Hindawi
Wireless Communications and Mobile Computing
Volume 2017, Article ID 5396092, 10 pages
https://doi.org/10.1155/2017/5396092

Research Article

Joint Design of Massive MIMO Precoder and Security Scheme for Multiuser Scenarios under Reciprocal Channel Conditions

Gustavo Anjos,[1] Daniel Castanheira,[1] Adão Silva,[1] Atílio Gameiro,[1] Marco Gomes,[2] and João Vilela[3]

[1] *Instituto de Telecomunicações and DETI, University of Aveiro, Aveiro, Portugal*
[2] *Instituto de Telecomunicações, Department of Electrical and Computer Engineering, University of Coimbra, Coimbra, Portugal*
[3] *CISUC, Department of Informatics Engineering, University of Coimbra, Coimbra, Portugal*

Correspondence should be addressed to Gustavo Anjos; gustavoanjos@ua.pt

Received 25 August 2017; Revised 30 October 2017; Accepted 13 November 2017; Published 10 December 2017

Academic Editor: Daniele Pinchera

The exploration of the physical layer characteristics of the wireless channel is currently the object of intensive research in order to develop advanced secrecy schemes that can protect information against eavesdropping attacks. Following this line of work, in this manuscript we consider a massive MIMO system and jointly design the channel precoder and security scheme. By doing that we ensure that the precoding operation does not reduce the degree of secrecy provided by the security scheme. The fundamental working principle of the proposed technique is to apply selective random rotations in the transmitted signal at the antenna level in order to achieve a compromise between legitimate and eavesdropper channel capacities. These rotations use the phase of the reciprocal wireless channel as a common random source between the transmitter and the intended receiver. To assess the security performance, the proposed joint scheme is compared with a recently proposed approach for massive MIMO systems. The results show that, with the proposed joint design, the number of antenna elements does not influence the eavesdropper channel capacity, which is proved to be equal to zero, in contrast to previous approaches.

1. Introduction

The growing demand for capacity that wireless networks have experienced in recent years has resulted from the emergence of a new set of services, cheap devices, and useful applications that started to play a crucial role in the professional and social domains of people's lives. The dependence of such services and applications increased in such a way that now they must be available anywhere, at any time, and in any circumstance. In addition to the flexible availability demand, some of these services require the exchange of private sensitive information, such as personal financial data, government-level classified information, or critical business reports. Due to the broadcast nature of the wireless channel, the protection of this kind of information in mobile networks is seen as a main system design parameter that must be carefully addressed. Since the release of the initial mobile standards, higher layer cryptographic protocols have been used as the main security platform to protect wireless communications from unintended receivers [1]. Although these protocols have found widespread acceptance, they rely on the assumption that an eavesdropper has computational resource limitations [2]. For instance, in asymmetric public key cryptosystems, the security level is supported by the assumption that the integer factorization of the product of two large prime numbers is a very intensive computational task taking into account current factorization techniques. However, in recent years, the advances in the field of number theory and the continuous increase in transistor integration levels are putting pressure on these types of protocols, forcing the use of larger key sizes, which in turn leads to a higher implementation complexity for cryptographic systems [3].

To complement the limitations of standalone cryptographic protocols [4, 5], the development of secrecy schemes that explore the physical layer characteristics of the wireless channel has been considered to efficiently improve information security in wireless networks. Physical layer security does not make any assumption regarding the level of computational capacity at the unintended receiver, being the secrecy provided by building on a channel advantage in relation to the eavesdropper [6]. The advancement of physical layer secrecy can be performed at two main levels: the coding domain and the signal level domain. In the coding domain, the target is to use error-correction codes that are designed to not only provide error detection but also implement some level of secrecy in a wiretap channel [7–10]. For signaling, techniques involving specific precoding designs, power allocation schemes, and cooperative jamming based on interference alignment (IA) [11, 12] and artificial noise injection have been defined in the literature [13–19].

The use of massive MIMO technology is being considered by the research community as mandatory evolution of the conventional MIMO systems to address the capacity requirements of future 5G mobile networks [20–23]. Over the last years, intensive research efforts have been made to solve some practical constraints associated with the large-scale deployment of massive MIMO. However, aspects related to information security have been left aside for some time, and only recently have they begun to be discussed. In [24], pilot contamination attacks in a Time Division Duplex (TDD) multicell multiuser massive MIMO scenario were analyzed. With the use of the same uplink training sequence of a legitimate receiver (Bob), the eavesdropper (Eve) can force the contamination of the channel estimated at the base station, which, in a subsequent downlink beamforming phase, will allow the unintended receiver to improve their ability to tap the communication. To address this problem, the authors derived a closed form solution for optimal power allocation between the information signal and noise, considering a maximum ratio transmission (MRT) precoder plus artificial noise (AN) generation at the legitimate transmitter. A null-space (NS) based precoder that was designed to mitigate the effect of a pilot contamination attack was also suggested. Considering again the same multicell multiuser scenario of [24], the work in [25] compared the use of NS-based precoding and random shaping matrix precoding for AN generation in an MRT-based massive MIMO transmitter under the presence of a multiantenna eavesdropper. Considering the large computational complexity required to calculate the NS of large channel matrices, the authors in [25] verified that the use of random shaping matrices for AN precoding could offer a good solution in terms of performance/complexity tradeoff. The work in [26] shows that by combining the information signal with artificial generated noise, a positive secrecy capacity can be obtained, assuming that the number of antennas at the eavesdropper is smaller than the total number of antennas at the legitimate transmitter. In the first scenario, a multiple-antenna transmitter forces the generated AN to lie in the null space of the legitimate receiver channel. In a second scenario, a single-antenna node cooperates with single-antenna relays to simulate the effect of a multiple-antenna transmitter generating AN. An attempt to force an independent relation between the secrecy capacity and the number of antennas at the eavesdropper was proposed in [27] with the development of the original symbol phase rotated (OSPR) technique. The idea of the OSPR scheme is to use the phase of the reciprocal wireless channel to define random rotations on the original data symbols that are exchanged in the downlink direction between a massive MIMO base station (BS) and several single-antenna user terminals (UTs). Considering that the reciprocal channels are available at both sides of the legitimate link, the intended receiver has all the information required to revert the original random phase rotations applied at the legitimate transmitter, while at the eavesdropper side, assuming no collocation with the legitimate UTs, the random phase rotations cannot be reverted. In [27], the authors claim that, even in the presence of a powerful massive MIMO eavesdropper equipped with an infinite number of antenna elements, the OSPR technique achieves a positive secrecy rate. Using the same basic idea considered in [27], the authors in [28] applied the OSPR scheme in the uplink direction. Another approach that exploits the channel reciprocity to provide secrecy in wireless single-antenna systems was proposed in [29]. The authors in [29] suggested a secrecy scheme that uses the reciprocal channel phase to randomly define discrete jamming signals. In the first part of the work, in order to evaluate the baseline secrecy level of the scheme, the authors consider random combinations of data and jamming signals. In the second part, an efficient data and jamming signal combining algorithm was developed, which allowed verifying a significant improvement over the secrecy level of the baseline scheme.

