. Moreover, the strict timing coordination can be relaxed since we are sending the same data from all base stations. Hence the delayed signals can be considered equivalent to multi-path components.

Considering a single user system, the received signal at the desired location will be,

$$r_d(t) = \sum_{i=1}^{B} g_i(t - \tau_i) s_{\text{Conf}}(t) + z(t), \qquad (21)$$

where B is the number of base-stations, g_i is the complex channel gain coefficient associated with the transmission of the i^{th} base-station, and τ_i is the corresponding delay. $s_{Conf}(t)$ is the confidential message intended for the legitimate user, and $z(t)$ is the additive Gaussian noise at the receiver.

On the other hand, at any other location the B signals will not be the same due to the directional modulation selectivity which inherently causes interference to all directions outside the information beams,

$$r_d(t) = \sum_{i=1}^{B} g_i(t - \tau_i)\mathbf{h}^{\dagger}(\theta_i)\mathbf{w}(t) + z(t). \qquad (22)$$

Including the knowledge of CSI in the synthesis process of $\mathbf{w}(t)$ at the transmitter would further improve the secrecy performance as shown in previous sections. Allowing the base stations to divide the data into different components each transmitted from a different base station and taking into account pre-compensation of channel effects, the data can be distributed in such a way that the signals can be coherently added at the user's locations to compose the intended data. This division pattern is not unique and does not need to be known at the receiver. Hence, it can be changed continuously to further secure the transmission (i.e., the synthesis process of $\mathbf{w}(t)$ can be changed from one transmission block to another).

A. Vulnerable Region Evaluation

To quantify the location-specific security achieved against eavesdropping in the wireless system, we define a new security metric called the vulnerable region. For a network with M users, VR is defined as the average of the Vulnerable regions of all users in the network

$$VR = \frac{1}{M}\sum_{i=1}^{M} VR_i \qquad (23)$$

where the vulnerable region of the i^{th} user VR_i is the region in which a receiver can decode the data of the i^{th} user. To test our scheme, we generate the location of users randomly within a 2-D grid served by B base stations. The number of users that can be served simultaneously, M, depends on the number of antenna array elements N. We consider the full capacity of the system by letting the number of users equal to the number of antenna array elements (i.e., $N = M$). We divide the area of the network into K square points. Hence, the number of squares in which the information of legitimate users is accessible normalized to the total points of the network gives the vulnerable region metric. We consider the signal at a location to be decodable when the bit error rate (BER) reaches a certain threshold η.

$$VR_i = \frac{1}{K}\sum_{k=1}^{K} U(\eta - BER_k) \qquad (24)$$

where $U(.)$ is the unit step function. The threshold η and the ratio between k and the total area of the covered grid can be chosen based on the secrecy requirement of the system.

V. Secrecy Performance

Here, we assume that the entries of $\mathbf{A}$ and $\mathbf{B}$ are independently identically distributed (i.i.d.) and they follow a complex Gaussian distribution with zero mean and a unit variance. Moreover, $\mathbf{A}$ and $\mathbf{B}$ are totally uncorrelated, which is a valid assumption unless the legitimate user and the eavesdropper are co-located.

For our system performance results, all users are assumed to be assigned an equal transmission power, $\sigma_j^2 = \frac{\mathcal{P}}{M}, \forall j \in$

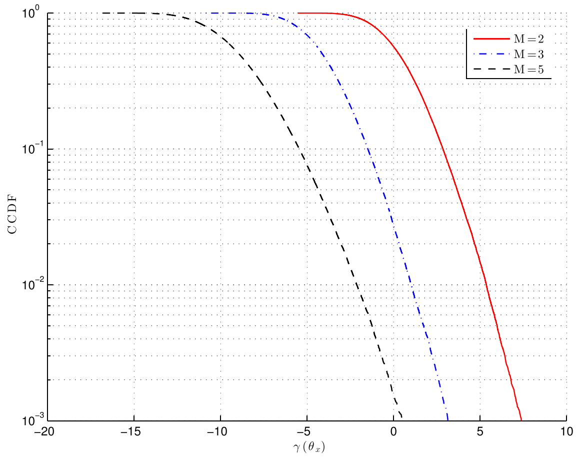

Fig. 3. CCDF of the received SINR from a single path at any random transmission direction θ_x.

