Hybrid Massive MIMO for Secure Transmissions Against Stealthy Eavesdroppers

Xiaohua Li, *Senior Member, IEEE*, Yun Zhang, *Member, IEEE*, and Wednel Cadeau

***Abstract*— Physical-layer secure transmissions require that the legitimate parties Alice and Bob have certain signal advantages over the eavesdropper Eve. Unfortunately, it is still unknown what advantages can be guaranteed realistically in practice. This letter shows that hybrid massive MIMO can be exploited to the advantage of Alice for this purpose. Specifically, it allows Alice to use large antenna arrays that stealthy eavesdroppers cannot afford in many practical situations. To realize this advantage, an efficient transmission scheme is developed with hybrid massive MIMO, random dumb antenna selection, and channel reciprocity-based signal randomization techniques. It can secure the transmission against multiple stealthy eavesdroppers. Transmission security is analyzed assuming eavesdroppers with sufficient side knowledge and channel estimation capabilities. Simulations are conducted to verify the superior performance.**

***Index Terms*— Physical layer security, hybrid massive MIMO, eavesdropping, channel reciprocity.**

I. Introduction

PHYSICAL-LAYER security exploits wireless channel properties to develop security protocols with low overhead [1]. It is attractive especially to systems with a lot of low-cost devices such as internet of things (IoT) and near field communications (NFC) where conventional cryptography may not be very suitable [2].

Physical-layer security requires legitimate parties have certain advantages over adversaries. For the transmission from Alice to Bob against the eavesdropper Eve, secure transmission with positive secrecy rate is possible only if Bob has higher rate or signal-to-noise ratio (SNR) than Eve [2]. As a potential way to meet such a demanding requirement, antenna array secure transmissions have attracted a major research attention during the recent decade [3]–[5].

Unfortunately, it is still unknown what advantages can be guaranteed realistically in practice, even for antenna array transmissions [6]. Eve can adopt sensitive receivers to boost SNR. Eve can use more antennas than Alice as the secrecy rate can be made zero in this case [5].

Recent progress of massive MIMO (multi-input multi-output) has shed a new light to this challenge [7]. In massive MIMO, the antenna array can be fairly large, in both antenna number and form factor. While each transceiver can only have a limited number of RF chains, hybrid massive MIMO allows the limited RF chains to operate a large number of antennas at low cost [8]. These unique properties may be exploited to the advantage of Alice for secure transmissions.

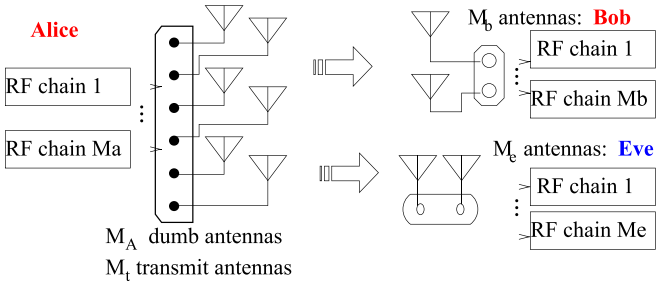

Fig. 1. Alice transmits to Bob in face of eavesdropper Eve.

Based on this idea, this letter develops an efficient secure transmission scheme where Alice uses hybrid massive MIMO and appropriate randomization techniques to operate a large number of dumb antennas. This scheme can overwhelm Eve's eavesdropping capability. It can also be integrated easily into practical massive MIMO systems.

The new scheme is shown secure against multiple *stealthy* eavesdroppers. This is different from many existing schemes that assume known eavesdroppers [5], [7], [10]. Stealthy means that Alice and Bob do not know the channel state information (CSI) of the eavesdroppers. It also means that the eavesdroppers need to hide their existence. As another unique contribution, this letter gives a security analysis under the more realistic assumption that eavesdroppers have sufficient side knowledge and channel estimation capability.

This letter is organized as follows. Section II presents the system model. Section III develops the new secure transmission scheme. Simulations and conclusions are given in Sections IV and V, respectively.

