IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON GREEN COMMUNICATIONS AND NETWORKING FOR 5G WIRELESS

Received May 28, 2016, accepted June 7, 2016, date of publication June 14, 2016, date of current version July 7, 2016.

Digital Object Identifier 10.1109/ACCESS.2016.2580673

Original Symbol Phase Rotated Secure Transmission Against Powerful Massive MIMO Eavesdropper

BIN CHEN[1], CHUNSHENG ZHU[2], (Student Member, IEEE), WEI LI[1], JIBO WEI[1], (Member, IEEE), VICTOR C. M. LEUNG[2], (Fellow, IEEE), AND LAURENCE T. YANG[3], (Senior Member, IEEE)

[1]College of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073, China
[2]Department of Electrical and Computer Engineering, The University of British Columbia, Vancouver, BC V6T 1Z4, Canada
[3]Department of Computer Science, St. Francis Xavier University, Antigonish, NS B2G 2W5, Canada

Corresponding author: B. Chen (lierbency@126.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 91338105 and Grant 61502518, in part by the China Scholarship Council under Grant 201306110074, in part by the Four-Year Doctoral Fellowship through The University of British Columbia, in part by the Natural Sciences and Engineering Research Council of Canada, in part by the Institute for Computing, Information, and Cognitive Systems/TELUS People and Planet Friendly Home Initiative through The University of British Columbia, in part by TELUS, and in part by the other industry partners.

ABSTRACT Massive multiple-input multiple-output (MIMO) has been extensively studied and considered as a key enabling technology for the fifth generation (5G) wireless communication systems, due to its potential to achieve high energy efficiency and spectral efficiency. As the concept of massive MIMO becomes more popular, it is plausible that the eavesdroppers will also employ massive antennas, which may remarkably enhance their ability to intercept the information. In this paper, motivated by the need to protect against the eavesdroppers equipped with powerful large antenna arrays, which has received scarce attention in the literature, a physical layer security approach called original symbol phase rotated (OSPR) secure transmission scheme is proposed to defend against eavesdroppers armed with unlimited antennas. The basic idea of the proposed OSPR scheme is to randomly rotate the phase of original symbols at the base station (BS) before they are transmitted, so that the massive MIMO eavesdropper will be confused by the intercepted signals, which may not represent the true information symbols. However, the legitimate users are able to infer the correct phase rotations and take proper inverse operations to recover the original symbols. We show that when the BS has a large enough, but finite number of antennas, the proposed OSPR scheme can achieve a considerable security performance in that the eavesdropper is unable to recover most of the original symbols, even with unlimited antennas. The process and the security performance of the proposed OSPR scheme are presented in detail. Simulation results are provided to further corroborate that the proposed OSPR scheme is a potential green secure transmission candidate technique for the future wireless networks.

INDEX TERMS Massive MIMO, physical layer security, secrecy analysis.

I. INTRODUCTION

The total energy consumption of three major telecommunication operators in China already accounted for approximately two thousandths of the comprehensive overall energy consumption of the Chinese society in 2014, as mentioned by the Vice President of China Mobile Communications Corporation in session 30 of Boao Forum for Asia Annual Conference 2016. Moreover, as the explosive growths of user demand in diverse wireless data services and computation power of mobile devices continue to intensify, energy consumption of wireless communication infrastructures has become a serious and vital issue, which cannot be effectively and efficiently accommodated by the current fourth generation (4G) of wireless communications technology [1]. Thus it is of great importance to develop and adopt green and energy-efficient broadband transmission schemes in the framework of the upcoming fifth generation (5G) communication systems. Massive multiple-input multiple-output (MIMO) [2], which is also known as large MIMO, full-dimension MIMO, or large-scale antenna systems, is one of those green communication technologies [3] that has the potential to significantly alleviate the energy and spectrum consumption crises in the

near future. Massive MIMO is currently under extensive investigations by both scientists and industrialists. It is widely considered to be a promising and critical technology to meet the requirements of unprecedented high energy efficiency and high spectral efficiency for green communications and networking envisioned in 5G systems [4]–[9], along with the forthcoming Internet of Things (IoT) [10].

Specifically, massive MIMO is capable of shifting most of the signal processing and computing loads from the user terminals (UTs) to the base stations (BSs), by leveraging time-division duplexing (TDD) and large antenna arrays with several hundred service antennas or more [11]. The energy consumption of battery-powered UTs can thus be significantly reduced, and the corresponding service life can be effectively prolonged. Furthermore, the exploitation of excess service antennas and law of large numbers at the BS enables the radiated energy to be extremely focused into certain intended regions in space, comparing with conventional MIMO schemes. This helps dramatically improve the signal beamforming sharpness and selectivity, which leads to much less interference between different UTs. Therefore, tens or more UTs are allowed to be simultaneously served in the same time-frequency resource block without badly interfering with each other [4]–[6]. Remarkable reduction in the required radiated power is also obtained in transmitting signals on both forward and reverse links [8], [9], while maintaining a certain system throughput. In addition to enhancing energy efficiency and spectral efficiency, the much sharper and finer wave beams with better directivity and selectivity, which are sophisticatedly generated by a massive MIMO BS under either line-of-sight or cluttered channel conditions, also benefit the physical layer security during signal transmissions [12], [13].

Physical layer security exploits the inherent characteristics and independent randomness of communication channels and noise to achieve secure transmissions [14]. Due to the open nature of wireless channels and the significance of information security, it has prompted decades of studies in various aspects since Wyner's pioneering work [15]. Note that physical layer security does not compete with traditional cryptographic technologies that are based on computational complexity. The former has complementary features and can be utilized to further enhance the security level of existing communication systems from the physical layer, which is independent of the higher layers. Along with the framework of wireless communication system evolving from single-input single-output (SISO) to point-to-point MIMO, multi-user MIMO, and massive MIMO as the state-of-the-art, different physical layer security techniques [16] have emerged.

At present, massive MIMO is already envisioned as a key enabling technology for 5G wireless cellular systems, due to its potential to reap and greatly strengthen all the advantages of conventional MIMO. However, while massive MIMO has attracted extensive attention, relatively few work has been done on the combination of physical layer security and massive MIMO [12]. The potential of massive MIMO to further boost the performance of physical layer security is not yet well recognized. Although the research on secrecy performance of conventional MIMO has produced considerable results, use of large antenna arrays is introducing new vitality into this area of research. Massive MIMO is not merely an extension of conventional MIMO when physical layer security is incorporated. As the number of BS antennas grows large, conventional MIMO turns into massive MIMO and becomes inherently immune to some issues [17], which can be viewed as an example of how quantitative change leads to qualitative change.