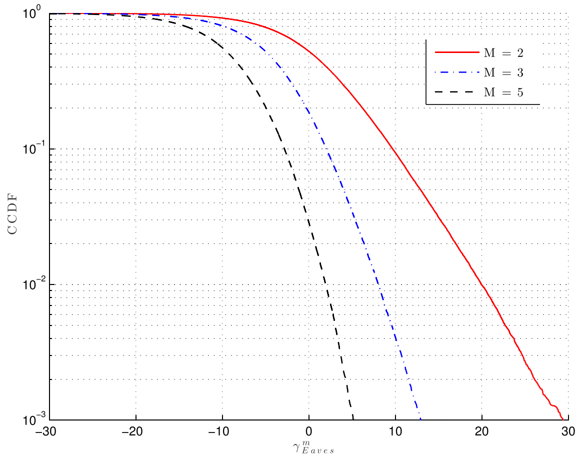

Fig. 4. CCDF of the received SINR by the eavesdropper.

$\{1, 2, \ldots, M\}$. The analysis of the power allocation for each user is not considered for this work. Also, the channel of the eavesdropper is always assumed to be noiseless $\sigma^2_{n_e} = 0$ as a secrecy worst-case scenario.

A. Eavesdropper with a Single Antenna

Fig. 3 shows the complementary cumulative distribution function (CCDF) of $\gamma(\theta)$ from (8), with a precoding matrix $\mathbf{D} = \mathbf{H}[\mathbf{H}^\dagger\mathbf{H}]^{-1}\mathbf{A}^\dagger[\mathbf{A}\mathbf{A}^\dagger]^{-1}$. It shows that with a very high probability, the power of the interfering streams will be much larger than the power of the desired stream (i.e., $P\{\gamma(\theta) < 0 \text{ dB}\}$). These results induce that the eavesdropper's channel has lower capacity than the legitimate user's channel. Notice that the effect of the noise at the eavesdropper is not considered in these results, which makes it the best case scenario for the received SINR. It can be directly inferred that with the increase in the number of users in the system, the received SINR drops dramatically.

The same analysis was carried for the received SINR at the eavesdropper, γ^m_{Eaves}, expressed by (14). In Fig. 4, the eavesdropper's channel suffers from high degradation with a high probability.[5]

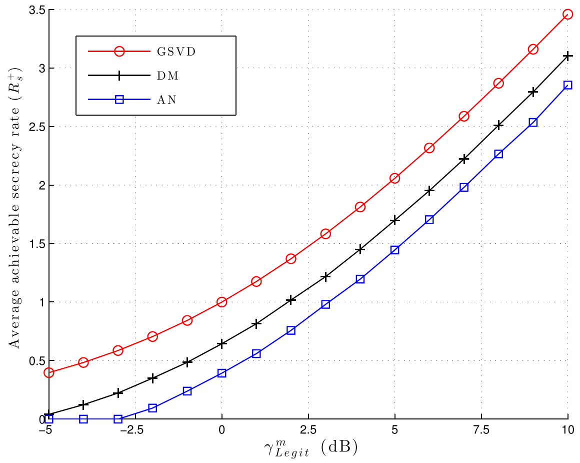

Fig. 5. The change of the average achievable secrecy rate (R_s) with the SINR of the legitimate user's channel (γ^m_{legit}).

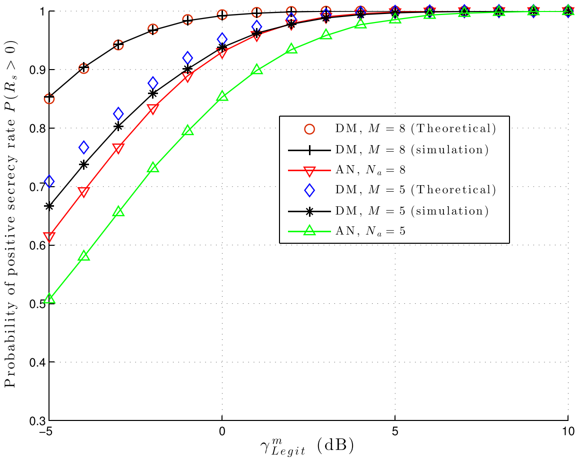

Fig. 6. The probability of achieving a positive secrecy rate $P(R_s > 0)$ against the received SINR at the legitimate user, for different system configurations.

Fig. 5 shows the change of the average achievable secrecy rate, expressed by (15), with the change of the SINR at the legitimate user, γ^m_{Legit}. Here, we compare three different schemes of secrecy namely, GSVD [12], DM, and AN. GSVD is know to achieve the secrecy capacity in case of full channel knowledge. We can see that the proposed scheme can achieve a secrecy rate closer to that of the GSVD, compared to the achievable rates when using the AN scheme.