In this paper, we propose to jointly design the security scheme and massive MIMO precoder. The target is to provide information secrecy in a multiuser massive MIMO scenario in the presence of a passive eavesdropper equipped with a large number of antenna elements. The joint design ensures that the precoding operation does not reduce the degree of secrecy provided by the security scheme and achieves a compromise between legitimate and eavesdropper channel capacities. The fundamental working principle of the joint scheme is to create equivocation at the unintended receiver by applying antenna selective random phase rotations in both the original data symbols and the precoder. To evaluate the merit of the proposed scheme, a comparison with a technique proposed in the literature [27] was performed by using the secrecy capacity as the metric in different multiuser massive MIMO configurations. The comparison showed that for the new proposed scheme the eavesdropper channel capacity is always zero, contrary to what occurs in the scheme proposed in [27], where some leakage of information was always verified. In summary, the main contributions of the presented work are outlined in the following two points:

(a) Mathematical analysis of the existing OSPR scheme using the secrecy capacity as evaluation metric: This analysis identifies some of the limitations of the OSPR scheme, which include the nonintentional phase reversions in the OSPR symbols caused by the MRT precoder that leads to zero secrecy capacity for the OSPR scheme. Moreover, the mathematical analysis is confirmed by simulation.

(b) Proposal of a joint design for the massive MIMO precoder and security scheme which removes the drawback of the OSPR scheme: We show analytically and by simulation that the proposed joint design forces the capacity of the eavesdropper channel always to zero, independently of the number of antennas at the eavesdropper. Furthermore, the zero channel capacity at the eavesdropper is obtained with minimal impact in the legitimate user's channel.

The remainder of the paper is organized as follows: Section 2 defines the general system characterization and the secrecy metrics used in the numerical evaluations. Section 3 starts by a description of the OSPR scheme proposed in [27] followed by the mathematical analysis of this secrecy scheme that enables the identification of secrecy breaches, justifying therefore the need for new approaches. The security scheme proposed in this manuscript is formulated in Section 4. In Section 5, the numerical evaluation results are presented. Finally, the main conclusions are outlined in Section 6.

Notations. Boldface capital letters denote matrices and boldface lowercase letters denote column vectors. The operations $(\cdot)^T$, $(\cdot)^H$, $(\cdot)^*$, and $\mathrm{tr}(\cdot)$ represent the transpose, the Hermitian transpose, the conjugate, and the trace of a matrix, respectively. Consider a vector $\mathbf{a}$; $\mathrm{diag}(\mathbf{a})$ corresponds to a diagonal matrix with diagonal entries equal to vector $\mathbf{a}$. The norm of vector $\mathbf{a}$ is defined as $\|\mathbf{a}\|$.

2. System Model and Metrics

In this section, the system setup, as well as the evaluation metrics used to assess the schemes performance, is presented.

2.1. System Model. Figure 1 depicts the general setup used in the schemes described in Sections 3 and 4. The system is a multiuser massive MIMO cell with K single-antenna user terminals (UT), one base station (BS), and one passive eavesdropper (Eve) employing N_t and N_e antennas, respectively. The assumption of a passive eavesdropper means that this node listens to the communication and does not cause any intentional interference in the communication channel, making his presence and location uncertain to the legitimate transmitter. In this work, Eve wants to tap the information that is exchanged between the BS and the UTs. We consider TDD channel reciprocity and perfect channel estimations at the BS, which are acquired through an uplink training process. Additionally, we assume that Eve is not collocated with any of the UTs nodes, that is, independence between all the channel responses is verified. In Figure 1, s_k, $k \in \{1,\dots,K\}$ represents the data symbol of user k. All the channel responses are modeled by zero mean and unity variance complex Gaussian fading coefficients with $\mathbf{H} \in \mathbb{C}^{K\times N_t}$ as the channel matrix between the BS and all of the K UTs, where $h_{k,i}$, $1 \le k \le K$, $1 \le i \le N_t$, denotes the entry at row k and column i of matrix $\mathbf{H}$. In this work, ideal RF up- and downconversion are assumed with all the baseband processing applied to an independent flat fading channel realization.

The vectors $\mathbf{h}_k^a \in \mathbb{C}^{1\times N_t}$, $k = 1,2,\dots,K$, and $\mathbf{h}_i^b \in \mathbb{C}^{K\times 1}$, $i = 1,2,\dots,N_t$, are defined as the channel vector between BS and UT k and between the BS antenna element i and the K UTs, respectively.

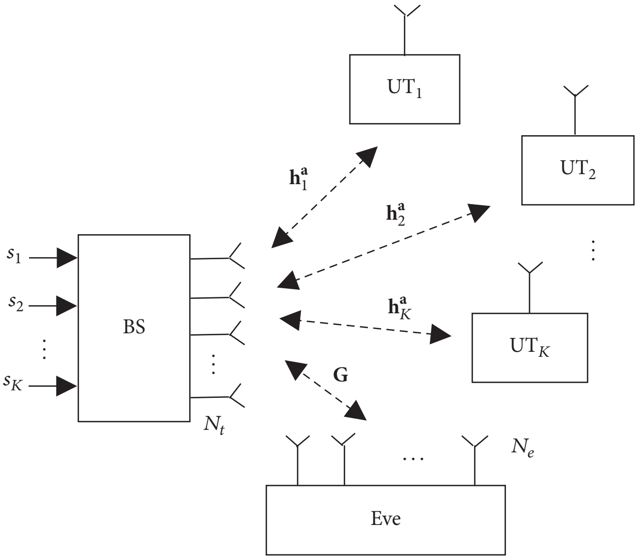

UT$_1$
UT$_2$
UT$_K$
$\mathbf{h}_1^\mathbf{a}$
$\mathbf{h}_2^\mathbf{a}$
$\mathbf{h}_K^\mathbf{a}$
s_1
s_2
s_K
BS
G
N_t
N_e
Eve

Figure 1: General system setup.

$$\mathbf{h}_k^a = \begin{bmatrix} h_{k,1} & h_{k,2} & \cdots & h_{k,N_t} \end{bmatrix},$$
$$\mathbf{h}_i^b = \begin{bmatrix} h_{1,i} & h_{2,i} & \cdots & h_{K,i} \end{bmatrix}^T. \tag{1}$$

The matrix $\mathbf{G} = \begin{bmatrix} \mathbf{g}_1 & \mathbf{g}_2 & \cdots & \mathbf{g}_{N_t} \end{bmatrix} \in \mathbb{C}^{N_e\times N_t}$ represents the channel responses between the BS and the eavesdropper, being the respective elements also modeled by complex Gaussian random variables with zero mean and unitary variance. The column vector $\mathbf{g}_i \in \mathbb{C}^{N_e\times 1}$, $i = 1,2,\dots,N_t$ defines the channel between BS antenna element i and the eavesdropper, where $g_{p,i}$ denotes its pth element.