Secure transmission in multi-cell multi-user massive MIMO system with maximum ratio transmission (MRT) precoding and artificial noise (AN) [18] at the BS is investigated in detail in [19], which shows that with massive MIMO BS, random AN shaping matrices can offer a favorable performance/complexity tradeoff compared with conventional AN shaping matrices. In conventional MIMO systems the latter is usually designed to lie in the null space of the main channel to ensure that legitimate UTs are not affected. However, the corresponding computational cost is not affordable in the case of a large channel matrix. With the benefits of massive MIMO, use of random AN to avoid computing the null space of a large matrix is a more attractive option due to its low complexity and considerable performance. The underlying reason is that unlike conventional MIMO, the interference of uncorrelated random AN vanishes as the number of BS antennas grows large. Additionally, the authors of [19] also point out that even with AN assistance, secure communication may not be guaranteed if the eavesdropper has too many antennas.

A key feature of massive MIMO is power scaling [8], which enables tremendous reduction in radiated energy expenditure while maintaining the system performance. It benefits both the battery-powered UTs and the BSs with low power consumption requirements, and makes massive MIMO a green technology. It also can be utilized to improve the secrecy performance of massive MIMO systems to a considerable extent. Exploiting the potential of power scaling law to secure wireless communication system is first reported in [20]. The assumptions of perfect channel state information (CSI) at the BS and a finite number of passive eavesdropper antennas are made in a single-cell scenario. A parameter called radiated power scaling (RPS) factor is proposed to optimally adjust the overall transmit power with different number of BS antennas. It demonstrates that with judiciously selected RPS factor, multiuser massive MIMO can decrease the achievable rate of an eavesdropper to almost zero while satisfying the rate requirements of legitimate UTs at a very low power consumption, without any assistance of AN or something else. The underlying essence is that by increasing the number of BS antennas and exploiting the power scaling law, we can properly adjust the RPS factor and choose a just-right transmit power to coherently focus the required energy to a specific spatial point through the sharp and fine beam generated by massive MIMO, while keeping the field strength

anywhere else as low as possible, thus maximally suppressing the achievable rate of the eavesdropper. This is different from beamforming, which is aimed at targeting the specific signals to the intended UTs. The power scaling feature makes massive MIMO a natural green secure transmission technique. In [21], the above work is further extended to the scenario in which the numbers of single-antenna legitimate UTs and antennas at the eavesdropper grow proportionally with the number of BS antennas. The corresponding results show that the optimal RPS factor converges to a different constant limit compared with the case of finite antennas at the eavesdropper. The secrecy performance is mainly determined by the ratios between the numbers of BS antennas, legitimate UTs and eavesdropper antennas. This indicates that positive secrecy rate may not be guaranteed if the ratio between the number of eavesdropper antennas and the number of BS antennas exceeds a certain limit.

The secrecy performance of power scaling in multi-cell massive MIMO scenario is then examined in [22]. The effects of pilot contamination, the length and power of pilot sequence and the power of data stream are all taken into account. The analysis shows that positive secrecy rate is still achievable at low cost via power scaling only, provided that the number of eavesdropper antennas is smaller than a threshold. In [17], both no training-phase jamming and training-phase jamming attack are studied in detail for physical layer security of massive MIMO downlink communications from the information theory perspective. The authors propose a δ-conjugate beamforming approach, which is also a power scaling strategy in essence, to achieve secure transmission without using stochastic encoding in the case of no training-phase jamming. Then pilot signal assignments encryption using cryptography and δ-conjugate beamforming are used in combination to defend against the active training-phase jamming attack, which aims at steering the beams towards the eavesdropper. Note that the fundamental premise of successful defense against the attack is that the number of BS antennas is above a certain threshold, which is a monotonic increasing function of the number of antennas at the eavesdropper. Therefore, the proposed strategies will not work effectively if the eavesdropper has a sufficient number of antennas to break this security premise.

From the above, we can see that if the eavesdropper is equipped with much more powerful massive MIMO or multiple eavesdroppers collaborate to form a large enough antenna array, almost all the existing physical layer security approaches based on signal processing, e.g., beamforming, AN aided precoding, or power scaling, will lose the battle against the adversaries. This phenomenon is also partly observed in [23] and [24], which are mainly dealing with conventional MIMO physical layer security. The underlying principle is that by deploying sufficiently powerful antennas, the adversary will have abundant spatial freedom degrees to facilitate the related signal processing, such as collecting weak signals or neutralizing the jamming interference, which results in a significant degradation in terms of secrecy rate. However, most of the physical layer security research work has avoided this issue, and to the best of our knowledge, so far little work exists that specifically aims at addressing the security problems of counteracting powerful massive MIMO eavesdroppers.

As pointed out in the subsection 'The Adversary Is Not Powerful' in [25], instead of spending money on buying extra computing resources of little use, really smart adversaries would prefer to employ more and better antennas to increase the area of monitoring and the ability of interception, which is indeed affordable and more aggressive. Therefore, it is necessary to address the physical layer security issues pertaining to the defense against eavesdroppers armed with powerful massive MIMO in the upcoming 5G era, since large antenna arrays will become popular by then.

Motivated by the possibility of facing powerful large antenna arrays equipped eavesdroppers, in this paper we propose an original symbol phase rotated (OSPR) secure transmission strategy to defend against eavesdroppers who are capable of driving the secrecy rate on the forward communication link to zero with massive MIMO. The basic idea of the proposed OSPR scheme is to randomly change the phase of original symbols at the BS before the symbols are transmitted, so that the massive MIMO eavesdropper can only perfectly intercept the phase rotated symbols even in the best case, while legitimate UTs are able to infer the correct phase rotations and take the inverse operation to recover the original symbols. Note that massive MIMO is used at the BS to facilitate the random rotation of symbol phase. As long as the eavesdropper cannot acquire the corresponding rotated phase, its interception will be full of symbol errors, no matter how many antennas it has. The proposed OSPR approach protects the data symbols at the initial stage and circumvents the security problem by avoiding fighting directly against the powerful massive MIMO eavesdropper. Moreover, the OSPR scheme employs the massive MIMO technique and spends no extra power on AN or jamming, thus making it potentially a green secure candidate transmission technique for 5G.

The rest of this paper is organized as follows. In Section II the forward link system model is described. Sections III presents the proposed OSPR secure transmission scheme in detail. In Section IV, we analyze the security performance of OSPR scheme, and Section V provides some simulation results. Finally, Section VI concludes the paper.