II. System Model

Consider Fig. 1 where Alice communicates with Bob in face of the eavesdropper Eve. The numbers of antennas used by Alice, Bob, and Eve are M_A, M_b, and M_e, respectively. The numbers of their RF chains are M_a, M_b and M_e, respectively. For simplicity, only Alice is assumed to have different antenna and RF chain numbers. The M_A antennas are called *dumb antennas* because they do not have fixed RF chains and are not always in use.

Alice and Bob conduct communications in short sessions. In each session m, Alice needs to transmit N symbol vectors $\mathbf{b}_m(n)$, $n = 0, \cdots, N-1$, securely to Bob. Each $\mathbf{b}_m(n)$ is an M_b dimensional vector. To furnish this, Bob first transmits a training signal to Alice. Then, Alice randomly selects M_t

Manuscript received September 10, 2017; accepted October 3, 2017. Date of publication October 12, 2017; date of current version January 8, 2018. This work was supported by US National Science Foundation under Grant CNS-1443885, Jiangsu Government Scholarship for Overseas Studies and Natural Science Foundation of China No. 61302155. The associate editor coordinating the review of this paper and approving it for publication was N. Tran. *(Corresponding author: Xiaohua Li.)*

X. Li and W. Cadeau are with the Department of Electrical and Computer Engineering, State University of New York at Binghamton, Binghamton, NY 13902 USA (e-mail: xli@binghamton.edu; wcadeau1@binghamton.edu).

Y. Zhang is with the College of Electronic Science and Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China (e-mail: y021001@njupt.edu.cn).

Digital Object Identifier 10.1109/LCOMM.2017.2762319

antennas to receive the signal, where $M_a \leq M_t \leq M_A$, and estimates the $M_t \times M_b$ dimensional channel matrix $\mathbf{H}_m^a$. Next, Alice pre-codes each $\mathbf{b}_m(n)$ to an $M_t \times 1$ dimensional vector $\mathbf{s}_m(n)$ for hybrid massive MIMO transmission.

Bob and Eve's received signals are, respectively,

$$\mathbf{x}_m^b(n) = \mathbf{H}_m^b \mathbf{s}_m(n) + \mathbf{v}_m^b(n), \quad (1)$$

$$\mathbf{x}_m^e(n) = \mathbf{H}_m^e \mathbf{s}_m(n) + \mathbf{v}_m^e(n), \quad (2)$$

where $\mathbf{x}_m^b(n)$ and $\mathbf{x}_m^e(n)$ are M_b and M_e dimensional received signal vectors, $\mathbf{H}_m^b$ and $\mathbf{H}_m^e$ are $M_b \times M_t$ and $M_e \times M_t$ dimensional channel matrices, $\mathbf{v}_m^b(n)$ and $\mathbf{v}_m^e(n)$ are additive white Gaussian noise vectors.

This letter assumes $M_t > M_b$ so Alice has redundant antennas to realize transmission security. No global CSI knowledge is assumed. With channel reciprocity, Alice can estimate its transmission channel $\mathbf{H}_m^b$ from $\mathbf{H}_m^a$. Note that channel reciprocity is a common assumption for both physical-layer security and massive MIMO, and has been demonstrated in many experiments [11]. Note also that although only one eavesdropper is shown in Fig. 1 and equation (2) for simplicity, the new scheme and the security analysis are still valid in case of multiple eavesdroppers.

Hybrid massive MIMO can be used to guarantee $M_A > M_e$ in many practical communication scenarios. First, Alice can easily install a large number of low-cost dumb antennas and randomly select just a small portion to use in each session. In contrast, as a receiver, Eve can generate M_e data streams only, the same number as its limited RF chains. It is costly for Eve to implement M_A RF chains for large M_A.

Second, and more importantly, the stealthy requirement will deter Eve from installing M_A antennas due to the large form factor. Eve can not use a bulky system without being caught in many practical scenarios. For example, for in-door communications inside buildings, offices, stores, etc., legitimate access points can be equipped with a large number of dumb antennas for secure transmissions to IoT and mobile devices. Stealthy eavesdroppers can not use the similar number of antennas in such well-controlled environments. Similar situation happens in NFC such as smart card check-out gates and RFID toll stations. In out-door scenarios such as 5G (Fifth Generation) micro-cells, legitimate base stations can afford large antenna arrays that stealthy eavesdroppers can not.