The signal transmitted by the BS is given by

$$\mathbf{x} = \sum_{k=1}^{K} \mathbf{w}_k s_R^k, \tag{2}$$

where $\mathbf{w}_k \in \mathbb{C}^{N_t\times 1}$ is the precoding vector for UT k and s_R^k is a function of the data symbol s_k and channel matrix $\mathbf{H}$. The transmission power is constrained to $E[\|\mathbf{x}\|^2] < 1$. More details on how to compute the precoding vector $\mathbf{w}_k$ and the rotated data symbol s_R^k are provided in Sections 3 and 4.

The signal received at UT k is given by

$$y_k = \mathbf{h}_k^a \mathbf{x} + \tilde{n}_k, \tag{3}$$

whereas the one received at Eve is defined as $\mathbf{y}_e \in \mathbb{C}^{N_e\times 1}$,

$$\mathbf{y}_e = \mathbf{G}\mathbf{x} + \tilde{\mathbf{n}}_e, \tag{4}$$

where $\tilde{n}_k$ and $\tilde{\mathbf{n}}_e \in \mathbb{C}^{N_e\times 1}$ are the zero mean white Gaussian noise with variance, σ_k^2 and σ_E^2, at UT k and Eve, respectively.

In the following, we assume that the BS has knowledge of the channel matrix $\mathbf{H}$ and index $i \in \{1,\dots,N_t\}$, the UT k only needs to know the channel $h_{k,i} = |h_{k,i}|e^{j\theta_{k,i}}$, for example, the channel between himself and the selected BS antenna from which it extracts the respective channel phase $\theta_{k,i}$, and Eve knows channel $\mathbf{g}_i$. To acquire channel $\mathbf{H}$ at the BS, each UT sends an orthogonal pilot sequence to the BS in the uplink training phase. The index i is selected at the BS uniformly at random from the set $\{1, \ldots, N_t\}$. Then, to acquire the reciprocal channel $h_{k,i}$ at UT $k = 1, \ldots, K$, the BS broadcasts a reference signal using only antenna i. The transmission of the broadcast reference signal at antenna element i of the BS will allow the eavesdropper to obtain $\mathbf{g}_i$. We assume that the channel estimations are perfect, and in the case of the eavesdropper, considering no collocation with any of the UTs or BS, the random phase rotations $\theta_{k,i}$ are not available.

2.2. Secrecy Metrics and Theorems. The secrecy evaluation of the schemes considered in this work was performed using the Fano inequality theorem in order to compute a bound on the secrecy capacity. In this subsection, the concept of secrecy capacity and the definition of the Fano theorem are briefly revised to ensure that the manuscript is self-contained.

2.2.1. Secrecy Capacity. The secrecy metric used in the evaluation of the schemes presented in Sections 3 and 4 is the secrecy capacity, C_s, which is formulated as

$$C_s = I(X, Y) - I(X, Z), \tag{5}$$

where $I(X, Y)$ defines the mutual information between random variables X and Y, with X being the random variable that defines the data source, Y the random variable observed at the legitimate receiver, and Z the one observed by the eavesdropper; the target of each secrecy scheme is to maximize $I(X, Y)$ and minimize $I(X, Z)$. The mutual information can be formulated as a function of the entropy. For instance, $I(X, Y)$ and $I(X, Z)$ have the following representations:

$$\begin{aligned} I(X, Y) &= h(X) - h(X \mid Y) \\ I(X, Z) &= h(X) - h(X \mid Z), \end{aligned} \tag{6}$$

where $h(X)$ is the differential entropy of the source with $h(X \mid Y)$ and $h(X \mid Z)$ being the equivocations at the legitimate receiver and at the eavesdropper, respectively. Note that when the eavesdropper is not able to acquire any information on X through the observation of Z, $h(X \mid Z) = h(X)$ and $I(X, Z) = 0$, which is what we expect, that is, an eavesdropper with zero channel capacity.

2.2.2. Fano Inequality. In this work, the *Fano inequality theorem* [30] is used to compute a bound on the secrecy capacity of the schemes presented in Sections 3 and 4. The *Fano* inequality allows us to relate the probability of error P_e with the equivocation rate; therefore, by using the error probability, an upper bound on $h(X \mid Y)$ and $h(X \mid Z)$ can be obtained.

Theorem 1 (Fano's inequality, [30]). *For any estimator $\widehat{X}$ considering the Markov chain, $X \rightarrow Y \rightarrow \widehat{X}$ with $P_e = P\{\widehat{X} \neq X\}$, an upper bound on the equivocation is defined as*

$$h(X \mid Y) \leq h\left(X \mid \widehat{X}\right) \leq h(P_e) + P_e \log_2(|X| - 1) \tag{7}$$

with $h(P_e)$ being the binary entropy given by

$$h(P_e) = -P_e \log_2 P_e - (1 - P_e) \log_2 (1 - P_e). \tag{8}$$

Using *Fano's* theorem, lower bounds on the capacities of the legitimate receiver and eavesdropper channels are obtained.

3. Secrecy Capacity Analysis of the OSPR Scheme

As mentioned before, this work provides a comparative analysis between the proposed scheme and the OSPR technique suggested in [27]. The purpose of this section is to briefly describe the OSPR scheme in which the fundamental working principle is to use the TDD reciprocal channel phase as a common source between the BS and UTs to define random phase rotations in the original data symbols. Furthermore, we show that the eavesdropper channel capacity is always positive, and for the special case of an infinite number of antennas at the eavesdropper and a single user terminal, the capacity is one; that is, the secrecy capacity is zero.

3.1. Precoding. Before the computation of the massive MIMO precoder, the OSPR security scheme uses the reciprocal channel random phases $\theta_{k,i}$, $k = 1, \ldots, K$, to rotate the original data symbols s_k, $k = 1, \ldots, K$. The result of this rotation is

$$s_R^k = s_k e^{j\theta_{k,i}}. \tag{9}$$

After the rotation of the original data symbols, the transmitted signal $\mathbf{x} \in \mathbb{C}^{N_t \times 1}$, as described in (2), is computed by applying the MRT precoder,

$$\mathbf{w}_k = \frac{1}{\sqrt{K}} \frac{\left(\mathbf{h}_k^a\right)^H}{\left\|\mathbf{h}_k^a\right\|}, \tag{10}$$

directly to the rotated data, s_R^k. The design of the MRT precoder is performed separately from the OSPR scheme without taking into account their combined behavior. As described in the following, some nonintentional phase reversions in the OSPR symbols are caused by the MRT precoder. This nonjoint design will lead to information leakage to the eavesdropper.