On the other hand, Fig. 6 compares the probability of achieving positive secrecy rates in the case of using DM, with the AN scheme from [14]. The figure shows that DM outperforms the AN scheme. Also the figure shows the theoretical curves of the DM schemes based on Theorem 1. We can see that the simulations match the theoretical results. Besides, it can be inferred that after a certain number of transmit antennas N_a, the enhancement of the performance of the AN scheme is no more significant.

Note that, increasing the number of transmit antennas for AN adds hardware (the number of required RF chains) and processing complexity. While, for DM, increasing the number

[5] Here, we refer to the degradation of the channel as the decrease happening to the value of the received SINR.

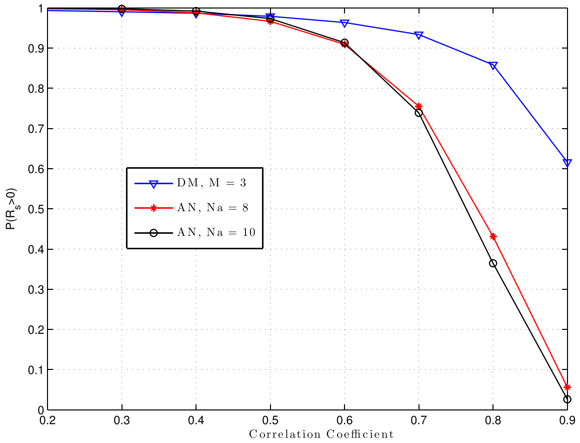

Fig. 7. The effect of the correlation between the channel of the legitimate user and the channel of the eavesdropper on achieving a positive secrecy rate $P(R_s > 0)$.

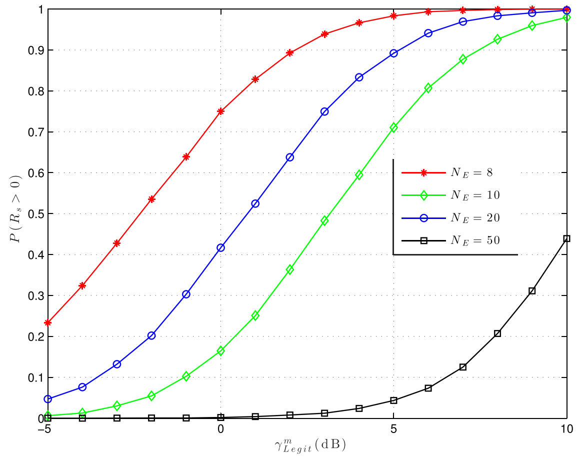

Fig. 9. The probability of achieving positive secrecy rate for different number of antennas at the eavesdropper.

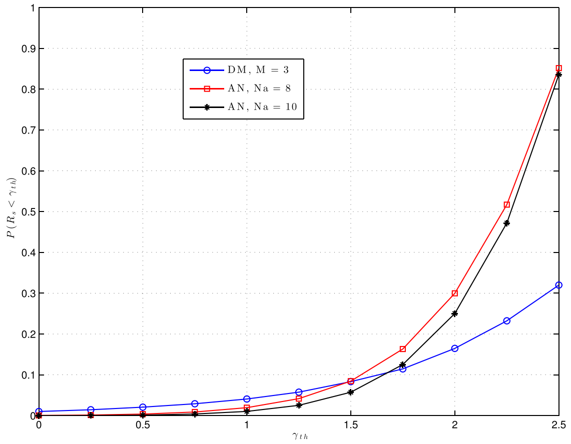

Fig. 8. The secrecy outage probability for different secrecy requirements $P(R_s < \gamma_{th})$.

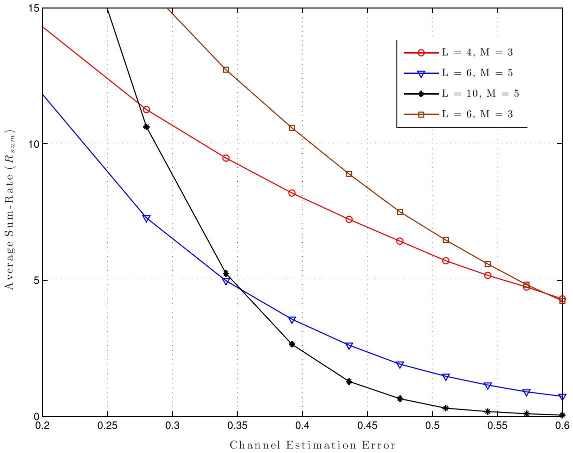

Fig. 10. The Average secrecy sum-rate against the channel estimation error.

of users M adds processing complexity only and keeps the hardware unchanged.