A challenging issue is cooperative eavesdropping. However, Eve can hardly operate a large number of eavesdropping devices stealthily in the well-controlled environment. The limited in-door or out-door micro-cell space also limits the number of stealthy devices. In addition, Eve can not simply hijack and use conventional IoT or mobile devices. But rather, a large number of special devices with joint baseband processing capabilities are needed. The high cost and high risk of losing stealthy will deter eavesdroppers. Therefore, $M_A > M_e$ or even $M_A \gg M_e$ can be guaranteed realistically in many practical communication scenarios.

III. Secure Transmission Scheme

A. Alice's Transmission to Bob

While secure transmission is possible theoretically when $M_A > M_e$ [5], it is nontrivial to realize it with practical transmission schemes. Most existing schemes assume known eavesdropper CSI which is unrealistic for stealthy eavesdroppers. This letter develops a new scheme based on [3], [12], and [13] because they do not need eavesdropper CSI. Nevertheless, the security of [3], [12], and [13] relies on the ideal assumption that Eve can not estimate its own CSI. In contrast, the new scheme does not need this assumption.

In this new scheme, with the hybrid massive MIMO technology, Alice pre-codes $\mathbf{b}_m(n)$ as

$$\mathbf{s}_m(n) = \mathbf{F}_m(n)\mathbf{E}_m(n)\mathbf{b}_m(n) \triangleq \mathbf{W}_m(n)\mathbf{b}_m(n), \quad (3)$$

where the $M_t \times M_a$ matrix $\mathbf{F}_m(n)$ denotes the analog RF phase shifting network [8], the $M_a \times M_b$ matrix $\mathbf{E}_m(n)$ represents the RF chains and $\mathbf{W}_m(n)$ is the composite pre-coding matrix.

Alice needs to find $\mathbf{W}_m(n)$ so that

$$\mathbf{H}_m^b \mathbf{W}_m(n) = \mathbf{H}_m^b \mathbf{F}_m(n)\mathbf{E}_m(n) = \mathbf{I}_{M_b}, \quad (4)$$

where $\mathbf{I}_{M_b}$ is the $M_b \times M_b$ dimensional identity matrix.

To develop a computationally efficient algorithm to calculate $\mathbf{W}_m(n)$, let Alice select M_b columns from $\mathbf{H}_m^b$ and put them into a square matrix $\mathbf{H}_{m,1}^b$. Then, leaving the rest $M_t - M_b$ columns to the matrix $\mathbf{H}_{m,2}^b$, Alice has $[\mathbf{H}_{m,1}^b, \mathbf{H}_{m,2}^b] = \mathbf{H}_m^b \mathbf{T}_m$, where $\mathbf{T}_m$ is a permutation matrix. Similarly, subdividing $\mathbf{W}_m(n)$ gives

$$\begin{bmatrix} \mathbf{W}_{m,1}(n) \\ \mathbf{W}_{m,2}(n) \end{bmatrix} = \mathbf{T}_m^T \mathbf{W}_m(n), \quad (5)$$

where $(\cdot)^T$ denotes transpose. With these new matrices, the condition (4) can be re-written as

$$\mathbf{H}_{m,1}^b \mathbf{W}_{m,1}(n) + \mathbf{H}_{m,2}^b \mathbf{W}_{m,2}(n) = \mathbf{I}_{M_b}. \quad (6)$$

As a result, to calculate $\mathbf{W}_m(n)$, Alice just needs to generate randomly the matrix $\mathbf{W}_{m,2}(n)$ and calculate

$$\mathbf{W}_{m,1}(n) = \left(\mathbf{H}_{m,1}^b\right)^{-1} \left(\mathbf{I}_{M_b} - \mathbf{H}_{m,2}^b \mathbf{W}_{m,2}(n)\right). \quad (7)$$