3.2. Decoding. To evaluate the security performance of the scheme suggested in [27], in this work, we consider that Eve applies a maximum ratio combining (MRC) equalizer to the received signal $\mathbf{y}_e$ in order to estimate s_k. Using $\mathbf{u}_i$ as the equalizer vector

$$\mathbf{u}_i = \frac{1}{\sqrt{N_e}} \frac{\mathbf{g}_i^H}{\left\|\mathbf{g}_i\right\|}, \tag{11}$$

the eavesdropper obtains

$$\widehat{y}_e = \mathbf{u}_i \mathbf{y}_e. \tag{12}$$

After applying $\mathbf{u}_i$ to the received signal $\mathbf{y}_e$, the obtained estimative, $\hat{y}_e$, is directly demodulated. Regarding the decoding process at the user terminals, the received signal y_k is directly demodulated after reverting the random phase rotations applied at the original symbols.

As demonstrated in the next point, the use of $\mathbf{u}_i$ will allow an eavesdropper with unlimited number of antennas to drive the secrecy capacity to zero, especially when only one UT is accessing the network.

3.3. Analysis. In this subsection, we analyze the secrecy capacity of the OSPR scheme. Using A_k as a power normalization factor,

$$A_k = \frac{1}{\sqrt{K}\left\|\mathbf{h}_k^a\right\|}, \tag{13}$$

from (2), (4), (10), (11), and (12), it follows that

$$\begin{aligned} \hat{y}_e = {} & \sum_{k=1}^{K} \sum_{m=1,m\neq i}^{N_t} \frac{A_k}{\sqrt{N_e}} \frac{\mathbf{g}_i^H \mathbf{g}_m}{\left\|\mathbf{g}_i\right\|} h_{k,m}^* e^{j\theta_{k,i}} s_k \\ & + \sum_{k=1}^{K} \frac{A_k}{\sqrt{N_e}} \frac{\mathbf{g}_i^H \mathbf{g}_i}{\left\|\mathbf{g}_i\right\|} \left|h_{k,i}\right| s_k + \frac{1}{\sqrt{N_e}} \frac{\mathbf{g}_i^H}{\left\|\mathbf{g}_i\right\|} \tilde{\mathbf{n}}_e. \end{aligned} \tag{14}$$

If we consider the limiting case of an eavesdropper with an infinite number of antenna elements, then

$$\begin{aligned} \lim_{N_e\to\infty} \frac{1}{\sqrt{N_e}} \frac{\mathbf{g}_i^H \mathbf{g}_m}{\left\|\mathbf{g}_i\right\|} &= \lim_{N_e\to\infty} \frac{1}{N_e} \sum_{p=1}^{N_e} g_{p,i}^* g_{p,m} \\ &= \mathbb{E}\left[g_{1,i}^* g_{1,m}\right] = 0, \end{aligned} \tag{15}$$

where the last equality follows from the independence of random variables $g_{1,i}$ and $g_{1,m}$. Similarly, it follows that

$$\begin{aligned} \lim_{N_e\to\infty} \frac{1}{\sqrt{N_e}} \frac{\mathbf{g}_i^H \mathbf{g}_i}{\left\|\mathbf{g}_i\right\|} &= \mathbb{E}\left[g_{1,i}^* g_{1,i}\right] = 1 \\ \lim_{N_e\to\infty} \frac{1}{\sqrt{N_e}} \frac{\mathbf{g}_i^H}{\left\|\mathbf{g}_i\right\|} \tilde{\mathbf{n}}_e &= \mathbb{E}\left[g_{1,i}^* n_1\right] = 0, \end{aligned} \tag{16}$$

where $\mathbb{E}[g_{1,i}^* g_{1,i}] = 1$ and $\mathbb{E}[g_{1,i}^* n_1] = 0$ following from the independence of the random variables $g_{1,i}$ and n_1. Equations (14), (15), and (16) lead to the simplification defined by

$$\begin{aligned} y_e' = \lim_{N_e\to\infty} \hat{y}_e &= \sum_{k=1}^{K} \frac{A_k}{\sqrt{N_e}} \frac{\mathbf{g}_i^H \mathbf{g}_i}{\left\|\mathbf{g}_i\right\|} \left|h_{k,i}\right| s_k \\ &= \sum_{k=1}^{K} A_k \left|h_{k,i}\right| s_k. \end{aligned} \tag{17}$$

Defining c_k as the positive constant

$$c_k = A_k \left|h_{k,i}\right| \geq 0 \tag{18}$$

the signal y_e' simplifies to

$$y_e' = \lim_{N_e\to\infty} \hat{y}_e = \sum_{k=1}^{K} c_k s_k. \tag{19}$$

Analyzing y_e', it is possible to realize that, for one user terminal and considering a PSK constellation for s_k, it follows that $y_e' = c_1 s_1$. Then, the eavesdropper can obtain all of the information, that is, s_1. As may be verified from (19) and the definition of A_k and c_k (see (13) and (18)), the secrecy level of the OSPR scheme proposed in [27] is reached not by the OSPR random phase rotation applied at the original data symbols but because the eavesdropper has no knowledge of $|h_{k,i}|$ and because the increasing interference that results when the number of user terminals accessing the network begins to grow.

4. Proposed Joint Scheme

To address the security faults of the OSPR scheme suggested in [27], in this work, we propose to jointly design the massive MIMO precoder and the security scheme. As demonstrated in this section, for the proposed joint precoder and security scheme, the resulting eavesdropper channel capacity is zero even for the limiting case of an eavesdropper with an infinite number of antennas. Regarding the capacity of the legitimate channel, as confirmed in Section 5.2, the degradation imposed by the joint design tends to zero for a number of antenna elements at the BS much larger than the number of user terminals, that is, for a massive MIMO scenario.

4.1. Precoding. In the proposed joint scheme, the design of the MRT precoder was accomplished by considering the random rotations applied to the original data symbols by the security scheme. The computation of the precoding vector, $\mathbf{w}_k$, for UT k is done as follows:

$$\mathbf{w}_k = \frac{1}{\left\|\mathbf{h}_k^a\right\|} \left[\, \left|h_{k,1}\right| e^{-j\theta_{k,1}} \quad \left|h_{k,2}\right| e^{-j\theta_{k,2}} \quad \cdots \quad \left|h_{k,i}\right| \quad \cdots \quad \left|h_{k,N_t}\right| e^{-j\theta_{k,N_t}} \,\right]^T. \tag{20}$$

In the vector $\mathbf{w}_k$ above, the phase of the precoding coefficient for antenna element i, the antenna selected randomly to extract the phases rotations, is changed from $-\theta_{k,i}$ to 0. The transmission signal, $\mathbf{x} \in \mathbb{C}^{N_t\times 1}$, is again defined as

$$\mathbf{x} = \sum_{k=1}^{K} \mathbf{w}_k s_R^k. \tag{21}$$

Through this modification of the MRT precoder, reversions of phase rotations created by the combination of the MRT and OSPR are avoided.