Notation: Uppercase and lowercase boldface letters denote matrices and column vectors. X^T, X^*, X^H and X^{-1} denote the transpose, conjugate, conjugate transpose and inverse of matrix X, respectively. I_N denotes the N-dimensional identity matrix, and 0_N denotes the all-zero column vector of length N. $|x|$ denotes the absolute value of a complex scalar x. We use $\|\cdot\|$ to denote the Frobenius or Euclidean norm of a matrix or vector, and $tr\,(X)$ to denote the trace of matrix X. The expectation and variance of the random variable x are denoted by $E\,(x)$ and $Var\,(x)$, respectively. $\mathbb{C}^{m\times n}$ represents the space of all $m \times n$ matrices with complex elements. $\mathbf{x} \sim \mathcal{CN}(0_N, \Sigma)$ denotes a circularly symmetric complex

Gaussian random vector $\mathbf{x} \in \mathbb{C}^{N\times 1}$ with zero mean and covariance matrix Σ.

II. SYSTEM MODEL

In this paper, we consider secure transmissions on the forward link in a single-cell scenario, in the presence of a passive eavesdropper armed with an unlimited number of antennas to intercept the transmitted signals, as shown in Fig. 1. A massive MIMO BS with a large but finite number of antennas simultaneously sends K mutually independent data streams to K autonomous single-antenna legitimate UTs, where data stream k is intended for UT k only. The number of BS antennas is denoted by N_b, and the number of eavesdropper antennas is denoted by N_e. Then we have $N_e \gg N_b \gg K > 0$, where N_b and K are finite, and N_e is infinite. Hence, both the BS and the eavesdropper have massive MIMO antenna arrays while the latter is far more powerful. The considered massive MIMO system operates in TDD mode. Reverse training and channel reciprocity, which means that the forward link channel matrix is the transpose of the reverse link channel matrix, are both used in the proposed OSPR scheme.

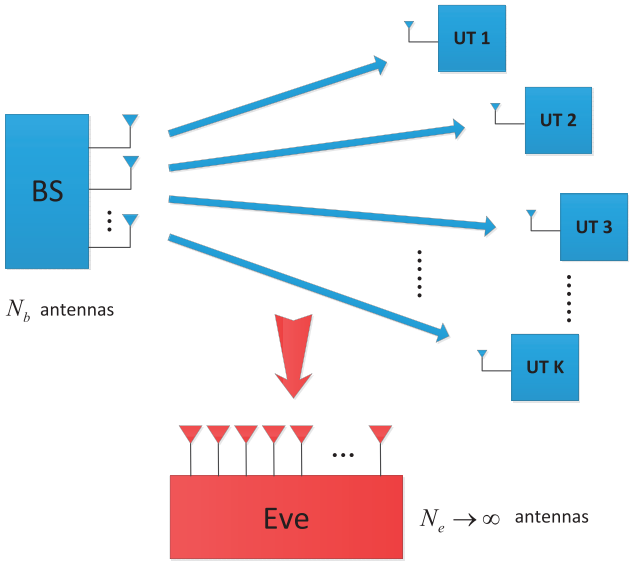


FIGURE 1. System model of the considered scenario.

A. CHANNEL MATRIX

We denote the channel matrix from the massive MIMO BS to the K legitimate UTs on the forward link as

$$\mathbf{H} = \begin{bmatrix} \mathbf{h}_{r,1} \\ \mathbf{h}_{r,2} \\ \vdots \\ \mathbf{h}_{r,K} \end{bmatrix} = \begin{bmatrix} \mathbf{h}_{c,1} & \mathbf{h}_{c,2} & \cdots & \mathbf{h}_{c,N_b} \end{bmatrix} = \begin{bmatrix} h_{1,1} & h_{1,2} & \cdots & h_{1,N_b} \\ h_{2,1} & h_{2,2} & \cdots & h_{2,N_b} \\ \vdots & \vdots & \ddots & \vdots \\ h_{K,1} & h_{K,2} & \cdots & h_{K,N_b} \end{bmatrix}, \quad (1)$$

and the channel matrix from the massive MIMO BS to the massive MIMO eavesdropper as $\mathbf{G} \in \mathbb{C}^{N_e\times N_b}$. The row vector $\mathbf{h}_{r,k} \in \mathbb{C}^{1\times N_b}$, $k = 1, 2, \ldots, K$, in (1) represents the channel vector from the BS to UT k. The column vector $\mathbf{h}_{c,i} \in \mathbb{C}^{K\times 1}$, $i = 1, 2, \ldots, N_b$, in (1) represents the channel vector from the ith BS antenna to all K UTs. We assume that all the channel matrix elements are independent and identically distributed (i.i.d.) $\mathcal{CN}(0, 1)$ random variables; thus none of the terminals are collocated. All the channels are assumed to be flat fading and block-invariant within a certain coherent interval length T, which facilitates the exploitation of channel reciprocity.

B. TRANSMITTED SIGNAL

The massive MIMO BS performs MRT precoding on the forward link. We assume that the BS adopts the optimal RPS factor derived in the limit case in [20, eq. (22)] to achieve a good energy efficiency and security performance trade-off. Then the final transmitted signal vector $\mathbf{x} \in \mathbb{C}^{N_b\times 1}$ after MRT precoding at the massive MIMO BS is given by

$$\mathbf{x} = \sum_{k=1}^{K} \mathbf{x}_k = \sum_{k=1}^{K} \frac{\mathbf{h}_{r,k}^H}{N_b} s_k, \quad (2)$$

where the mutually independent complex symbol s_k, $k = 1, 2, \ldots, K$, with uniform power constraint $E\left(\|s_k\|^2\right) \le p_s$, represents the original data symbol intended for UT k.

The total radiated power of the massive MIMO BS is given by

$$P_{total} = E\left(\|\mathbf{x}\|^2\right) = \sum_{k=1}^{K} \frac{\left\|\mathbf{h}_{r,k}^H\right\|^2}{(N_b)^2} \mathbf{E}\left(\|s_k\|^2\right) \overset{(a)}{\approx} \sum_{k=1}^{K} \frac{1}{N_b} \mathbf{E}\left(\|s_k\|^2\right), \quad (3)$$

where step (a) follows the law of large numbers and the corresponding results in [8, eqs. (4) and (5)], when N_b is large enough.