With this transmission scheme, Bob's signal is simplified to

$$\mathbf{x}_m^b(n) = \mathbf{b}_m(n) + \mathbf{v}_m^b(n), \quad (8)$$

from which the symbol vector $\mathbf{b}_m(n)$ can be easily detected. The SNR is

$$\gamma_b = \frac{\mathrm{tr}\{E[\mathbf{b}_m(n)\mathbf{b}_m^H(n)]\}}{\mathrm{tr}\{E[\mathbf{v}_m^b(n)(\mathbf{v}_m^b(n))^H]\}} = \frac{\sigma_b^2}{\sigma_{vb}^2}, \quad (9)$$

where $\mathrm{tr}\{\cdot\}$ denotes matrix trace, $E[\cdot]$ denotes expectation, $(\cdot)^H$ denotes Hermitian, σ_b^2 is the symbol variance, and σ_{vb}^2 is Bob's noise variance.

Considering that $\mathbf{W}_{m,2}(n)$ is arbitrary, in order to strengthen security, Alice can make $\mathbf{W}_{m,2}(n)\mathbf{b}_m(n)$ to have Gaussian distribution with zero mean and a secret covariance matrix $\mathbf{C}_m^{wb}$. This can be conducted as follows. Based on (3)(5), Alice can get $\mathbf{W}_{m,2}(n)\mathbf{b}_m(n) = \mathbf{F}_{m,2}(n)\mathbf{E}_m(n)\mathbf{b}_m(n)$, where $\mathbf{F}_{m,2}(n)$ is the $(M_t - M_b) \times M_a$ submatrix of $\mathbf{F}_m(n)$. Therefore, for each $\mathbf{b}_m(n)$, Alice first determines $\mathbf{F}_{m,2}(n)$ and then samples $\mathbf{E}_m(n)$ from appropriate Gaussian distributions to make $\mathbf{F}_{m,2}(n)\mathbf{E}_m(n)\mathbf{b}_m(n)$ having the desired Gaussian distribution.

Furthermore, from (5) and (7), one can see that

$$\mathbf{W}_m(n) = \mathbf{A}_m \mathbf{W}_{m,2}(n) + \mathbf{B}_m, \tag{10}$$

where

$$\mathbf{A}_m = \mathbf{T}_m \begin{bmatrix} -\left(\mathbf{H}^b_{m,1}\right)^{-1} \mathbf{H}^b_{m,2} \\ \mathbf{I}_{M_t - M_b} \end{bmatrix}, \quad \mathbf{B}_m = \mathbf{T}_m \begin{bmatrix} \left(\mathbf{H}^b_{m,1}\right)^{-1} \\ \mathbf{0} \end{bmatrix}. \tag{11}$$

It can also be readily seen that $\mathbf{s}_m(n)$ has Gaussian distribution with zero mean and covariance matrix

$$\mathbf{R}^{wb}_m \triangleq E[\mathbf{s}_m(n)\mathbf{s}^H_m(n)] = \mathbf{A}_m \mathbf{C}^{wb}_m \mathbf{A}^H_m + \sigma^2_b \mathbf{B}_m \mathbf{B}^H_m. \tag{12}$$

Alice can make both $\mathbf{T}_m$ and $\mathbf{C}^{wb}_m$ time-varying and secret to enhance security.

The average transmission power during M sessions is $\frac{1}{M}\sum_{m=0}^{M-1} \mathrm{tr}\{\mathbf{R}^{wb}_m\}$. Alice can adjust the transmission power through $\mathbf{C}^{wb}_m$. Higher transmission power degrades the SNR of Eve, which means Alice can use it to adjust the tradeoff between power efficiency and security [12].

To mitigate the potential numerical problems in calculating $(\mathbf{H}^b_{m,1})^{-1}$, if M_b is not big, Alice can do an exhaustive search to find some $\mathbf{H}^b_{m,1}$ with good conditions to use. Otherwise, the following efficient regularization technique can be used, i.e.,

$$\mathbf{W}_{m,1}(n) = \left(\mathbf{H}^b_{m,1} + \beta \mathbf{I}_{M_b}\right)^{-1} \left(\mathbf{I}_{M_b} - \mathbf{H}^b_{m,2}\mathbf{W}_{m,2}(n)\right), \tag{13}$$

where β is the regularization factor. In this case, Bob's received signal becomes

$$\mathbf{x}^b_m(n) = \mathbf{b}_m(n) + \beta \mathbf{W}_{m,1}(n)\mathbf{b}_m(n) + \mathbf{v}^b_m(n). \tag{14}$$

Since $\mathbf{W}_{m,1}(n)$ is random, Bob has to treat $\mathbf{W}_{m,1}(n)\mathbf{b}_m(n)$ as noise. Large β saves transmission power but reduces Bob's SNR. Alice can choose β to realize the appropriate tradeoff between power efficiency and Bob's receiving performance.