Fig. 7 shows the effect of the correlation between the legitimate channel and the eavesdropper's channel. As channels are being more correlated, AN loses performance faster than DM. This indicates that DM is more immune to channel correlation.

Another aspect of comparison is the ability to provide higher secrecy requirements. It is clear from Fig. 8 that DM can provide better performance when there are higher secrecy requirements. The figure shows that when the minimum secrecy rate threshold γ_{th} increases, DM tends to keep a more stable performance compared to AN.

B. Eavesdropper with an Arbitrary Number of Antennas N_E

As mentioned before, Due to the assumption of the availability of channel information of the legitimate users at the eavesdropper side, the eavesdropper can regenerate the precoding matrix and decode the legitimate data (for $N_E \geq M$) in the case of AN system. For our scheme, we add another component to the pre-coder, which is exclusively available at the base station.

It is assumed that the eavesdropper has the knowledge about the structure of the antenna array used at the base station. This means it knows the general structure of the matrix $\mathbf{H}$, but it is not aware of the values of θ_l.

Fig. 9 shows the probability of having positive secrecy rate for different number of antennas at the eavesdropper N_E. The proposed scheme can still achieve positive secrecy rate for an eavesdropper with large number of antennas, while the number of elements of the antenna array is fixed at $N = 10$.

C. Multiple Access Secrecy Rate

As discussed before, in the case of perfect knowledge of the channel of each of the users, the pre-coder is capable of eliminating the effect of each signal on the other non-intended users. Here, we are showing the effect of channel estimation error on the secrecy performance. To be more practical, we adopted the channel estimation error model of the LTE system [36]. Fig. 10 shows the secrecy sum-rate against the channel estimation error, for different channel structures and different number of users.

It is shown that the increase in the number of users in the system affects the secrecy rate. This is due to the increase

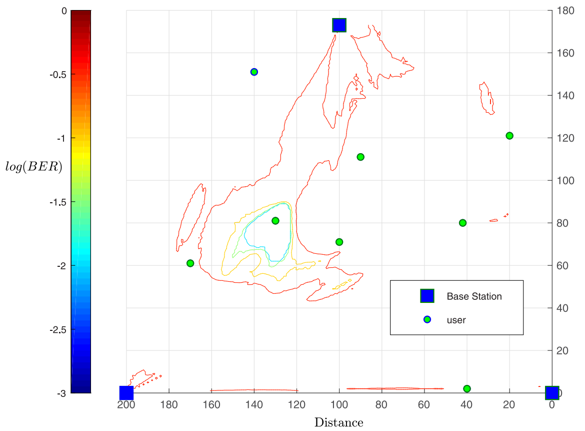

Fig. 11. BER performance contour with 4-QAM and N = 8.

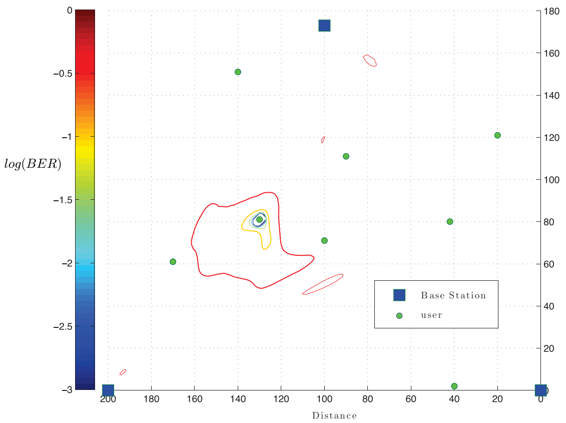

Fig. 12. BER performance contour with 16-QAM and N = 8.

in the number of interfering signals that leak to the legitimate data. On the other side, having a more diverse channel helps to maintain some resistance against estimation error. The diverse channel helps to average the interference imposed on the legitimate signal, which is a zero-mean random variable.

D. Secrecy Using CoMP

The CoMP scheme requires the signal to be transmitted from several geographically separated base stations to provide security so that, along each direction of transmission, the data is not decodable. Here, we simulate a 100 × 100 area ($K = 10^4$) covered by 3 base-stations ($B = 3$). The number of users served in that area is based on the number of used antenna elements ($M = N = 8$). The BER threshold is chosen as $\eta = 10^{-2}$.

Fig. 11 shows the simulation of equally separated base stations. The base stations are configured such that the broadside direction of each antenna array is pointing towards the center of the equilateral triangular shape of the base stations positions. Using 4-QAM modulation scheme, contours of the noiseless BER performance for one of the users is shown where circles represent the users and squares are the base stations.

Fig. 12 shows the case where 16-QAM modulation is used. Notice how the secure region is reduced with increasing the modulation order. To further control the secure area, the number of activated antenna arrays elements is changed accordingly. Increasing the number of antenna elements narrows the information beam-width, reducing the vulnerable region as shown next.

In order to profile the performance of this location-specific security technique, we use the average VR metric to measure variations of the secure area. Fig. 13 shows the effect of varying the number of antenna elements of the base stations. It is clear that, for a given modulation order, as the number of elements increases, the VR reduces significantly. Furthermore, different modulation orders are simulated. As mentioned previously, higher modulation order allows for more confined VR. Hence, using both: antenna size and modulation order, full control over VR is attained.

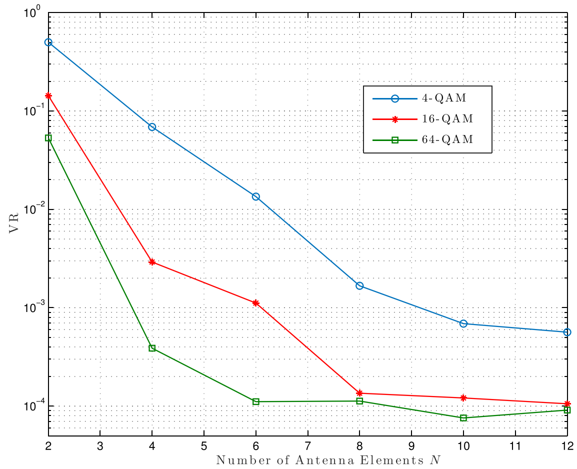

Fig. 13. Vulnerable region reduction with number of antenna elements for different modulation orders.

VI. Conclusion

We introduced 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 can degrade the performance of the eavesdropper regardless of its original channel quality. The amount of degradation increases with the increase of the number of legitimate users in the system. Moreover, the secrecy analysis shows that the proposed system is always able to achieve a positive secrecy rate with high probability under different scenarios. The analysis also shows that our proposed DM scheme outperforms the conventional AN scheme. We show that this scheme has some immunity against eavesdroppers with a high number of receiving antennas. Besides, the scheme has a stable performance for high secrecy requirements. Moreover, a different location-specific secure scheme was proposed using CoMP transmission. The new technique limits the detectability of the message to a certain geographical area called *vulnerable region*. Changing the number of active array elements can control the area of the vulnerable region. Simulations validate the performance of this scheme for different antenna sizes and modulation orders.

Appendix A
Distribution of the Achievable Rate and the Received SINR

Starting from (12), with the assumption of i.i.d. elements of $\mathbf{A}$ and the large number of antenna elements N, it is valid to assume that the elements of the resulting vector $\mathbf{v}$ are complex Gaussian random variables according to the central limit theorem ($v_j \sim CN(0, 1)$).

For the proposed system to serve K users, at least $(N > K)$ antenna elements are needed. The number of involved users K, not the number of antennas N, is the main determinant for the performance of the system. The assumption of a large number of antennas is made in order to assure that the system is able to serve a large enough number of users. With larger number of users involved, the central limit theorem assumption is justified. On the other hand, when a limited number of users is present, we can see that there is a mismatch between the simulation and theoretical results, which appears in Figure 6.

This would make the squared magnitude follow an exponential distribution ($|v_j|^2 \sim Exp(\lambda)$), with the shape parameter $\lambda = 1$.