C. RECEIVED AND INTERCEPTED SIGNALS

The massive MIMO BS transmits the signal vector x on the forward link, then the kth UT receives signal $r_{b,k}$, $k = 1, 2, \ldots, K$, given by

$$r_{b,k} = \mathbf{h}_{r,k}\mathbf{x} + n_k = \frac{\mathbf{h}_{r,k}\mathbf{h}_{r,k}^H}{N_b} s_k + \sum_{i=1, i\neq k}^{K} \frac{\mathbf{h}_{r,k}\mathbf{h}_{r,i}^H}{N_b} s_i + n_k, \quad (4)$$

and the massive MIMO eavesdropper intercepts signal vector $\mathbf{r}_e \in \mathbb{C}^{N_e\times 1}$, given by

$$\mathbf{r}_e = \mathbf{G}\mathbf{x} + \mathbf{n}_e, \quad (5)$$

where all the entries of the receiver noise vectors n_k and $\mathbf{n}_e \in \mathbb{C}^{N_e\times 1}$ are i.i.d. $\mathcal{CN}(0, \sigma_k^2)$ and $\mathcal{CN}(0, \sigma_e^2)$ random variables, respectively.

III. ORIGINAL SYMBOL PHASE ROTATED SECURE TRANSMISSION

The OSPR approach is proposed on the forward link transmission to defend against an eavesdropper armed with powerful enough massive MIMO. We consider the worst case in this paper that the number of antennas at the eavesdropper is infinite to meet the 'sufficient powerful' condition, as mentioned in Section II. Although some jamming techniques can achieve positive secrecy rate in the case that the eavesdropper has more antennas than the BS, they will need unlimited power to maintain a positive secrecy rate as the number of eavesdropper's antennas grows infinitely large, which is unbearable and extremely energy inefficient. The eavesdropper with unlimited number of antennas will make most of the existing physical layer security approaches impotent. In this section, we thoroughly present the proposed OSPR green secure transmission scheme to address this issue, which has the following stages.

A. REVERSE TRAINING

First, each of the K UTs simultaneously sends a sequence of pilot signal to the massive MIMO BS on the reverse link. The pilot signals transmitted by different UTs all have a length of τ symbols, where $K \leq \tau < T$ and T is the coherence interval length as defined in Section II. This guarantees that all the pilot signal sequences can be mutually orthogonal, which are the optimum training signals. The used pilot signals are denoted as matrix $\sqrt{p_p}\mathbf{\Phi}$, where $\mathbf{\Phi} \in \mathbb{C}^{K\times\tau}$ is a unitary matrix with $\mathbf{\Phi}\mathbf{\Phi}^H = \mathbf{I}_K$ and p_p is the power of the length τ pilot signal sequence. The mutually orthogonal pilot signals are known at the BS and the eavesdropper, and we assume that the massive MIMO BS is able to perfectly estimate the forward link channel matrix $\mathbf{H}$ by exploiting the received training pilot sequences and channel reciprocity.

B. RANDOMLY ROTATE THE ORIGINAL SYMBOL PHASE

At this stage, the massive MIMO BS utilizes the information of the obtained column vector $\mathbf{h}_{c,i} \in \mathbb{C}^{K\times 1}, i = 1, 2, \ldots, N_b$, in (1) of the channel matrix $\mathbf{H}$ to change the phase of original complex symbol $s_k, k = 1, 2, \ldots, K$. The expansion of $\mathbf{h}_{c,i}$ is expressed as

$$\mathbf{h}_{c,i} = \begin{bmatrix} \mathbf{h}_{1,i} \\ \mathbf{h}_{2,i} \\ \vdots \\ \mathbf{h}_{K,i} \end{bmatrix}, \tag{6}$$

where the complex vector element $h_{k,i}, k = 1, 2, \ldots, K$, represents the channel from the ith massive MIMO BS antenna to the kth UT.

The ith antenna is randomly chosen from the N_b antennas at the BS. Then the phase rotated symbol for UT k is given by

$$s_{ospr,k} = s_k \cdot e^{j\angle h_{k,i}}, \tag{7}$$

where $\angle h_{k,i}$ denotes the phase of the complex entry $h_{k,i}$. After finishing this random phase changing operation, $s_{ospr,k}$ is used to replace the original symbol s_k in (2). The randomly rotated symbol $s_{ospr,k}$ will then be processed by MRT precoding method according to the steps shown in Section II, and the original symbol s_k is hidden.

C. BROADCAST THE REFERENCE SIGNAL

After the process of random phase rotation is finished, the massive MIMO BS uses the ith antenna which is chosen in the last step to directly broadcast a reference signal. The reference signal has a length of λ symbols, where $1 \leq \lambda < T - \tau$. We assume that the reference signal is known to all terminals including the massive MIMO eavesdropper.

Then UT k can estimate the corresponding channel information $h_{k,i}$ by exploiting the forward link broadcasted reference signal, and we assume the estimation is perfect. With the acquired knowledge of $h_{k,i}$, UT k is able to obtain the rotation phase $\angle h_{k,i}$. It is worth emphasizing that only the selected ith antenna is used to broadcast the reference signal, and one symbol length may be enough for UT k to estimate the CSI $h_{k,i}$ in the ideal situation. So the related resource burden for broadcasting the reference signals is small.

D. DATA TRANSMISSION AND SYMBOL RECOVERY

The massive MIMO BS then sends the signal vector $\mathbf{x}$ to all legitimate UTs, which contains the rotated symbol $s_{ospr,k}$, $k = 1, 2, \ldots, K$, not the original symbol s_k. The kth legitimate UT first receives the signal $r_{b,k}$, then its receiver outputs $\hat{s}_{ospr,k}$ which is the detection result based on (4). Finally, the UT k recovers the original symbols by taking the following inverse operation

$$\hat{s}_k = \hat{s}_{ospr,k} \cdot e^{j\left(-\angle h_{k,i}\right)}, \tag{8}$$

where the angle information $\angle h_{k,i}$ is obtained by exploiting the reference signal in the last step, $\hat{s}_k$ is the final recovered result of the original symbol s_k.

E. STRUCTURE OF THE COHERENCE INTERVAL

All the activities above and the structure of the corresponding coherence interval are summarized in Fig. 2. The massive MIMO eavesdropper intercepts the transmission signals all the time.

Moreover, in the case that the coherence interval is long enough to accommodate multiple data symbols, the random phase rotation process in the proposed OSPR security scheme can be further used symbol by symbol or on demand to enhance the secrecy performance, since there are many antennas at the massive MIMO BS that can be randomly chosen without repetition. In this situation, the reference signal broadcasting step is repeated, in order to let the legitimate UTs acquire the updated information of the rotated phase, which can be equivalently viewed as the encryption key in traditional cryptography. The corresponding structure is also presented in Fig. 2.