This scheme is computationally efficient. The major complexity comes from calculating $(\mathbf{H}^b_{m,1})^{-1}$, which has complexity $O(M_b^3)$. In practice, we can make M_b small or even $M_b = 1$ if data rate is not the primary concern. This compares favorably to other schemes such as [4], [5], and [10] whose complexity is $O(M_t^2 M_b)$. This scheme is especially suitable for IoT, NFC and 5G systems with a lot of low-cost devices.

B. Analysis of Passive Eavesdropping

The secrecy rate can be derived similarly as [12] and [13]. Nevertheless, the new scheme does not need the ideal assumption made in [12] and [13], i.e., Eve can not estimate its CSI $\mathbf{H}^e_m$. Its security can be analyzed by considering specifically Eve's side knowledge and strong channel estimation capability.

Eve may get some side knowledge about $\mathbf{b}_m(n)$ and $\mathbf{s}_m(n)$ from pilots, context, etc. Such knowledge not only leaves backdoors for Eve to estimate $\mathbf{H}^e_m$, but also reduces or can even completely nullify the secrecy rate. If Eve knows sufficient number of symbols $b_{m,n,d}$ of $\mathbf{b}_m(n)$, where $0 \le d \le M_b - 1$, an equalizer can be estimated as

$$\mathbf{g}_m = \arg\min_{\mathbf{g}} E[|b_{m,n,d} - \mathbf{g}^H \mathbf{x}^e_m(n)|^2]. \tag{15}$$

It can be shown that the optimal solution to (15) is

$$\mathbf{g}^H_m = E[b_{m,n,d}(\mathbf{x}^e_m(n))^H]\left(E[\mathbf{x}^e_m(n)(\mathbf{x}^e_m(n))^H]\right)^+ \xrightarrow{\text{converge to}} \mathbf{e}^T_d \mathbf{H}^b_m (\mathbf{H}^e_m)^+, \tag{16}$$

where $(\cdot)^+$ denotes matrix pseudo-inverse, and $\mathbf{e}_d$ is the unit vector with only one non-zero element which is 1 in the dth entry. It is easy to see that Eve can use $\mathbf{g}^H_m \mathbf{x}^e_m(n)$ to detect the transmitted symbols if $(\mathbf{H}^e_m)^+ \mathbf{H}^e_m \approx \mathbf{I}$. Note that Eve does not need to know Bob's channel $\mathbf{H}^b_m$.

This attack is effective against almost all physical-layer secure transmission schemes. The primary reason is that the condition (4) has to be satisfied in order for Bob to detect $\mathbf{b}_m(n)$ from the randomized signals. There are two ways to mitigate this attack: 1) ensure $M_t > M_e$ so that $(\mathbf{H}^e_m)^+ \mathbf{H}^e_m$ is far away from $\mathbf{I}$; and 2) reduce N and scramble $\mathbf{b}_m(n)$ so that Eve can not get enough known symbols $b_{m,n,d}$. The new scheme is designed to exploit both ways to guarantee security. The random antenna selection also plays an important role. Note that Bob does not need many pilot symbols thanks to the simplified signal model (8).

Without sufficient amount of known symbols in one session, Eve may consider all the sessions to accumulate known symbols. This means Eve needs to work on the extended model

$$\mathbf{x}^e_m(n) = \tilde{\mathbf{H}}^e \tilde{\mathbf{s}}_m(n) + \mathbf{v}^e_m(n), \tag{17}$$

where the $M_e \times M_A$ matrix $\tilde{\mathbf{H}}^e$ includes the channel coefficients from all the M_A transmit antennas to M_e receiving antennas, and the elements of the $M_A \times 1$ dimensional signal vector $\tilde{\mathbf{s}}_m(n)$ are either zero or equal to those of $\mathbf{s}_m(n)$. In this case, thanks to Alice's random antenna selection, it is impossible for Eve to combine all the known symbols together to estimate $\tilde{\mathbf{H}}^e$.