4.2. Decoding. In the case of the user terminals, the decoding at the legitimate receiver k is performed as follows. Consider that antenna element i is selected at the BS to extract the random phase rotations. Let I_k be defined as the interference term from the other user terminals; then, signal y_k received at UT k is given by

$$\begin{aligned} y_k &= A_k \left[\left|h_{k,i}\right|^2 e^{j\theta_{k,i}} + \sum_{n=1,n\neq i}^{N_t} \left|h_{k,n}\right|^2 \right] s_k e^{-j\theta_{k,i}} + I_k \\ &\quad + \tilde{n}_k, \end{aligned} \tag{22}$$

$$I_k = \sum_{m=1,m\neq k}^{K} A_m \left[h_{k,i} \left|h_{m,i}\right| + \sum_{n=1,n\neq i}^{N_t} h_{k,n} h_{m,n}^* \right] s_m e^{-j\theta_{m,i}}. \tag{23}$$

At the user terminal, k, the equalization is done computing u_k as defined below

$$\begin{aligned} u_k &= N_t^{-1} e^{j\theta_{k,i}} \\ \hat{y}_k &= u_k y_k. \end{aligned} \tag{24}$$

After applying u_k to y_k, the estimated value of $\hat{y}_k$ is directly hard or soft demodulated to obtain the original data. On the eavesdropper side, as shown in the next section, the channel capacity is always zero for any applied decoder.

Further, as shown in the remainder of this subsection, when the number of antenna elements at the BS grows to infinity, a legitimate user can acquire all of the information; that is, the legitimate channel capacity is maximum.

Starting by considering an infinite number of antenna elements at the BS, that is, $N_t \rightarrow \infty$, the following simplifications can be performed in the received equalized signal $\hat{y}_k$:

$$\lim_{N_t\to\infty} \frac{1}{N_t} \sum_{n=1,n\neq i}^{N_t} h_{k,n} h_{k,n}^* = \mathbb{E}\left[h_{k,1} h_{k,1}^*\right] = 1, \tag{25}$$

$$\lim_{N_t\to\infty} \frac{1}{N_t} \sum_{n=1,n\neq i}^{N_t} h_{k,n} h_{m,n}^* = \mathbb{E}\left[h_{k,1} h_{m,1}^*\right] = 0. \tag{26}$$

Applying (25) to (22) and (26) to (23), the estimated signal, $\hat{y}_k$, can be simplified in (27) as

$$\begin{aligned} \lim_{N_t\to\infty} \hat{y}_k &= \lim_{N_t\to\infty} A_k \left[\frac{\left|h_{k,i}\right|^2 e^{j\theta_{k,i}}}{N_t} + 1 \right] s_k \\ &\quad + \frac{1}{N_t} \sum_{m=1,m\neq k}^{K} A_m h_{k,i} \left|h_{m,i}\right| s_m e^{-j\theta_{m,i}} e^{j\theta_{k,i}} \\ &\quad + \frac{1}{N_t} \tilde{n}_k e^{j\theta_{k,i}} = A_k s_k. \end{aligned} \tag{27}$$

Because A_k is a positive constant, from (27), it is possible to conclude that all of the information regarding the source can be obtained from $\hat{y}_k$ when the number of antennas at the BS grows to infinity.

4.3. Analysis. The main target of any secrecy scheme is to enforce the independence between the source and the signal observed by the eavesdropper. If the independence between these signals is verified, a zero capacity for the eavesdropper channel is achieved; that is, the mutual information between the source and the eavesdropper received signal is zero.

In the remainder of this section, we mathematically demonstrate that, for the proposed joint massive MIMO precoder and security scheme, the mutual information between the source and the eavesdropper received signal is zero.

Consider the worst possible scenario, which is a noiseless eavesdropper channel. For this case, the received signal, $\tilde{\mathbf{y}}_e$, at the eavesdropper is

$$\begin{aligned} \tilde{\mathbf{y}}_e &= \lim_{\sigma_E\to 0} \mathbf{y}_e \\ &= \sum_{k=1}^{K} A_k \left[\left(\sum_{m=1,m\neq i}^{N_t} \mathbf{g}_m h_{k,m}^* \right) + \mathbf{g}_i \left|h_{k,i}\right| \right] s_R^k. \end{aligned} \tag{28}$$

As previously defined, s_R^k is equal to the original data symbol s_k but with a random phase rotation of

$$s_R^k = s_k e^{-j\theta_{k,i}}. \tag{29}$$

Then, it follows that

$$\begin{aligned} \tilde{\mathbf{y}}_e &= \lim_{\sigma_E\to 0} \mathbf{y}_e \\ &= \sum_{k=1}^{K} A_k \left[\left(\sum_{m=1,m\neq i}^{N_t} \mathbf{g}_m h_{k,m}^* \right) + \mathbf{g}_i \left|h_{k,i}\right| \right] s_k e^{-j\theta_{k,i}}. \end{aligned} \tag{30}$$

Now, let us define $\mathbf{c}_k$ and T_k as follows:

$$\begin{aligned} \mathbf{c}_k &= A_k \left[\left(\sum_{m=1,m\neq i}^{N_t} \mathbf{g}_m h_{k,m}^* \right) + \mathbf{g}_i \left|h_{k,i}\right| \right], \\ T_k &= s_k e^{-j\theta_{k,i}}. \end{aligned} \tag{31}$$

Then, the received signal at the eavesdropper can be rewritten as

$$\tilde{\mathbf{y}}_e = \sum_{k=1}^{K} \mathbf{c}_k T_k. \tag{32}$$

Note that T_k is a function of $\theta_{k,i}$ but c_k is independent of $\theta_{k,i}$. Due to the uniform distribution of $\theta_{k,i}$, any possible fixed value of T_k can be generated by any s_k, $k = 1, \ldots, K$, considering a PSK constellation. Therefore, without the knowledge of $\theta_{k,i}$, the random variable T_k is independent of s_k. As c_k and T_k are both independent of s_k, the set $(\mathbf{c}_1, \ldots, \mathbf{c}_K, T_1, \ldots, T_K)$ defines a multidimensional constellation point $\tilde{\mathbf{y}}_e$ observed by Eve and that point can be generated with equal probability by any possible set of K data symbols s_k, $k = 1, \ldots, K$. If each constellation point $\tilde{\mathbf{y}}_e$ observed by Eve can be generated with equal probability by any possible set of K data symbols, then $\tilde{\mathbf{y}}_e$ and the source are fully independent and, as a consequence, the mutual information between them is zero.