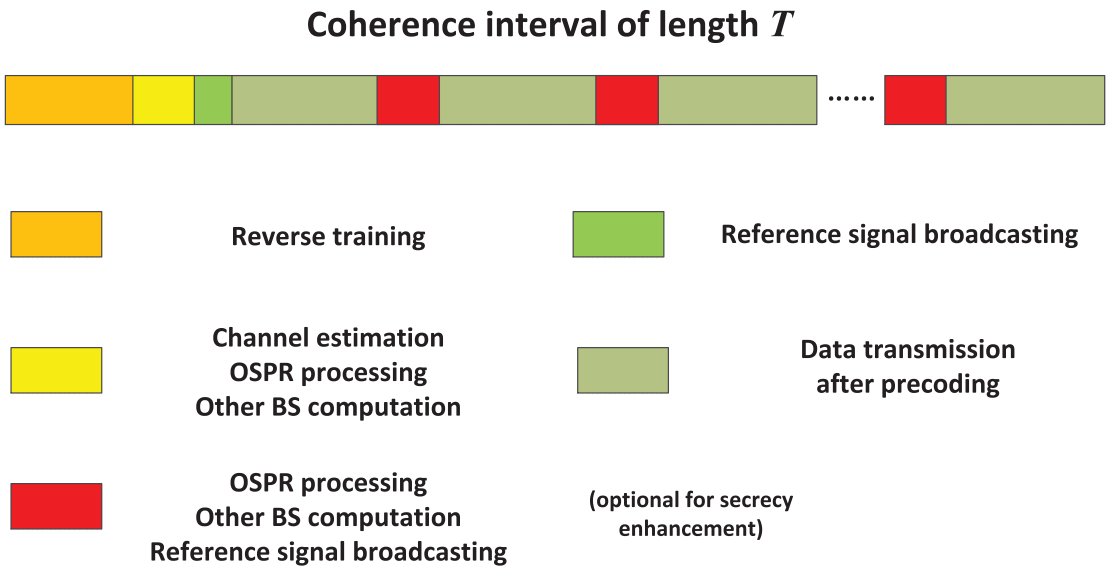


FIGURE 2. The coherence interval structure of the OSPR secure transmission scheme.

IV. SECURITY ANALYSIS

In this section, the secrecy performance of the proposed OSPR secure transmission scheme on the forward link is analyzed in detail. We present the analysis by closely following each of the steps of the OSPR scheme described in Section III. The massive MIMO eavesdropper is assumed to have perfect knowledge of the mechanism about the OSPR scheme. The importance of equipping large number of antennas at the BS is presented. We show that the massive MIMO eavesdropper can hardly obtain the real data symbols although it is armed with an unlimited number of antennas.

A. SECURITY AT THE STAGE OF REVERSE TRAINING

At this stage, the K legitimate UTs transmit the mutually orthogonal pilot signals to the massive MIMO BS. We consider the worst case scenario that the massive MIMO eavesdropper can perfectly intercept the pilot signals. Then it is able to perfectly infer the CSI between itself and the legitimate UTs. However, it cannot extract any information about the main channel $\mathbf{H}$. This is because, first, all terminals are not colocated and all the channels are independent as presented in Section II, and second, no information of $\mathbf{H}$ is used by any UT in the reverse training phase. Hence, even if the massive MIMO eavesdropper has an infinite number of antennas and can exploit powerful blind channel estimation techniques, it can hardly acquire any information about $\mathbf{H}$.

B. SECURITY AT THE STAGE OF RANDOM PHASE ROTATION

The massive MIMO BS performs the channel estimation, random phase rotation, MRT precoding and other necessary signal processing and computations locally and quietly, without radiating any signals. Thus the massive MIMO eavesdropper can do nothing but wait. It is obvious that no information can be intercepted and the powerful eavesdropper antenna array is useless at this stage.

C. SECURITY AT THE STAGE OF REFERENCE SIGNAL BROADCASTING

We consider the worst case scenario that the massive MIMO eavesdropper is able to perfectly intercept the reference signal broadcasted by the ith BS antenna, and perfectly obtain the CSI between itself and the ith antenna which is randomly selected at the massive MIMO BS. Nonetheless, the massive MIMO eavesdropper still cannot extract any information about the main channel CSI matrix $\mathbf{H}$ from the intercepted reference signal. The reason is similar to the case at the stage of reverse training, and it is not further repeated here.

Moreover, the massive MIMO eavesdropper can hardly get the overall information about the CSI matrix $\mathbf{G}$ between itself and the BS by learning the reference signal, since only one antenna among the large number of candidate antennas at the BS is randomly chosen to broadcast the reference signal, and all the channels are time-varying. Nor can the eavesdropper know which antenna is chosen to broadcast the reference signal in the considered scenario, since the random selection process is locally performed at the massive MIMO BS, and the intercepted reference signal can provide little useful information when the entire knowledge of the channel matrix $\mathbf{G}$ is absent.

D. SECURITY AT THE STAGE OF DATA TRANSMISSION

At this stage, the massive MIMO BS transmits the processed data symbols through the open wireless medium. We consider

the worst case scenario that the massive MIMO eavesdropper is able to perfectly estimate the equivalent CSI, which is the product of the precoding matrix and the channel matrix $\mathbf{G}$, by exploiting powerful channel estimation approaches (either blind or not). Furthermore, it can perfectly extract $s_{ospr,k}$, $k = 1, 2, \ldots, K$, which is the de facto symbol transmitted by the massive MIMO BS, from the intercepted signal vector $\mathbf{r}_e$ without any contamination by cancelling all the interferences and receiver noises.

However, the perfectly obtained equivalent CSI cannot be exploited to extract useful information about the main channel matrix $\mathbf{H}$, since the massive MIMO eavesdropper only acquires little knowledge of the channel matrix $\mathbf{G}$ at the last stage of reference signal broadcasting. Hence, the massive MIMO eavesdropper knows little about the CSI matrix $\mathbf{G}$, $\mathbf{H}$ and which antenna is randomly chosen to change the phase of the original symbol s_k, according to the analysis above. Then it can hardly acquire the information of $\angle h_{k,i}$. Thus even if the massive MIMO eavesdropper has an unlimited number of antennas and knows that the symbol $s_{ospr,k}$ is not the right one, it cannot recover the original symbol s_k without the knowledge of $\angle h_{k,i}$. Finally, the legitimate UTs can recover the original symbol to correctly acquire the transmitted information, while the massive MIMO eavesdropper only obtains the signals that are randomly rotated.