Consider the extreme case that Eve knows $\tilde{\mathbf{H}}^e$. Because M_e is much less than M_A, Eve can not estimate $\tilde{\mathbf{s}}_m(n)$ reliably through inverting $\tilde{\mathbf{H}}^e$. However, because there are only M_t non-zero elements in $\tilde{\mathbf{s}}_m(n)$, Eve can try compressive sensing to estimate $\tilde{\mathbf{s}}_m(n)$. Compressive sensing requires that

$$M_e > c M_t \log M_A \tag{18}$$

with some constant c. Obviously, Alice can use a sufficiently large M_t to mitigate this attack.

Consider another even more extreme case that Eve knows both $\tilde{\mathbf{H}}^e$ and a sufficient number of elements of $\tilde{\mathbf{s}}_m(n)$. Because of the increased sparsity, Eve may be able to estimate $\tilde{\mathbf{s}}(n)$ in this case. Then, Eve can extract $\mathbf{s}_m(n)$ from $\tilde{\mathbf{s}}(n)$ and try to estimate $\mathbf{b}_m(n)$ from

$$\mathbf{s}_m(n) = \mathbf{W}_m(n)\mathbf{b}_m(n) + \tilde{\mathbf{v}}^e_m(n), \tag{19}$$

where $\tilde{\mathbf{v}}^e_m(n)$ is the estimation error. In this new scheme, the randomized pre-coding is strengthened specifically to mitigate this attack. Because $\mathbf{W}_m(n)\mathbf{b}_m(n)$ has Gaussian distribution, Eve has to find both $\mathbf{W}_m(n)$ and $\mathbf{b}_m(n)$ by solving (12). This is infeasible because (12) is highly nonlinear and has a secret time-varying matrix $\mathbf{C}^{wb}_m$.

Finally, Eve may use exhaustive search to assist eavesdropping. First, instead of relying on (15), Eve may test all possible $\mathbf{g}_m$ exhaustively. Since Alice can increase M_t at low

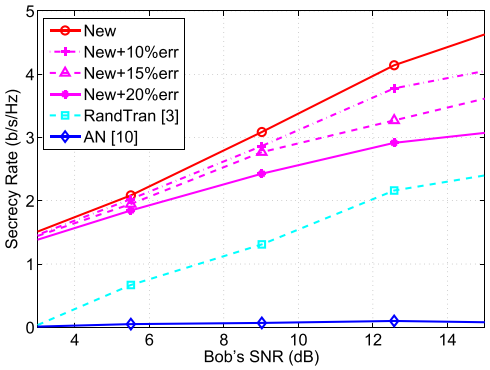

Fig. 2. Secrecy rate as function of Bob's SNR. **New**, **New+10%err**, **New+15%err**, **New+20%err**: New scheme under 0, 10%, 15%, 20% channel reciprocity errors. **RandTran [3]**: scheme of [3]. **AN [10]**: scheme of [10].

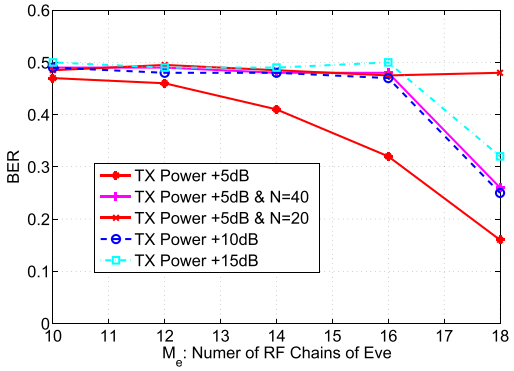

Fig. 3. Eve's BER as function of M_e, evaluated when Alice used various transmission powers and session lengths N.

cost, this attack can be easily made computationally infeasible. Even a binary quantization of the $\mathbf{g}_m$ elements leads to $O(2^{M_t})$ complexity. Second, to combat Alice's random antenna selection, Eve may search exhaustively over all possible antenna selections. Nevertheless, for each possible antenna selection, Eve still needs to solve either (16) or (19), which has been shown as infeasible.

Therefore, the new scheme can guarantee transmission security, and this is also true in case of multiple eavesdroppers.

IV. Simulations

Simulations were conducted to evaluate the new secure transmission scheme and to compare it with the schemes in [3] and [10]. Secrecy rate and bit error rate (BER) were used as performance metrics. Parameters were set as $M_A = 256$, $M_t = 20$, $M_a = 10$, $M_b = 4$, $M = 100$ and $N = 1000$. Each secrecy rate or BER value was obtained as the average of 100 runs of the simulations. Channels were generated randomly. There were three stealthy eavesdroppers, each assumed to have noise-free signals and to apply all the N transmitted symbol vectors as pilots for channel/equalizer estimation.

In the first experiment, Alice's transmission power was fixed and Bob's noise power was adjusted to generate various SNRs. Each eavesdropper used $M_e = 8$ RF chains. Imperfect channel reciprocity was also simulated, where $\mathbf{H}_m^b = (\mathbf{H}_m^a)^T + \Delta\mathbf{H}_m$ and the percentage of channel reciprocity error was defined as $\|\Delta\mathbf{H}_m\|/\|\mathbf{H}_m^b\|$. Simulation results are shown in Fig. 2. It can be seen that the new scheme was able to achieve high secrecy rates even in case of significant reciprocity errors. In comparison, the scheme of [3] had much lower secrecy rates because it did not use hybrid massive MIMO and because Eve was able to estimate CSI to some extent. The scheme of [10] failed because the existence of more than one stealthy eavesdroppers violated its ideal assumptions.

In the second experiment, Eve's RF chain number changed between $M_e = 10$ and $M_e = 18$. In this case, to enhance security, Alice's transmission power was increased by 5dB, 10dB and 15dB over the first experiment. Session length was reduced to $N = 20$ and $N = 40$ to degrade Eve's equalization capability. Results in Fig. 3 show that Eve suffered from a high BER and thus failed eavesdropping.

V. Conclusions

This letter develops a practical physical-layer secure transmission scheme by using hybrid massive MIMO with a large number of dumb antennas to overwhelm eavesdroppers. With random antenna selection and signal randomization, this scheme is shown secure against multiple stealthy eavesdroppers. This scheme can be used to realize physical-layer security in many practical wireless communication scenarios.

References

[1] 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, 3rd Quart., 2014.

[2] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. Nat. Acad. Sci. USA*, vol. 114, no. 1, pp. 19–26, Jan. 2017.

[3] X. Li, J. Hwu, and E. P. Ratazzi, "Using antenna array redundancy and channel diversity for secure wireless transmissions," *J. Commun.*, vol. 2, no. 3, pp. 24–32, May 2007.

[4] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[5] 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.

[6] W. Trappe, "The challenges facing physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, Jun. 2015.

[7] 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.

[8] A. Liu and V. Lau, "Phase only RF precoding for massive MIMO systems with limited RF chains," *IEEE Trans. Signal Process.*, vol. 62, no. 17, pp. 4505–4515, Sep. 2014.

[9] 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, Jun. 2016.

[10] J. Zhu, W. Xu, and N. Wang, "Secure massive MIMO systems with limited RF chains," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 5455–5460, Jun. 2017.

[11] J. Vieira, F. Rusek, O. Edfors, S. Malkowsky, L. Liu, and F. Tufvesson, "Reciprocity calibration for massive MIMO: Proposal, modeling, and validation," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 3042–3056, May 2017.

[12] Q. Li, H. Song, and K. Huang, "Achieving secure transmission with equivalent multiplicative noise in MISO wiretap channels," *IEEE Commun. Lett.*, vol. 17, no. 5, pp. 892–895, May 2013.

[13] H.-M. Wang, T. Zheng, and X.-G. Xia, "Secure MISO wiretap channels with multiantenna passive eavesdropper: Artificial noise vs. artificial fast fading," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 94–106, Jan. 2015.