5. Evaluation Results

The numerical results regarding the secrecy capacity of the schemes defined in Sections 3 and 4 are presented in this subsection considering a QPSK constellation. For all of the results, the mutual information is measured in bits per channel use (Bpcu) in the interval $[0, 1]$. This means that when the capacity reaches the value of one, all the information from the source is obtained. However, if the mutual information is equal to zero, no information is extracted from the observed signal.

5.1. OSPR Scheme. The eavesdropper channel capacity for the OSPR scheme defined in [27] was evaluated using the lower bound provided by the *Fano inequality theorem* for several network parameters. The curves in Figure 2 describe the capacity of the eavesdropper noiseless channel computed as a function of the number of antenna elements at Eve, assuming that only one UT is accessing the network, that is, no interuser interference. The results show that for a fixed number of antenna elements at Eve, the capacity of the eavesdropper channel can be reduced by increasing the number of antennas at the legitimate transmitter. However, for a fixed number of elements at the legitimate transmitter, the secrecy capacity of the OSPR scheme reduces to zero if the number of antennas at the eavesdropper grows to infinity, thus confirming the mathematical analysis performed in Section 3.3.

The main conclusion for this first set of results is that when just one UT is accessing the network, the OSPR scheme cannot avoid the driving of the secrecy capacity to zero if the eavesdropper has an unlimited number of antenna elements.

Next, to evaluate the scheme proposed in [27] in a more realistic scenario, Figure 3 describes the capacity of the eavesdropper channel when more than one UT is present. The eavesdropper capacity curves in Figure 3 show that by increasing the number of users in the network, the capacity of the eavesdropper channel decreases, which allows the improvement of the secrecy level of the system, as verified in the analysis performed at the end of Section 3.3. However, for a reduced number of users, the OSPR technique cannot avoid the leakage of information from the legitimate link to the eavesdropper.

5.2. Proposed Joint Scheme. To compare the performance of the proposed scheme with the OSPR solution defined in [27], the secrecy capacity for the joint technique was evaluated again using the *Fano inequality theorem*, which provides a lower bound on the legitimate channel capacity and, in this case, is equal to the secrecy capacity.

The first evaluation was performed by assuming just one user terminal accessing the network, considering $N_t = 16$ and $N_e = 512$, being the results presented in Figure 4. The numerical results in Figure 4 show that for the joint design, the secrecy capacity is maximum in the high SNR regime; therefore, contrary to what occurs with the OSPR technique, the eavesdropper cannot get any information exchanged between the BS and the user terminal in this case, even by

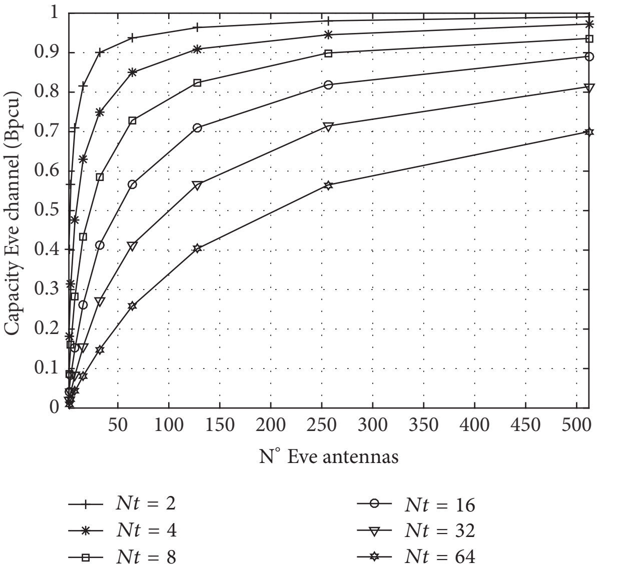


FIGURE 2: Eve channel capacity for 1 UT in a noiseless channel considering the OSPR scheme.

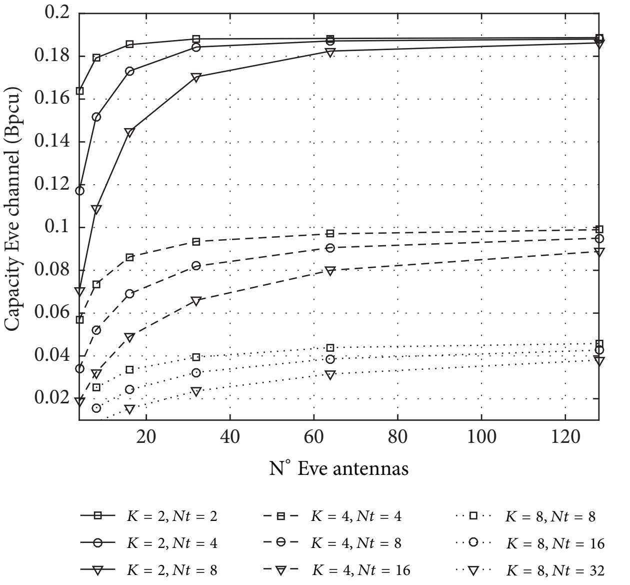


FIGURE 3: Eve channel capacity for multiple UTs in a noiseless channel.

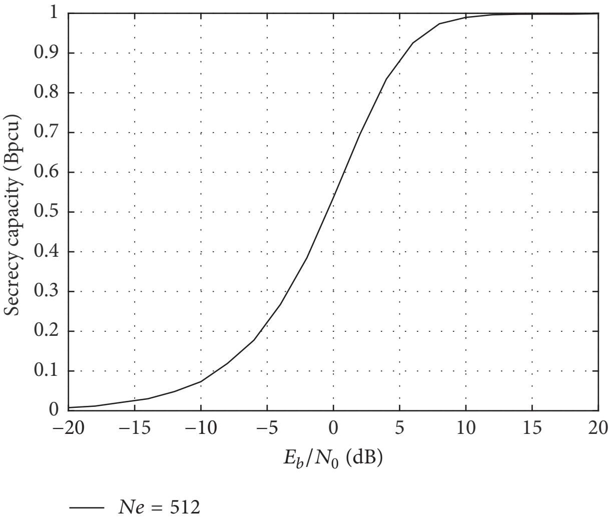


Figure 4: Secrecy capacity for the 1UT configuration considering the proposed joint scheme.