E. EFFECT OF THE MASSIVE ANTENNAS AT THE BS

The BS adopts massive MIMO techniques to improve the energy efficiency. More importantly, the large number of BS antennas enhances the secrecy performance of the proposed OSPR secure transmission scheme. This is because the OSPR scheme randomly selects one antenna among all the BS antennas to encrypt the original symbol. The random selection process is the key factor of the OSPR secure transmission strategy. The more candidate antennas at the BS available for random selection, the harder it is for the massive MIMO eavesdropper to guess which antenna is chosen and acquire the information of $\angle h_{k,i}$, and successfully recover the original symbols.

Consider the simple case that the BS has two antennas and only one UT is served. The random phase rotation process of the OSPR security scheme is used symbol by symbol in this case. Since there are only two antennas at the BS, the eavesdropper can acquire the entire knowledge of the two column vectors of channel matrix $\mathbf{G}$ by intercepting the reference signal twice or more, during one coherence interval. Then it can exploit the perfectly estimated equivalent CSI matrix, which is the product of precoding matrix and the channel matrix G, at the data transmission stage to further infer the information of the channel matrix $\mathbf{H}$. From the perspective of the powerful massive MIMO eavesdropper, now it may be able to exhaustively test the rotated phase $\angle h_{k,i}$, and finally recover the original symbol. However, if the BS has a massive number, e.g., tens or hundreds of antennas, then the channel matrix $\mathbf{G}$ will be too large for the eavesdropper to exhaustively learn during one coherence interval. Therefore, the massive MIMO eavesdropper can hardly recover the original symbol when the BS has enough antennas to randomly choose from. This presents the key role of the large antenna array at the BS on enhancing the security performance.

V. SECURITY PERFORMANCE EVALUATION

In this section, we evaluate the security performance of the proposed OSPR secure transmission scheme, and simulation results are presented.

We consider the practical case that the original symbol s_k, $k = 1, 2, \ldots, K$, is finite alphabet quadrature phase-shift-keying (QPSK) modulated, and the constellation is

$$\left\{ \frac{\sqrt{2}}{2}(1+j), \frac{\sqrt{2}}{2}(1-j), \frac{\sqrt{2}}{2}(-1+j), \frac{\sqrt{2}}{2}(-1-j) \right\}, \tag{9}$$

where the modulated symbol power is normalized. We set $N_b = 64, 128, 256, 512, 1024$ and $K = 16$, where $N_b = 64$ is assumed to be large enough for the proposed OSPR scheme to work properly, as mentioned in Section IV. This assumption is made for the convenience of simulations. The signal-to-noise ratio (SNR) of the kth UT is $SNR_k = \frac{1}{\sigma_k^2}$. We consider the worst case scenario that the eavesdropper has an unlimited number of antennas, i.e., $N_e = \infty$, and $\sigma_e^2 = 0$, which means that the corresponding $SNR_e = \infty$. Therefore, it can perfectly intercept the transmitted signal symbol $s_{ospr,k}$.

We emphasize that if the chosen $\angle h_{k,i} \leq \frac{\pi}{4}$ or $\angle h_{k,i} \geq \frac{7\pi}{4}$, then the original symbol s_k will not be rotated since QPSK modulation is employed. Otherwise, the original symbol will be rotated to the corresponding quadrant, and replaced by the QPSK symbol that is in the same quadrant. The legitimate UTs are aware of these rules. Furthermore, throughout this paper, we assume that all the channel estimations are perfect.

First, we analyze the symbol error rate (SER) of the massive MIMO eavesdropper. We assume that the eavesdropper aims at intercepting the symbols sent to the kth UT. Since the rotated symbol $s_{ospr,k}$ can be perfectly intercepted, the SER of the eavesdropper is the probability $\Pr\left\{\frac{\pi}{4} < \angle h_{k,i} < \frac{7\pi}{4}\right\}$ when the ith BS antenna is randomly chosen, where $\Pr\left\{\frac{\pi}{4} < \angle h_{k,i} < \frac{7\pi}{4}\right\}$ is exactly the probability that the original symbol s_k is rotated. This is due to the employed OSPR secure transmission scheme. The $\angle h_{k,i}$ is uniformly distributed over the range $[0, 2\pi]$, since $h_{k,i}$ is an i.i.d. $\mathcal{CN}(0, 1)$ random variable as defined in Section II. We also assume that the ith antenna is randomly chosen with equal probability from all the BS antennas. Therefore, the SER $P_{e,SER}$ of the powerful massive MIMO eavesdropper is given by

$$\begin{aligned} P_{e,SER} &= \sum_{i=1}^{N_b} \frac{1}{N_b} \cdot \Pr\left\{\frac{\pi}{4} < \angle h_{k,i} < \frac{7\pi}{4}\right\} \\ &= \Pr\left\{\frac{\pi}{4} < \angle h_{k,i} < \frac{7\pi}{4}\right\} \\ &= \frac{3}{4}. \end{aligned} \tag{10}$$

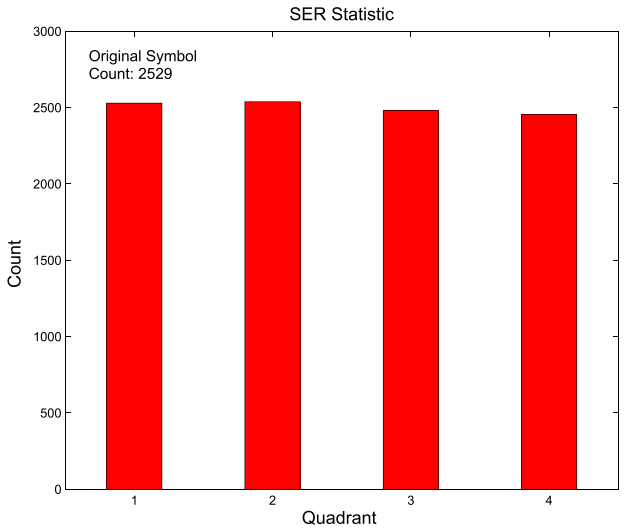


FIGURE 3. SER of the massive MIMO eavesdropper.

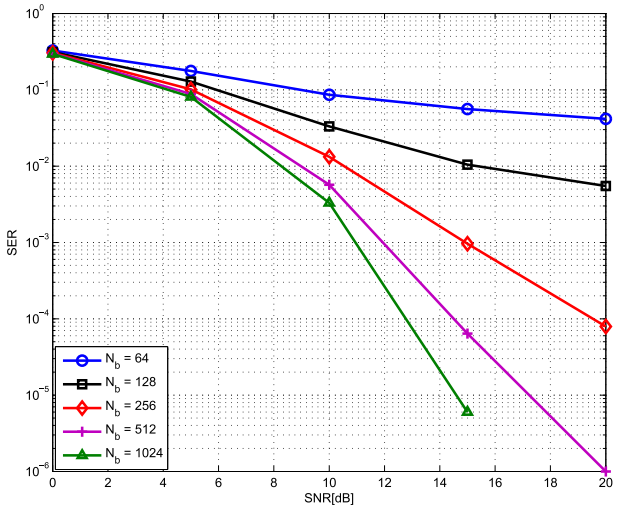


FIGURE 4. SER of the *k*th user terminal.

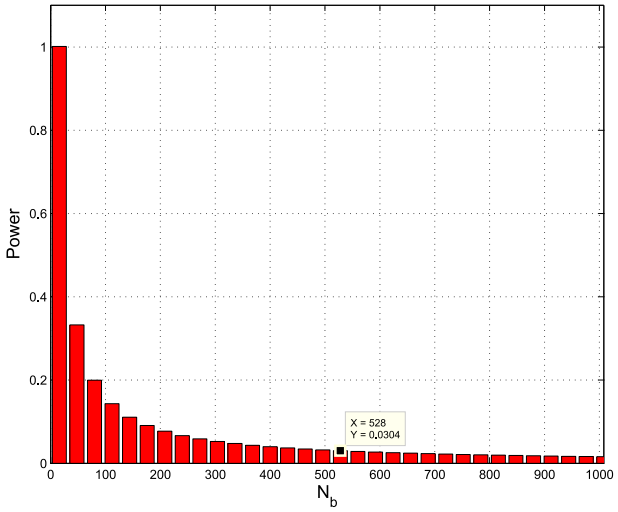


FIGURE 5. The total radiated power of the massive MIMO BS.

The eavesdropper SER simulation result is shown in Fig. 3. We set $N_b = 64$ and the random phase rotation process is used once in every coherence interval. We assume that the length of data transmission shown in Fig. 2 in one coherence interval is 1, for the convenience of simulation. Then 10000 coherence intervals are simulated, which means 10000 symbols are tested in total. The original QPSK symbol is $\left\{\frac{\sqrt{2}}{2}(1+j)\right\}$, which is in the first quadrant of the modulated constellation. The X axis in Fig. 3 denotes the quadrant where the intercepted symbols fall in. From the plot we can see that 2529 symbols intercepted by the massive MIMO eavesdropper are in the first quadrant, which means the remaining 7471 symbols are wrong. Thus the simulated SER is 0.7471, or approximately 0.75. This verifies the analytical result. The figure also shows that the number of symbols in different quadrant are almost identical, since the rotated angle $\angle h_{k,i}$ is uniformly distributed over the range $[0, 2\pi]$. The high SER of the eavesdropper indicates a great reduction of the successfully recovered original information, and corroborates the security performance of the proposed OSPR scheme.

Next, the SER plot for the kth legitimate UT as a function of SNR_k when the OSPR scheme is employed, is shown in Fig. 4. 10000, 100000 and 1000000 symbols are simulated for the case of 64, 128 and 256 BS antennas, respectively. 5000000 symbols are simulated for the case of 512 and 1024 BS antennas. We can see that as the number of BS antennas increases, the SER performance becomes better and better. The performance enhancement is significant. The reason is that with more antennas at the BS, the ability to cancel the intra-cell interference and noise, i.e., the second and third terms in (4), becomes stronger. Fig. 4 also shows that increasing the SNR cannot effectively improve the SER performance, when the number of BS antennas is not large enough compared with the number of served UTs. Fig. 3 and Fig. 4 demonstrate the effectiveness of the proposed OSPR secure transmission scheme. The SER of massive MIMO eavesdropper is high, while the massive MIMO BS can work properly and the legitimate UTs can recover the original symbols normally. Therefore, the signal transmission stage can be secured by the OSPR scheme to a large extent.

Fig. 5 illustrates the total radiated power of the massive MIMO BS as a function of the number of BS antennas N_b, from simulation results based on (3). We can see that the power consumption decreases significantly as the number of BS antennas increases. The plot demonstrates that with more BS antennas, the corresponding wireless system is able to achieve better energy efficiency, which potentially makes the proposed OSPR approach a green secure transmission scheme.

VI. CONCLUSION

In this paper, we have proposed a novel secure transmission scheme called OSPR to defend against eavesdroppers armed with massive antennas in a single-cell scenario.

The proposed OSPR secure transmission scheme has been introduced step by step. The corresponding security performance has been comprehensively investigated under certain assumptions. Practical simulation results with finite alphabet QPSK inputs have been provided to further corroborate the effectiveness of the proposed scheme. We have shown that as long as the BS is equipped with a sufficient number of antennas, the powerful massive MIMO eavesdropper will not be able to recover most of the original symbols (i.e., the SER is high), even if it has an infinite number of antennas, while the legitimate UTs are able to correctly recover the original symbols. Thus the security performance of the system is guaranteed to a large extent. We have also shown that the proposed OSPR scheme does not affect the high energy efficiency of the massive MIMO BS, and it involves no jamming like approach which is power consuming. This makes the proposed OSPR scheme a good candidate for green and secure transmissions.

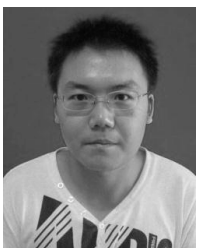
Note that the assumptions made in this paper are optimistic. The effects of imperfect CSI, imperfect channel estimation and multi-cell scenario have not been considered. They are left for future work along with a detailed information theoretic analysis.

REFERENCES

[1] C.-X. Wang *et al.*, "Cellular architecture and key technologies for 5G wireless communication networks," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 122–130, Feb. 2014.
[2] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of base station antennas," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3590–3600, Nov. 2010.
[3] A. Gupta and R. K. Jha, "A survey of 5G network: Architecture and emerging technologies," *IEEE Access*, vol. 3, pp. 1206–1232, 2015.
[4] F. Rusek *et al.*, "Scaling up MIMO: Opportunities and challenges with very large arrays," *IEEE Signal Process. Mag.*, vol. 30, pp. 40–46, Jan. 2013.
[5] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive MIMO for next generation wireless systems," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 186–195, Feb. 2014.
[6] L. Lu, G. Y. Li, A. L. Swindlehurst, A. Ashikhmin, and R. Zhang, "An overview of massive MIMO: Benefits and challenges," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 5, pp. 742–758, Oct. 2014.
[7] F. Boccardi, R. W. Heath, A. Lozano, T. L. Marzetta, and P. Popovski, "Five disruptive technology directions for 5G," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 74–80, Feb. 2014.
[8] H. Q. Ngo, E. G. Larsson, and T. L. Marzetta, "Energy and spectral efficiency of very large multiuser MIMO systems," *IEEE Trans. Commun.*, vol. 61, no. 4, pp. 1436–1449, Apr. 2013.
[9] H. Yang and T. L. Marzetta, "Performance of conjugate and zero-forcing beamforming in large-scale antenna systems," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 2, pp. 172–179, Feb. 2013.
[10] C. Zhu, V. C. M. Leung, L. Shu, and E. C. H. Ngai, "Green Internet of Things for smart world," *IEEE Access*, vol. 3, pp. 2151–2162, Nov. 2015.
[11] T. L. Marzetta, "Massive MIMO: An introduction," *Bell Labs Tech. J.*, vol. 20, pp. 11–22, Mar. 2015.
[12] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.
[13] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.
[14] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.
[15] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[16] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. PP, no. 99, pp. 1–39, May 2016.
[17] Y. O. Basciftci, C. E. Koksal, and A. Ashikhmin. (Mar. 2016). "Physical layer security in massive MIMO." [Online]. Available: https://arxiv.org/pdf/1505.00396v2
[18] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[19] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, Sep. 2014.
[20] B. Chen *et al.*, "Radiated power scaling factor and its effect on the secrecy performance of multi-user massive MIMO system," in *Proc. ACM MobiHoc MSCC Workshop*, Hangzhou, China, Jun. 2015, pp. 7–12.
[21] B. Chen, C. Zhu, W. Chen, K. Wang, and J. Wei, "Secrecy analysis for forward link multi-user massive MIMO system with MRT precoding," in *Proc. IEEE/CIC Int. Conf. Commun. China AINIS Workshop*, Shenzhen, China, Nov. 2015, pp. 1–6.
[22] J. Zhu and W. Xu, "Securing massive MIMO via power scaling," *IEEE Commun. Lett.*, vol. 20, no. 5, pp. 1014–1017, May 2016.
[23] 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.
[24] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
[25] W. Trappe, "The challenges facing physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, Jun. 2015.

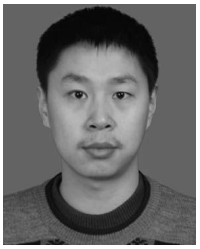
BIN CHEN received the B.Sc. (*summa cum laude*) degree in communication engineering from the National University of Defense Technology (NUDT), Changsha, China, in 2010.

He is currently pursuing the Ph.D. degree with the Department of Communication Engineering, College of Electronic Science and Engineering, NUDT. His research interests include massive MIMO, physical layer security, MIMO precoding, and detection.



CHUNSHENG ZHU (S'12) received the B.E. degree in network engineering from the Dalian University of Technology, China, in 2010, and the M.Sc. degree in computer science from St. Francis Xavier University, Canada, in 2012.

He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, The University of British Columbia, Canada. He has more than 60 papers published or accepted by refereed international journals (e.g., the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, the IEEE TRANSACTIONS ON COMPUTERS, the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, the IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING, the IEEE SYSTEMS JOURNAL) and conferences (e.g., the IEEE Globecom and the IEEE ICC). His current research interests include wireless sensor networks, cloud computing, Internet of Things, social networks, and security.



WEI LI received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees from the National University of Defense Technology (NUDT), Changsha, China, in 2002, 2006, and 2012, respectively, all in communication engineering.

He is currently a Lecturer with the Department of Communication Engineering, School of Electronic Science and Engineering, NUDT. His research interests include wireless communications, wireless network resource allocation, and physical-layer security. He received the Exemplary Reviewer Award from the IEEE COMMUNICATIONS LETTERS in 2014.

JIBO WEI (M'03) received the B.S. and M.S. degrees from the National University of Defense Technology, Changsha, China, in 1989 and 1992, respectively, and the Ph.D. degree from Southeast University, Nanjing, China, in 1998, all in electronic engineering.

He is currently the Director and a Professor with the Department of Communication Engineering, NUDT. His research interests include wireless network protocols and signal processing in communications, particularly in the areas of multiple-input multiple-output, multicarrier transmission, cooperative communications, and cognitive networks.

Dr. Wei serves as an Editor for the *Journal on Communications*. He is a Senior Member of the China Institute of Communications and Electronics and a member of the IEEE Communication and Vehicular Technology Societies.

VICTOR C. M. LEUNG (S'75–M'89–SM'97–F'03) received the B.A.Sc. (Hons.) and Ph.D. degrees in electrical engineering from the University of British Columbia (UBC) in 1977 and 1982, respectively. He is currently a Professor of Electrical and Computer Engineering and holder of the TELUS Mobility Research Chair. He has co-authored more than 900 technical papers in archival journals and refereed conference proceedings, several of which had won best-paper awards. His research is in the areas of wireless networks and mobile systems. He is a fellow of the Royal Society of Canada, the Canadian Academy of Engineering, and the Engineering Institute of Canada. He is serving on the Editorial Boards of the IEEE JSAC-SGCN, the IEEE Wireless Communications Letters, the IEEE Access, and several other journals. He has provided leadership to the technical program committees and organizing committees of numerous international conferences. He was a recipient of the 1977 APEBC Gold Medal, the NSERC Postgraduate Scholarships from 1977 to 1981, a 2012 UBC Killam Research Prize, and an IEEE Vancouver Section Centennial Award.

LAURENCE T. YANG (M'97–SM'15) received the B.E. degree in computer science and technology from Tsinghua University, China, and the Ph.D. degree in computer science from the University of Victoria, Canada.

He is a Professor with the Department of Computer Science, St. Francis Xavier University, Canada. His research interests include parallel and distributed computing, embedded and ubiquitous or pervasive computing, and big data. He has published more than 220 papers in various refereed journals (around 40% on top IEEE/ACM Transactions and Journals, others mostly on Elsevier, Springer, and Wiley Journals). His research has been supported by the National Sciences and Engineering Research Council, and the Canada Foundation for Innovation.