Considering the worst case where the eavesdropper channel is noiseless ($\sigma_{n_e}^2 = 0$), we can rewrite (14) as,

$$\gamma_{\text{Eaves}}^{m} = \frac{|\mathbf{b}\tilde{\mathbf{H}}^{\dagger}\mathbf{d}_m|^2 \sigma_m^2}{|\mathbf{b}\tilde{\mathbf{H}}^{\dagger}\mathbf{D}_m|^2 \sigma_{int}^2} \tag{25}$$

letting $X = |\mathbf{b}\tilde{\mathbf{H}}^{\dagger}\mathbf{d}_m|^2$, $Y = |\mathbf{b}\tilde{\mathbf{H}}^{\dagger}\mathbf{D}_m|^2$, and $Z = X + Y$, the eavesdropper achievable rate would be,

$$\begin{aligned} R_e &= \log(1 + \gamma_{\text{Eaves}}^{m}) \\ &= \log(1 + \frac{X\sigma_m^2}{Y\sigma_{int}^2}) \\ &= \log(\frac{Z\mathcal{P}}{Y\sigma_{int}^2}) \\ &= \log(\frac{\mathcal{P}}{\sigma_{int}^2}) - \log(\frac{Y}{Z}) \end{aligned} \tag{26}$$

with Y and Z following the exponential distribution $Exp(1)$. Then, the received SINR will take the form,

$$\gamma_{\text{Eaves}}^{m} = \frac{\sigma_{int}^2 \, e^{(R_e - \mu)}}{\mathcal{P}} - 1. \tag{27}$$

The formula in (26) resembles a random variable with a Logistic distribution, $Logistic(\mu, \beta)$. where $\mu = \log(\frac{\mathcal{P}}{\sigma_{int}^2})$ is the location parameter, and $\beta = 1/M$ is the scale parameter,

$$F_{R_e}(r) = 0.5\left[1 + \tanh\left(\frac{r - \mu}{2\beta}\right)\right], \tag{28}$$

Moreover, The received SINR $\gamma_{\text{Eaves}}^{m}$ would follow the Shifted-Log-Logistic distribution with parameters $\alpha = e^{\mu} - 1$, $\sigma = Me^{-\mu}$, and $\varepsilon = \mu$. Then, the CDF of the SINR is given as,

$$F_{\gamma_{\text{Eaves}}^{m}}(\gamma) = \frac{1}{1 + \left(1 + \frac{\varepsilon(\gamma - \alpha)}{\sigma}\right)^{-\frac{1}{\varepsilon}}}. \tag{29}$$

Hence, the secrecy outage probability can be calculated as,

$$\begin{aligned} P(R_s \leq \gamma_{th}) &= P\left[(R_l - \gamma_{th}) \leq R_e\right] \\ &= 1 - F_{R_e}(R_l - \gamma_{th}). \end{aligned} \tag{30}$$

References

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

[2] X. Zhou, L. Song, and Y. Zhang, Eds., *Physical Layer Security in Wireless Communications*. Boca Raton, FL, USA: CRC Press, 2013.

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

[4] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 29, no. 4, pp. 656–715, 1949.

[5] M. F. Hanif, L.-N. Tran, M. Juntti, and S. Glisic, "On linear precoding strategies for secrecy rate maximization in multiuser multiantenna wireless networks," *IEEE Trans. Signal Process.*, vol. 62, no. 14, pp. 3536–3551, Jul. 2014.

[6] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.

[7] C.-Y. Wu, P.-C. Lan, P.-C. Yeh, C.-H. Lee, and C.-M. Cheng, "Practical physical layer security schemes for MIMO-OFDM systems using precoding matrix indices," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1687–1700, Sep. 2013.

[8] 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," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 807–812.

[9] J. Tang *et al.*, "A MIMO cross-layer precoding security communication system," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, San Francisco, CA, USA, Oct. 2014, pp. 500–501.

[10] G. Geraci, J. Yuan, and I. B. Collings, "Large system analysis of the secrecy sum-rates with regularized channel inversion precoding," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Paris, France, Apr. 2012, pp. 533–537.

[11] S. A. A. Fakoorian and A. L. Swindlehurst, "Dirty paper coding versus linear GSVD-based precoding in MIMO broadcast channel with confidential messages," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Texas City, TX, USA, Dec. 2011, pp. 1–5.

[12] S. A. Fakoorian and A. L. Swindlehurst, "Optimal power allocation for GSVD-based beamforming in the MIMO Gaussian wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Cambridge, MA, USA, Jul. 2012, pp. 2321–2325.

[13] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, Aug. 2014.

[14] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Lett.*, vol. 19, no. 2, pp. 71–74, Feb. 2013.

[15] N. Yang, M. Elkashlan, T. Q. Duong, J. Yuan, and R. Malaney, "Optimal transmission with artificial noise in MISOME wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2170–2181, Apr. 2016.

[16] J. G. Andrews *et al.*, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, Jun. 2014.

[17] W. Roh *et al.*, "Millimeter-wave beamforming as an enabling technology for 5G cellular communications: Theoretical feasibility and prototype results," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 106–113, Feb. 2014.

[18] M. P. Daly and J. T. Bernhard, "Directional modulation technique for phased arrays," *IEEE Trans. Antennas Propag.*, vol. 57, no. 9, pp. 2633–2640, Sep. 2009.

[19] M. P. Daly and J. T. Bernhard, "Directional modulation and coding in arrays," in *Proc. IEEE Int. Symp. Antennas Propag. (APSURSI)*, Spokane, WA, USA, Jul. 2011, pp. 1984–1987.

[20] M. P. Daly, E. L. Daly, and J. T. Bernhard, "Demonstration of directional modulation using a phased array," *IEEE Trans. Antennas Propag.*, vol. 58, no. 5, pp. 1545–1550, May 2010.

[21] M. P. Daly and J. T. Bernhard, "Beamsteering in pattern reconfigurable arrays using directional modulation," *IEEE Trans. Antennas Propag.*, vol. 58, no. 7, pp. 2259–2265, Jul. 2010.

[22] T. Hong, M.-Z. Song, and Y. Liu, "Dual-beam directional modulation technique for physical-layer secure communication," *IEEE Trans. Antennas Propag. Lett.*, vol. 10, pp. 1417–1420, Dec. 2011.

[23] N. Valliappan, A. Lozano, and R. W. Heath, Jr., "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3231–3245, Aug. 2013.

[24] O. N. Alrabadi and G. F. Pedersen, "Directional space-time modulation: A novel approach for secured wireless communication," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2012, pp. 3554–3558.

[25] Y. Ding and V. F. Fusco, "A vector approach for the analysis and synthesis of directional modulation transmitters," *IEEE Trans. Antennas Propag.*, vol. 62, no. 1, pp. 361–370, Jan. 2014.

[26] Y. Ding and V. F. Fusco, "Establishing metrics for assessing the performance of directional modulation systems," *IEEE Trans. Antennas Propag.*, vol. 62, no. 5, pp. 2745–2755, May 2014.

[27] Y. Ding and V. F. Fusco, "MIMO-inspired synthesis of directional modulation systems," *IEEE Antennas Wireless Propag. Lett.*, vol. 15, pp. 580–584, Mar. 2016.

[28] M. Hafez and H. Arslan, "On directional modulation: An analysis of transmission scheme with multiple directions," in *Proc. IEEE Int. Conf. Commun. (ICC)*, London, U.K., Jun. 2015, pp. 459–463.

[29] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[30] T. Hayashi, M. Nakano, and A. Yamaguchi, "Novel AoA estimation method using delay profile in downlink," in *Proc. Int. Workshop Antenna Technol. (iWAT)*, Karlsruhe, Germany, Mar. 2013, pp. 35–38.

[31] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[32] M. Ben-Zid, Ed., *Recent Trends in Multi-user MIMO Communications*. Rijeka, Croatia: InTech, 2013.

[33] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[34] R. Irmer *et al.*, "Coordinated multipoint: Concepts, performance, and field trial results," *IEEE Commun. Mag.*, vol. 49, no. 2, pp. 102–111, Feb. 2011.

[35] M. Sawahashi, Y. Kishiyama, A. Morimoto, D. Nishikawa, and M. Tanno, "Coordinated multipoint transmission/reception techniques for LTE-advanced [coordinated and distributed MIMO]," *IEEE Wireless Commun.*, vol. 17, no. 3, pp. 26–34, Jun. 2010.

[36] A. Serra, J. Olmos, and M. Lema, "Modelling channel estimation error in LTE link level simulations," EURO-COST, Barcelona, Spain, Tech. Rep. IC1004 TD(12)03067, Feb. 2012, pp. 8–10.

[37] M. Hafez, T. Khattab, T. Elfouly, and H. Arslan, "Secure multiple-users transmission using multi-path directional modulation," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kuala Lumpur, Malaysia, May 2016, pp. 1–5.

Mohammed Hafez (S'07) received the B.Sc. and M.Sc. degrees in electrical engineering from Alexandria University, Alexandria, Egypt, in 2010 and 2014, respectively. He was a Research Assistant with the Department of Electrical Engineering, Qatar University, Doha, Qatar, from 2011 to 2014. He was also a Research Assistant with the Department of Electrical Engineering, Alexandria University, from 2010 to 2011. He is currently a Ph.D. candidate with the Wireless Communications and Signal Processing Group (WCSP), at the University of South Florida, Tampa, FL, USA. His current research interests include physical layer security and physical layer design/signal processing for 5G networks.

Marwan Yusuf received the B.Sc. degree from Ain Shams University, Egypt, in 2010, and the M.Sc. degree in electrical, electronic and communications engineering from Istanbul Medipol University, Turkey, in 2016. His research interests include wireless communications and signal processing for 5G, physical layer security, and Internet-of-Things.

Tamer Khattab (M'94) received the B.Sc. and M.Sc. degrees in electronics and communications engineering from Cairo University, Giza, Egypt, and the Ph.D. degree in electrical and computer engineering from The University of British Columbia, Vancouver, BC, Canada, in 2007. From 1994 to 1999, he was with IBM, Egypt, as a Software Development Team Lead, where he was involved in the development of several client–server corporate tools for IBM Laboratories. From 2000 to 2003, he joined Alcatel Canada's Network and Service Management R&D, Vancouver, BC, Canada, as a member of the technical staff, where he was involved in the development of core components for Alcatel 5620 Network and Service Manager. From 2006 to 2007, he was a Post-Doctoral Fellow with The University of British Columbia, where he was involved in prototyping advanced Gigabit/sec wireless LAN baseband transceivers. He joined Qatar University (QU) in 2007, where he is currently an Associate Professor of Electrical Engineering. He is also a senior member of the technical staff with the Qatar Mobility Innovation Center, a Research and Development Center owned by QU and funded by Qatar Science and Technology Park. His research interests cover physical layer transmission techniques in optical and wireless networks, information theoretic aspects of communication systems, and MAC layer protocol design and analysis.

Tarek Elfouly (M'06–SM'13) received the DEA and Ph.D. degrees from the University of Franche Comte, France, in 1996 and 2000, respectively. He was an Assistant Professor with Ain Shams University, Cairo, Egypt, before joining Qatar University. He is currently an Associate Professor with the College of Engineering, Qatar University. He has over 12 years of experience in computer network research. He has authored or co-authored over 80 papers, more than half of them are related to wireless sensing and network security. He supervised many post graduate students and served as an examiner for many others. He has many projects under development related to computer networks and security. His projects have won many national and regional awards. His research interests include network security and protocols, physical layer security, and wireless sensor networks especially in the field of structural health monitoring and health applications.

Hüseyin Arslan (S'95–M'98–SM'04–F'16) received the B.S. degree from Middle East Technical University, Ankara, Turkey, in 1992, and the M.S. and Ph.D. degrees from Southern Methodist University, Dallas, TX, USA, in 1994 and 1998, respectively. From 1998 to 2002, he was with the Research Group of Ericsson Inc., NC, USA, where he was involved with several projects related to 2G and 3G wireless communication systems. Since 2002, he has been with the Electrical Engineering Department, University of South Florida, Tampa, FL, USA, where he is currently a Professor. In 2013, he joined Istanbul Medipol University to found the Engineering College, where he was the Dean of the School of Engineering and Natural Sciences. He has also served as the Director of the Graduate School of Engineering and Natural Sciences with Istanbul Medipol University. In addition, he was a part-time Consultant for various companies and institutions, including Anritsu Company, Savronik Inc., and The Scientific and Technological Research Council of Turkey.

His research interests are related to advanced signal processing techniques at the physical and medium access layers, with cross-layer design for networking adaptivity and quality of service control. He is interested in many forms of wireless technologies, including cellular radio, wireless PAN/LAN/MANs, fixed wireless access, aeronautical networks, underwater networks, *in vivo* networks, and wireless sensors networks. His current research interests are on 5G and beyond, physical layer security, interference management (avoidance, awareness, and cancellation), cognitive radio, small cells, powerline communications, smart grid, UWB, multi-carrier wireless technologies, dynamic spectrum access, co-existence issues on heterogeneous networks, aeronautical (high altitude platform) communications, *in vivo* channel modeling and system design, and underwater acoustic communications. He has served as the technical program committee chair, technical program committee member, session and symposium organizer, and workshop chair in several IEEE conferences. He is currently a member of the Editorial Board for the IEEE SURVEYS AND TUTORIALS and the *Sensors Journal*. He has also served as a member of the Editorial Board for the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING, the *Elsevier Physical Communication Journal*, the *Hindawi Journal of Electrical and Computer Engineering*, and *Wiley Wireless Communication and Mobile Computing Journal*.