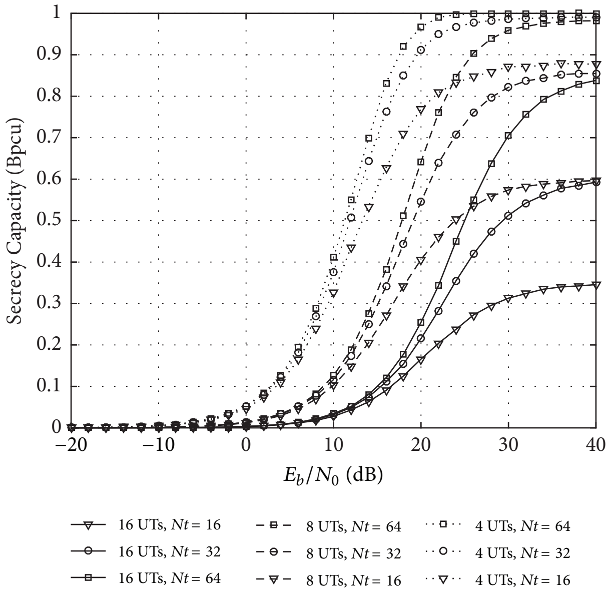


Figure 5: Secrecy capacity for multiple UTs considering the proposed joint scheme for 64 antenna elements at Eve.

employing a massive antenna array with 512 antenna elements.

For the joint solution, the secrecy capacity does not depend on the number of antenna elements at the eavesdropper, with the capacity of the eavesdropper channel being always zero.

In the results presented in Figure 5, the mean secrecy capacity was evaluated by fixing the number of antenna elements at the eavesdropper to 64. In this case, the number of antennas at the BS was defined as $N_t \in \{16, 32, 64\}$ with the number of user terminals being equal to $K \in \{4, 8, 16\}$. The analysis of the results in Figure 5 shows that by increasing the number of user terminals in the network, the secrecy capacity achieves lower values.

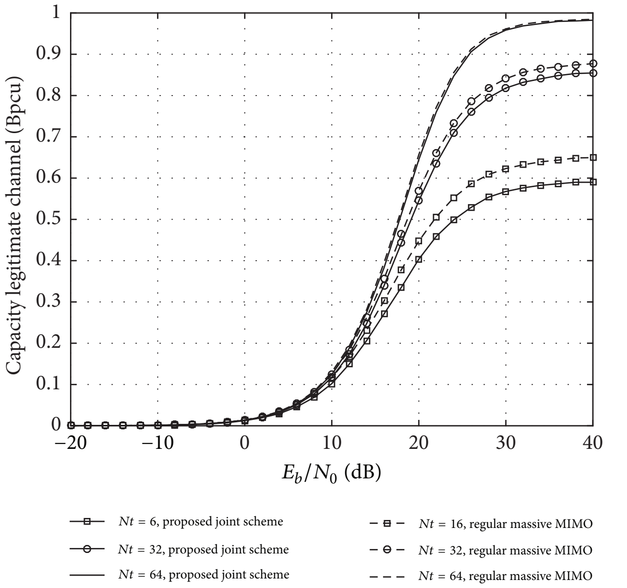


Figure 6: Secrecy capacity comparison between regular MRT massive MIMO precoding and the proposed joint scheme.

However, the cause of this reduction is the degradation of the legitimate channel capacity due to the additional interference of other user terminals, with the eavesdropper channel capacity being always zero, as mentioned before and as shown mathematically in Section 4.3. Another point that should be observed is that increasing the number of antenna elements at the BS, the secrecy capacity improves due to the multiple access orthogonalization. To assess the capacity degradation in the legitimate channel for the proposed scheme, a comparison between the capacity of a regular massive MIMO MRT precoding technique and the proposed scheme is done in Figure 6. The curves in Figure 6 were obtained for 8 user terminals and a number of antenna elements at the base station, which is defined by $N_t \in \{16, 32, 64\}$. The results show that when the number of elements at the base station is much larger than the number of user terminals accessing the network, the degradation of the legitimate channel capacity goes to zero. Therefore, the proposed joint scheme adds security to the massive MIMO system with negligible capacity loss when compared to the same massive MIMO system without any security measure.

6. Conclusion

In this work, we proposed a joint scheme to add security to massive MIMO systems. In the proposed approach, the channel precoder and security scheme are jointly designed. The joint design assures that the secured data does not become unsecure after passing through the channel precoder. As mathematically demonstrated, the simple concatenation of the two blocks, channel precoder, and security scheme, without considering the coupling between them, results in the leakage of information from the source to the eavesdropper, which can lead to the complete recovery of the transmitted data. Nevertheless, the OSPR scheme does not reduce the capacity of the legitimate link. In contrast, in the proposed joint approach, the capacity of the eavesdropper channel is zero, and the capacity of the legitimate link is only very slightly reduced. As a result, the secrecy capacity of the proposed joint scheme is much higher than the one where the channel precoder and security schemes are simply concatenated without considering the coupling between the two parts.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported by the European Regional Development Fund (FEDER), through the Competitiveness and Internationalization Operational Program (COMPETE 2020) of the Portugal 2020 framework, and by FCT/MEC through national funds, under Projects SWING2 POCI-01-0145-FEDER-016753 and UID/EEA/50008/2013.

References

[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, “A survey on wireless security: technical challenges, recent advances, and future trends,” *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[2] M. Atallah, G. Kaddoum, and L. Kong, “A survey on cooperative jamming applied to physical layer security,” in *Proceedings of the IEEE International Conference on Ubiquitous Wireless Broadband, ICUWB 2015*, Canada, October 2015.

[3] W. Stallings, *Cryptography and Network Security Principles and Practice*, Prentice Hall, NY, USA, 2006.

[4] B. Schneier, “Cryptographic design vulnerabilities,” *The Computer Journal*, vol. 31, no. 9, pp. 29–33, 1998.

[5] M. Sandirigama and R. Idamekorala, “Security weaknesses of WEP protocol IEEE 802.11b and enhancing the security with dynamic keys,” in *Proceedings of the IEEE Toronto International Conference—Science and Technology for Humanity, TIC-STH’09*, pp. 433–438, Canada, September 2009.

[6] S. A. A Mukherjee, J. Fakoorian, A. L. Huang, and A. L. Swindlehurst, “Principles of physical layer security in multiuser wireless networks: a survey,” *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[7] M. Bloch, M. Hayashi, and A. Thangaraj, “Error-Control Coding for Physical-Layer Secrecy,” *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1725–1746, 2015.

[8] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, “Coding for secrecy: An overview of error-control coding techniques for physical-layer security,” *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 41–50, 2013.

[9] D. Sarmento, J. Vilela, W. K. Harrison, and M. Gomes, “Interleaved coding for secrecy with a hidden key,” in *Proceedings of the IEEE Globecom Workshops, GC Wkshps 2015*, USA, December 2015.

[10] J. P. Vilela, M. Gomes, W. K. Harrison, D. Sarmento, and F. Dias, “Interleaved Concatenated Coding for Secrecy in the Finite Blocklength Regime,” *IEEE Signal Processing Letters*, vol. 23, no. 3, pp. 356–360, 2016.

[11] V. R. Cadambe and S. A. Jafar, “Interference alignment and degrees of freedom of the *k*-user interference channel,” *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 54, no. 8, pp. 3425–3441, 2008.

[12] D. Castanheira, A. Silva, and A. l. Gameiro, “Retrospective interference alignment: degrees of freedom scaling with distributed transmitters,” *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 63, no. 3, pp. 1721–1730, 2017.

[13] E. Tekin and A. Yener, “The general Gaussian multiple-access and two-way wiretap channels: achievable rates and cooperative jamming,” *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[14] A. L. Swindlehurst, “Fixed SINR solutions for the MIMO wiretap channel,” in *Proceedings of the 2009 IEEE International Conference on Acoustics, Speech, and Signal Processing, ICASSP 2009*, pp. 2437–2440, Taiwan, April 2009.

[15] J. Wang and A. L. Swindlehurst, “Cooperative jamming in MIMO ad-hoc networks,” in *Proceedings of the 43rd Asilomar Conference on Signals, Systems and Computers*, pp. 1719–1723, USA, November 2009.

[16] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, “Wireless secrecy regions with friendly jamming,” *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 256–266, 2011.

[17] J. Huang and A. L. Swindlehurst, “Cooperative jamming for secure communications in MIMO relay networks,” *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4871–4884, 2011.

[18] J. Yang, I.-M. Kim, and D. I. Kim, “Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers,” *IEEE Transactions on Wireless Communications*, vol. 12, no. 6, pp. 2840–2852, 2013.

[19] J. Xie and S. Ulukus, “Secure degrees of freedom of one-hop wireless networks,” *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 60, no. 6, pp. 3359–3378, 2014.

[20] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, “Massive MIMO for next generation wireless systems,” *IEEE Communications Magazine*, vol. 52, no. 2, pp. 186–195, 2014.

[21] L. Lu, G. Y. Li, A. L. Swindlehurst, A. Ashikhmin, and R. Zhang, “An overview of massive MIMO: benefits and challenges,” *IEEE Journal of Selected Topics in Signal Processing*, vol. 8, no. 5, pp. 742–758, 2014.

[22] K. Zheng, L. Zhao, J. Mei, B. Shao, W. Xiang, and L. Hanzo, “Survey of large-scale MIMO systems,” *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1738–1760, 2015.

[23] A. Swindlehurst, E. Ayanoglu, P. Heydari, and F. Capolino, “Millimeter-wave massive MIMO: the next wireless revolution?” *IEEE Communications Magazine*, vol. 52, no. 9, pp. 56–62, 2014.

[24] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, “Secure Massive MIMO transmission in the presence of an active eavesdropper,” in *Proceedings of the IEEE International Conference on Communications, ICC 2015*, pp. 1434–1440, UK, June 2015.

[25] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Transactions on Wireless Communications*, vol. 13, no. 9, pp. 4766–4781, 2014.

[26] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008.

[27] B. Chen, C. Zhu, W. Li, J. Wei, V. C. M. Leung, and L. T. Yang, "Original symbol phase rotated secure transmission against powerful massive MIMO eavesdropper," *IEEE Access*, vol. 4, pp. 3016–3025, 2016.

[28] B. Chen, C. Zhu, L. Shu et al., "Securing uplink transmission for lightweight single-antenna UEs in the presence of a massive MIMO eavesdropper," *IEEE Access*, vol. 4, pp. 5374–5384, 2016.

[29] G. Anjos, D. Castanheira, A. Silva, and A. Gameiro, "Exploiting reciprocal channel estimations for jamming to secure wireless communications," in *Proceedings of the Wireless Days (WD)*, pp. 136–142, Porto, Portugal, March 2017.

[30] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, John Wiley & Sons, NJ, USA, 2012.

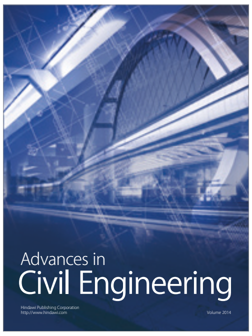
Journal of
Engineering

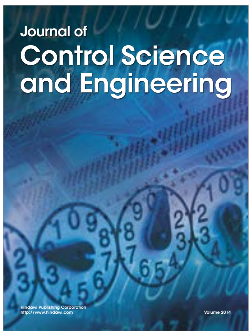
The Scientific World Journal

International Journal of
Rotating Machinery

Journal of
Sensors

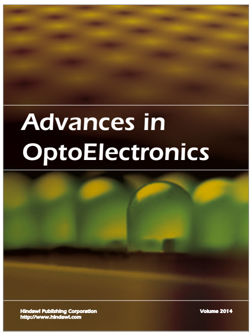
International Journal of
Distributed Sensor Networks


Advances in
Civil Engineering


Journal of
Control Science and Engineering

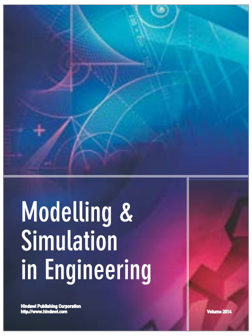
Journal of
Robotics

Journal of
Electrical and Computer Engineering

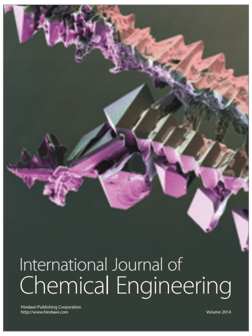

Advances in
OptoElectronics

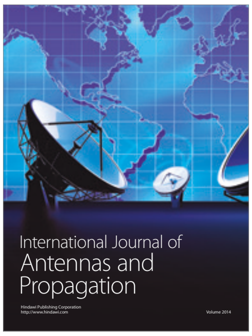
VLSI Design

International Journal of
Navigation and Observation

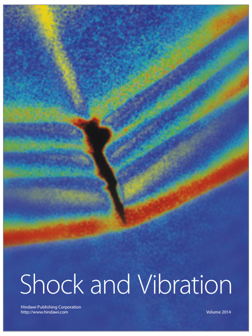

Modelling & Simulation in Engineering

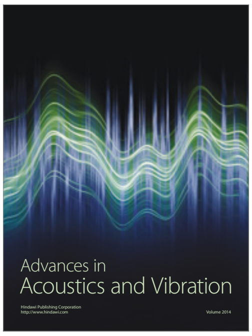
International Journal of
Aerospace Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration