# Asymptotic Studies for the Impact of Antenna Selection on Secure Two-Way Relaying Communications with Artificial Noise

Zhiguo Ding, *Member, IEEE*, Zheng Ma, *Member, IEEE*, and Pingzhi Fan, *Member, IEEE*

***Abstract*—In this paper, we consider a two-way relaying scenario with one pair of source nodes, one relay and one eavesdropper. All nodes are equipped with multiple antennas, and we study the impact of antenna selection on such a secure communication scenario. Three transmission schemes with different tradeoff between secure performance and complexity are investigated respectively. Particularly, when antenna selection is implemented at the relay and no artificial noise is introduced, the condition to realize secure transmissions is established. Then by allowing the sources to inject artificial noise into the system, the secure performance is evaluated by focusing on different eavesdropping strategies. When both the relay and the sources send artificial noise, a low complexity strategy of antenna selection is proposed to efficiently utilize the antennas at the sources and the relay. The developed asymptotic results demonstrate that, by adding more artificial noise and performing joint antenna selection, a better secure performance, such as a larger secrecy rate and a lower outage probability, can be realized at a price of imposing more complexity on the system. Simulation results are also provided to demonstrate the accuracy of the developed analytical results.**

***Index Terms*—Physical layer security, antenna selection, cooperative relaying, diversity gains.**

## I. Introduction

PASSIVE eavesdropping has been recognized as an inherent and challenging issue in wireless communications due to the broadcasting nature of radio propagation. Conventionally, wireless security has been realized by relying on protocols and algorithms operating at the higher layers of the communication systems. Recent progress in physical layer security sheds light on more computationally efficient methods to achieve secure transmissions over the wireless medium. The concept of physical layer security was originally developed for the Wyner wiretap model in [1] and recently extended to general wireless communication scenarios [2]. Fundamental limits of physical layer security, such as the secrecy capacity and achievable secrecy rates, have been developed for various communication scenarios [3]–[6]. (See [7] and [8] for reviews of progress in this area.)

Existing studies for the classical wiretap channel with one source-destination pair and one eavesdropper have demonstrated that a secrecy rate larger than zero cannot always be guaranteed. Therefore, users' targeted quality of service cannot be met, which limits the importance of physical layer security in practice. The use of cooperative jamming and relay chatting can efficiently degrade the reception reliability at the eavesdropper and improve the achievable secrecy rates at legitimate receivers, where the works in [9]–[11] consider scenarios with single-antenna nodes. Exploiting multiple antennas and multiple-nodes cooperation to improve the physical layer secure transmissions has recently attracted a lot of interests. The use of multiple-antenna nodes in multi-user secrecy scenarios has been studied in [12] and [13], where various strategies to design precoding and introduce artificial noise have been proposed. A typical approach for the use of artificial noise is to put artificial noise into the null space of the channel matrix related to the legitimate receiver, so introducing such noise can only damage the eavesdropping capability, but not the reliability at the legitimate receiver. Game theoretic approaches have been developed in [14] by considering the interaction between the jammer and legitimate users.

In this paper, we focus on the two-way relaying communication scenario with one pair of source nodes, one relay and one eavesdropper, where all nodes are equipped with multiple antennas. The applications of such two-way relaying channels include the scenario in which two users wish to establish private key exchanging with the help of a trusted relay. Recall that the use of multiple antennas typically requires multiple RF chains which consist of amplifiers, AD/DA converters, etc., and leads to high cost and complexity. Such a drawback motivates the approaches of antenna selection [15], [16]. As discussed in [17], performing antenna selection at the receiver can be viewed as a direct extension from traditional RAKE receivers, and transmit antenna selection can be realized by

Manuscript received July 12, 2013; revised September 20 and November 22, 2013; accepted January 9, 2014. The associate editor coordinating the review of this paper and approving it for publication was D. Niyato.

Z. Ding is with School of Electrical, Electronic, and Computer Engineering Newcastle University, NE1 7RU, UK (e-mail: z.ding@newcastle.ac.uk).

Z. Ma and P. Fan are with the Key Lab of Information Coding and Transmission, Southwest Jiaotong University, Chengdu, 610031, China. Z. Ma is also with the National Mobile Communications Research Laboratory, Southeast University, Nanjing, 210096, China (e-mail: pingzhifan@gmail.com, zma@home.swjtu.edu.cn).

Z. Ding's work was supported by the UK EPSRC under grant number EP/I037423/1.

The work of Z. Ma and P. Z. Fan was supported by the National Basic Research Program of China (973 Program) (Grant No. 2012CB316100), National Natural Science Foundation of China (60872013), Fok Ying Tung Education Foundation (Grant No. 122001), Program for New Century Excellent Talents in University (Grant No. NECT-10-0705), China Scholarship Council Funding, 111 Project Foundation (Grant No. 111-2-14). Open Research Fund of National Mobile Communications Research Laboratory, Southeast University (Grant No. 2011D16), Key Grant Project of Chinese Ministry of Education (Grant No. 311031100), Young Innovative Research Team of Sichuan Province (Grant No. 2011JTD0007).

Digital Object Identifier 10.1109/TWC.2014.022714131252

either utilizing the feedback from the receiver or acquiring channel state information at the transmitter. The application of antenna selection to conventional two-way relaying scenarios without eavesdroppers can be found in [18], [19], and the impact of antenna selection on the performance of secure transmissions in wiretap channels has been investigated in [20].

In this paper, three transmission schemes with different tradeoff between secure performance and complexity are investigated respectively. We first focus on the scenario when the source nodes perform beamforming and relay selection is implemented only at the relay. Without adding any artificial noise, we carry out the analytic studies for the performance achieved by the proposed scheme. Particularly the metric used in this paper is based on the probability to have a non zero secrecy rate, i.e. $P(\mathcal{I}_s > 0)$, where $\mathcal{I}_s$ denotes the achievable secrecy rate. Note that this probability for the event to achieve a secrecy rate larger than zero can be viewed as a special case of the conventional outage probability by setting the targeted data rate as zero. For example, the conventional definition of the outage probability is $P(\mathcal{I}_s < R)$, where $R$ is the targeted data rate. By setting $R = 0$, the probability to have a non zero secrecy rate can be straightforwardly obtained from the conventional outage probability. Specifically by fixing the number of the antennas at the relay, the secrecy rate becomes a constant at high SNR, which means that the studied probability for having zero secrecy rates never goes to zero, no matter how large the SNR is. However, when there is a large number of antennas at the relay, the extreme value theory can be utilized to develop asymptotic results which show that the studied probability is decreasing to zero, due to the fact that antenna selection at the relay can help the legitimate receivers, but not the eavesdropper.

Then we focus on the scenario with more system complexity in which artificial noise is introduced partially. Particularly the relay still uses one antenna for transmitting and receiving, but the sources will perform beamforming as well as cooperative jamming, which preserves simple data processing at the relay but increases the complexity at the sources. Again the probability to achieve a secrecy rate larger than zero is used as the criterion for the performance evaluation. The developed asymptotic results show an interesting phenomenon that injecting a certain amount of interference into the system can degrade the reception reliability of the eavesdropper and improve the achievable secrecy rates. However, there is a threshold for the amount of interference, above which further injecting interference will not cause much performance degradation to the eavesdropper, since the relay transmission is not protected and becomes the weakest link in such a secure communication system.

Motivated by such a phenomenon, to fully suppress the eavesdropping capability, artificial noise needs to be added to both source and relay transmissions. In addition, the criterion of antenna selection will also need to be tailored for such a secure transmission strategy, as shown in the third part of this paper. Compared to the previous two scenarios, extra computational complexity is required and all antennas at the relay need to be used for cooperative jamming, but a much better secure performance can be achieved. The developed asymptotic results demonstrate that the outage probability for any targeted secrecy data rate is a decreasing function of the SNR, and the achievable diversity gain is the product of the number of antennas at the sources and the relay. It is worth pointing out that the diversity gain achieved by the schemes for the previous scenarios is zero, and therefore the use of the third scheme can significantly improve the reliability of secure transmissions, at a price of more system complexity.

## II. Secure Transmissions Without Artificial Noise

Consider a physical layer security communication scenario where one pair of source nodes wish to exchange information via a relay, with the existence of an eavesdropper. The relay is equipped with $N$ antennas and all the other nodes have $M$ antennas[1]. All the wireless channels and receiver noise are assumed to be identically and independent complex Gaussian distributed with zero mean and unit variance. Time division duplexing is used in order to exploit the reciprocal property of the incoming and outgoing channels. It is assume that the eavesdropper has access to the global channel state information (CSI); however, the legitimate nodes only know the CSI not related to the eavesdropper. Such a CSI assumption is realistic since the eavesdropper's CSI will not be revealed to the legitimate transceivers in practical communication systems. It is worth pointing out that the considered scenario is more challenging compared to the case that the legitimate nodes have some priori information about the eavesdropper's channels. For example, if global CSI is known to all nodes, there is no need to generate artificial noise, and perfect secrecy can be realized by ensuring that the eavesdropper is located inside of the null space of the source precoders. Prior to transmission, the $i^*$-th antenna at the relay is selected based on the following criterion:

$$\begin{aligned}\min\{|\mathbf{h}_{i^*}|^2, |\mathbf{g}_{i^*}|^2\} \\ = \max\left\{\min\{|\mathbf{h}_i|^2, |\mathbf{g}_i|^2\}, 1 \leq i \leq N\right\},\end{aligned} \quad (1)$$

where $|\cdot|$ denotes the norm, $\mathbf{h}_i$ is the $M \times 1$ channel vector from the first source to the $i$-th antenna at the relay, and $\mathbf{g}_i$ is similarly defined for the channel for the second source. Note that the max-min criterion in (1) has been commonly used for relay selection in cooperative networks as an alternative to the one based on the harmonic mean, as can be found in [21], [22]. The reason to use such a criterion is to select a relay which has a balanced connection to both source nodes.

During the first time slot, each source sends $\mathbf{x}_i = \mathbf{p}_i s_i$, where $s_i$ is the information bearing message, and the beamforming vectors are $\mathbf{p}_1 = \frac{\mathbf{h}_{i^*}}{\sqrt{|\mathbf{h}_{i^*}|^2}}$ and $\mathbf{p}_2 = \frac{\mathbf{g}_{i^*}}{\sqrt{|\mathbf{g}_{i^*}|^2}}$. At the end of the first time slot, the $i^*$-th antenna of the relay receives

$$y_R = \mathbf{h}_{i^*}^H \mathbf{x}_1 + \mathbf{g}_{i^*}^H \mathbf{x}_2 + n_R = |\mathbf{h}_{i^*}| s_1 + |\mathbf{g}_{i^*}| s_2 + n_R,$$

[1] The proposed transmissions schemes in Sections II-IV, such as the source beamforming vectors, the jamming precoding matrix and the antenna selection algorithms, can be extended to the asymmetrical scenario, in which sources have different number of antennas. However, the use of the symmetrical setting can simplify the development of the analytical results. In addition, this symmetrical setting is reasonable in the context of two-way communications. Therefore in this paper, we only consider that the two sources have the same number of antennas.

where $n_R$ is the additive noise at the relay. During the second time slot, the relay transmits $x_R = \beta(|\mathbf{h}_{i^*}|s_1 + |\mathbf{g}_{i^*}|s_2 + n_R)$, where $\beta$ is the power normalization factor, i.e. $\beta = \frac{1}{\sqrt{|\mathbf{h}_{i^*}|^2+|\mathbf{g}_{i^*}|^2+\frac{1}{\rho}}}$, where $\rho$ is the transmit SNR. Consequently the first source observes

$$\mathbf{y}_1 \quad = \quad \mathbf{h}_{i^*}\frac{(|\mathbf{h}_{i^*}|s_1 + |\mathbf{g}_{i^*}|s_2 + n_R)}{\sqrt{|\mathbf{h}_{i^*}|^2 + |\mathbf{g}_{i^*}|^2 + \frac{1}{\rho}}} + n_1, \qquad (2)$$

where $n_1$ denotes the noise at the first source. After removing the self-interference, the maximum ratio combining strategy (MRC) is applied at the sources, i.e., detection is based on $\frac{\mathbf{h}_{i^*}^H}{\sqrt{|\mathbf{h}_{i^*}|^2+|\mathbf{g}_{i^*}|^2+\frac{1}{\rho}}}\mathbf{y}_1$, and the SNR at the two sources is given by

$$\begin{aligned} SNR_1 &= \frac{\rho|\mathbf{h}_{i^*}|^2|\mathbf{g}_{i^*}|^2}{2|\mathbf{h}_{i^*}|^2 + |\mathbf{g}_{i^*}|^2 + \frac{1}{\rho}}, \qquad (3)\\ SNR_2 &= \frac{\rho|\mathbf{h}_{i^*}|^2|\mathbf{g}_{i^*}|^2}{|\mathbf{h}_{i^*}|^2 + 2|\mathbf{g}_{i^*}|^2 + \frac{1}{\rho}}. \end{aligned}$$

On the other hand, over two time slots, the eavesdropper observes

$$\mathbf{y}_E = \underbrace{\begin{bmatrix} \mathbf{H}_{E1}^H\mathbf{p}_1 & \mathbf{H}_{E2}^H\mathbf{p}_2 \\ \beta|\mathbf{h}_{i^*}|\mathbf{h}_{ER} & \beta|\mathbf{g}_{i^*}|\mathbf{h}_{ER} \end{bmatrix}}_{\mathbf{H}_E} \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} + \begin{bmatrix} \mathbf{n}_{E1} \\ \mathbf{n}_{E2} + \beta\mathbf{h}_{ER}n_R \end{bmatrix},$$

where $\mathbf{H}_{E1}^H$ is the $M \times M$ channel matrix between the first source and the eavesdropper, $\mathbf{H}_{E2}^H$ and $\mathbf{h}_{ER}$ are defined similarly. Therefore an achievable secrecy rate from the first source to the second source is

$$\begin{aligned} \mathcal{I}_{1\to 2} = \Bigg[\log\left(1 + \rho\frac{|\mathbf{h}_{i^*}|^2|\mathbf{g}_{i^*}|^2}{|\mathbf{h}_{i^*}|^2 + 2|\mathbf{g}_{i^*}|^2 + \frac{1}{\rho}}\right) - \log\Bigg(1 \\ +\rho\ \frac{1}{\left[(\mathbf{H}_E^H\mathbf{H}_E)^{-1}\mathbf{H}_E^H\mathbf{C}_n\mathbf{H}_E(\mathbf{H}_E^H\mathbf{H}_E)^{-1}\right]_{1,1}}\Bigg)\Bigg]^+, \qquad (4) \end{aligned}$$

where $[\mathbf{A}]_{i,j}$ denotes an element of $\mathbf{A}$ at its $i$-th row and $j$-th column, $[a]^+ = \max\{a, 0\}$, $\mathbf{H}_E$ denotes the channel matrix at the eavesdropper , and the noise covariance matrix is

$$\mathbf{C}_n = \begin{bmatrix} \mathbf{I}_M & \mathbf{0}_M \\ \mathbf{0}_M & \mathbf{I}_M + \beta^2\mathbf{h}_{ER}\mathbf{h}_{ER}^H \end{bmatrix}.$$

It is worth pointing out that the achievable secrecy rate in (4) is obtained by assuming that simple linear methods, such as zero forcing approaches, have been used here for the detection at the eavesdropper, given the fact that the eavesdropper can separate the mixture. For more complicated scenarios, sophisticated criteria, such as the capacity region of multiple access channels, will be used as shown in the next section. To obtain the explicit results about the secrecy rate, we first provide the following proposition which will also be used in the next section.

*Proposition 1:* Consider four $M \times 1$ identically and independently complex Gaussian distributed vectors, $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ and $\mathbf{d}$. Construct the following two matrices

$$\mathbf{A} = \begin{bmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{d} \end{bmatrix}, \quad \mathbf{B} = \begin{bmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{c} & \mathbf{c} \end{bmatrix}.$$

The following property holds

$$P\left(\frac{1}{[\mathbf{A}^H\mathbf{A}]_{i,i}^{-1}} > \frac{1}{[\mathbf{B}^H\mathbf{B}]_{i,i}^{-1}}\right) \to 1, \qquad (5)$$

when $M \to \infty$.

*Proof:* See Appendix. ■

It is worth pointing out that the proposition as well as the following lemma are obtained with the condition $M \to \infty$, but these results also hold for a moderate $M$ as demonstrated in Section IV.

In this section, the criterion for the performance evaluation is based on the probability to achieve a secrecy rate larger than zero. To evaluate this probability, we first apply the above proposition to obtain a lower bound for the achievable secrecy rate which is a simple function of $\min\{|\mathbf{h}_{i^*}|^2, |\mathbf{g}_{i^*}|^2\}$. However, the complicated density function of $\min\{|\mathbf{h}_{i^*}|^2, |\mathbf{g}_{i^*}|^2\}$ makes it difficult to carry out asymptotic studies for the addressed probability. Instead, the extreme value theory will be applied as shown in the proof of the following lemma.

**Lemma** *1:* For $M \to \infty$ and $\frac{N}{M} \to \infty$, the probability to have zero secrecy rates is zero, i.e. $P(\mathcal{I}_{1\to 2} > 0) \to 1$.

*Proof:* See Appendix. ■

The lemma requires the assumptions, $M \to \infty$ and $\frac{N}{M} \to \infty$. The assumption of $M \to \infty$ is required for the application of Proposition 1 in order to obtain the lower bound of the secrecy rate. The step to apply extreme order statistics requires $N \to \infty$ with a fixed $M$. Therefore together we need the two assumptions, $M \to \infty$ and $\frac{N}{M} \to \infty$. For the addressed physical layer security scenario, the assumption $\frac{N}{M} \to \infty$ is very helpful to improve the system security. For example, if $N = M$ and $M \to \infty$, it means that the eavesdropper has the same capability as the relay, which leads to a high security risk. On the other hand, if $N >> M$, we can make it sure that the data rate supported by the relay channels is much larger than that of the eavesdropper, which yields a higher secrecy rate. The lemma is matched with our expectation since the use of more relay antennas can benefit the reception reliability at the legitimate receiver, but the achievable secrecy rate is quite small for a moderate number of source and relay antennas, as shown later by the simulation results. The reason is that the eavesdropping capability is quite strong since the eavesdropper is equipped with multiple antennas. In the next section, artificial noise will be transmitted by the sources, which is analog to reduce the number of the eavesdropper's antennas.

## III. Secure Transmission with Partially Added Artificial Interference

In this section, we will study the performance of the strategy by only adding artificial noise during the first time slot and keep the second time slot exactly the same as before. The rational behind such a strategy is that the signal processing complexity at the relay can still be kept the minimum. Compared to the previous section, the extra complexity comes from the fact that during the first time slot, the sources need to perform beamforming and send artificial noise simultaneously. Specifically, during the first time slot, each source sends the following

$$\mathbf{x}_i = \mathbf{p}_i s_i + \mathbf{P}_i \mathbf{w}_i, \tag{6}$$

where the $M \times x$ precoding matrix $\mathbf{P}_1$ contains $x$ eigenvectors of the orthogonal projection matrix $\left(\mathbf{I}_M - \frac{\mathbf{h}_{i^*}\mathbf{h}_{i^*}^H}{\mathbf{h}_{i^*}^H\mathbf{h}_{i^*}}\right)$ corresponding to its $x$ non-zero eigenvalues, the precoding matrix $\mathbf{P}_2$ is designed similarly, and the parameter $x$ defines how much interference will be injected into the system. Note that $x \leq (M-1)$ due to the fact that the rank of the orthogonal projection matrices is $(M-1)$. Such precoding matrices ensure that the relay does not observe any interference signals, and also simplify the analysis, where the effective channels at the eavesdropper become independent, as shown later.

At the end of the first time slot, at the $i^*$-th antenna, the relay receives

$$\begin{aligned} y_R &= \mathbf{h}_{i^*}^H(\mathbf{p}_1 s_1 + \mathbf{P}_1\mathbf{w}_1) + \mathbf{g}_{i^*}^H(\mathbf{p}_2 s_2 + \mathbf{P}_2\mathbf{w}_2) + n_R \\ &= |\mathbf{h}_{i^*}|s_1 + |\mathbf{g}_{i^*}|s_2 + n_R, \end{aligned}$$

which is exactly the same as the previous section. Since the second phase is also the same as before, we can have the same SNR expressions as in the previous section.

Over two time slots, the eavesdropper will observe

$$\mathbf{y}_E = \begin{bmatrix} \mathbf{H}_{E,1}^H\mathbf{p}_1 & \mathbf{H}_{E,2}^H\mathbf{p}_2 & \mathbf{H}_{E,1}^H\mathbf{P}_1 & \mathbf{H}_{E,2}^H\mathbf{P}_2 \\ \beta\mathbf{h}_{E,R}|\mathbf{h}|_{i^*} & \beta\mathbf{h}_{E,R}|\mathbf{g}_{i^*}| & \mathbf{0}_{M\times x} & \mathbf{0}_{M\times x} \end{bmatrix} \times \begin{bmatrix} s_1^T & s_2^T & \mathbf{w}_1^T & \mathbf{w}_2^T \end{bmatrix}^T + \mathbf{n}_E. \tag{7}$$

Depending on how much interference is added into the system, the performance of the eavesdropping capability can be analyzed differently.

### A. When $2x + 1 \leq M$

Recall that the dimension of the eavesdropper's channel matrix in (7) is $2M \times (2x+2)$, but its row rank is only $(M+1)$. When $(M+1) \geq (2x+2)$ or equivalently $2x + 1 \leq M$, the eavesdropper has the capability to separate the source signals from interference. One possible approach is to first construct the following projection matrix

$$\mathbf{Q}_E = \mathbf{I}_M - \breve{\mathbf{H}}_E\left(\breve{\mathbf{H}}_E^H\breve{\mathbf{H}}_E\right)^{-1}\breve{\mathbf{H}}_E^H,$$

where $\breve{\mathbf{H}}_E = \begin{bmatrix}\mathbf{H}_{E,1}^H\mathbf{P}_1 & \mathbf{H}_{E,2}^H\mathbf{P}_2\end{bmatrix}$. Denote the eigenvalue decomposition of this matrix as $\breve{\mathbf{U}}\breve{\mathbf{U}}^H = \mathbf{Q}_E$, where the dimension of $\breve{\mathbf{U}}$ is $M \times (M - 2x)$ and we have used the fact that the eigenvalues of the projection matrix are either 1 or 0. We multiply the $M$ observations from the first time slot by $\breve{\mathbf{U}}^H$, i.e. $\breve{\mathbf{U}}^H\mathbf{y}_{E1}$, where $\mathbf{y}_E = \begin{bmatrix}\mathbf{y}_{E1}^T & \mathbf{y}_{E2}^T\end{bmatrix}^T$. The signal model at the eavesdropper can be written as

$$\breve{\mathbf{y}}_E = \begin{bmatrix} \breve{\mathbf{U}}^H\mathbf{H}_{E,1}^H\mathbf{p}_1 & \breve{\mathbf{U}}^H\mathbf{H}_{E,2}^H\mathbf{p}_2 \\ \beta\mathbf{h}_{E,R}|\mathbf{h}_{i^*}| & \beta\mathbf{h}_{E,R}|\mathbf{g}_{i^*}| \end{bmatrix}\begin{bmatrix} s_1 \\ s_2 \end{bmatrix} + \breve{\mathbf{n}}_E, \tag{8}$$

where $\breve{\mathbf{y}}_E = \begin{bmatrix}(\breve{\mathbf{U}}^H\mathbf{y}_{E1})^T & \mathbf{y}_{E2}^T\end{bmatrix}^T$ and $\breve{\mathbf{n}}_E$ is defined similarly. As shown in (8), the interference has been canceled since $\breve{\mathbf{U}}^H\mathbf{H}_{E,i}^H\mathbf{P}_i = 0$. The covariance matrix of $\breve{\mathbf{n}}_E$ is $\breve{\mathbf{C}}_n = diag\begin{bmatrix}\mathbf{I}_{M-2x} & \mathbf{I}_M + \beta^2\mathbf{h}_{ER}\mathbf{h}_{ER}^H\end{bmatrix}$.

Observing the signal model in (8), the effect of the added interference is to reduce the dimension of the channel matrix at the eavesdropper. Or in the other words, introducing interference has an effect to reduce the number of the antennas at the eavesdropper. Therefore an achievable secrecy rate will be

$$\mathcal{I}_{1\to 2} = \log\left(1 + \rho\frac{|\mathbf{h}_{i^*}|^2|\mathbf{g}_{i^*}|^2}{|\mathbf{h}_{i^*}|^2 + 2|\mathbf{g}_{i^*}|^2 + \frac{1}{\rho}}\right) - \log\left(1 + \rho\frac{1}{\left[(\breve{\mathbf{H}}^H\breve{\mathbf{H}})^{-1}\breve{\mathbf{H}}^H\breve{\mathbf{C}}_n\breve{\mathbf{H}}(\breve{\mathbf{H}}^H\breve{\mathbf{H}})^{-1}\right]_{1,1}}\right). \tag{9}$$

Following similar steps, we can have the lower bound on the secrecy rate as

$$\tilde{\mathcal{I}}_{1\to 2} = \log\frac{\min\{|\mathbf{h}_{i^*}|^2, |\mathbf{g}_{i^*}|^2\}}{4} + \log\left[(\breve{\mathbf{H}}_E^H\breve{\mathbf{H}}_E)^{-1}\right]_{1,1}, \tag{10}$$

where $\breve{\mathbf{H}}_E = \begin{bmatrix} \breve{\mathbf{U}}^H\mathbf{H}_{E,1}^H\mathbf{p}_1 & \breve{\mathbf{U}}^H\mathbf{H}_{E,2}^H\mathbf{p}_2 \\ \mathbf{h}_{E,R} & \tilde{\mathbf{h}}_{E,R} \end{bmatrix}$, and $\tilde{\mathbf{h}}_{E,R}$ is an auxiliary complex Gaussian vector independent to $\mathbf{h}_{E,R}$. Since the unitary transformation of a Gaussian matrix does not change its statistical property, $\breve{\mathbf{H}}_E$ is still a classical $(2M-2x)\times 2$ Gaussian matrix, and therefore the density function of $\frac{1}{\left[(\breve{\mathbf{H}}_E^H\breve{\mathbf{H}}_E)^{-1}\right]_{1,1}}$ is $f_{\chi\sim 2M-2x-1}(y) = \frac{y^{2M-2x-2}}{(2M-2x-2)!}e^{-x}$, a Chi-square distributed variable with $2(2M-2x-1)$ degrees of freedom, instead of $2(2M-1)$ as in the previous section. Following similar steps in the previous section, we can obtain the following lemma.

**Lemma** *2:* For $\frac{N}{M} \to \infty$, the probability to have zero secrecy rates is zero, i.e. $P(\mathcal{I}_{1\to 2} > 0) \to 1$.

Although the above lemma indicates that the scheme with artificial noise achieves the same asymptotic performance as the previous one, by introducing more interference, i.e. increasing $x$, will degrade the eavesdropping capability as shown in the following lemma.

**Lemma** *3:* Denote $\mathcal{I}_{1,x}^E$ as the data rate at which the eavesdropper can intercept the first user's information when the amount of the artificial noise is $x$. For the case with a fixed $x$ and $M \to \infty$, the probability that the eavesdropping capability is degraded by enlarging $x$ is one. i.e.

$$P(\mathcal{I}_{1,x-1}^E > \mathcal{I}_{1,x}^E) \to 1. \tag{11}$$

*Proof:* See Appendix. ■

Note that the scheme introduced in the previous section can be viewed as a special case with $x = 0$, and Lemma 3 shows that the achievable secrecy rate can be enlarged by injecting more interference into the communication system, since such interference will degrade the eavesdropping performance but not to the legitimate receivers. Although the lemma is proved with the condition of $M \to \infty$, for the scenarios that the value of $M$ is moderate, the conclusion in Lemma 3 still holds, as can be observed according to the simulation results shown in Section V.

### B. When $2x + 1 > M$

When $2x + 1 > M$, we can find that the channel matrix at the eavesdropper shown in (7) is no longer full rank. Or in other words, the two source nodes have injected so much interference that the eavesdropper cannot cancel such interference. Because the eavesdropper is severely interferenced during the first time slot, there is no need to consider the observations from this duration. As shown in the appendix, such a strategy did not cause much damage to the performance at the eavesdropper at high SNR.

Therefore after removing the observations severely damaged by interference and performing MRC, we can obtain the following signal model at the eavesdropper

$$\mathbf{h}_{E,R}^H \bar{\mathbf{y}}_E = \beta |\mathbf{h}_{E,R}|^2 \left[ |\mathbf{h}_{i^*}| \quad |\mathbf{g}_{i^*}| \right] \left[ s_1^T \quad s_2^T \right]^T + \mathbf{h}_{E,R}^H \bar{\mathbf{n}}_E. \quad (12)$$

Different to the previous MIMO case, the signal model in (12) is analog to a set of underdetermined linear equations. Although free of interference, the eavesdropper needs to detect two source messages based on a single observation. In the following, the capacity region of multiple access channels (MAC) will be used to bound the eavesdropping capability, and the detailed discussions about its relationship to zero forcing detection will be provided at the end of this section. Note that the noise power based on (12) can be expressed as

$$\begin{aligned} \mathcal{E}\{\mathbf{h}_{E,R}^H \bar{\mathbf{n}}_E \bar{\mathbf{n}}_E^H \mathbf{h}_{E,R}\} &= \frac{1}{\rho} \mathbf{h}_{ER}^H \left( \mathbf{I}_M + \beta^2 \mathbf{h}_{ER} \mathbf{h}_{ER}^H \right) \mathbf{h}_{ER} \quad (13) \\ &= \frac{|\mathbf{h}_{ER}|^2}{\rho} \left( 1 + \frac{|\mathbf{h}_{ER}|^2}{|\mathbf{h}_{i^*}|^2 + |\mathbf{g}_{i^*}|^2 + \frac{1}{\rho}} \right). \end{aligned}$$

With such a noise power, the use of the capacity region of MAC yields

$$\begin{cases} \mathcal{I}_{E1} & \leq \log \left( 1 + \rho \frac{|\mathbf{h}_{E,R}|^2 |\mathbf{h}_{i^*}|^2}{|\mathbf{h}_{ER}|^2 + |\mathbf{h}_{i^*}|^2 + |\mathbf{g}_{i^*}|^2 + \frac{1}{\rho}} \right) \\ \mathcal{I}_{E2} & \leq \log \left( 1 + \rho \frac{|\mathbf{h}_{E,R}|^2 |\mathbf{g}_{i^*}|^2}{|\mathbf{h}_{ER}|^2 + |\mathbf{h}_{i^*}|^2 + |\mathbf{g}_{i^*}|^2 + \frac{1}{\rho}} \right) \\ \mathcal{I}_{E1} + \mathcal{I}_{E2} & \leq \log \left( 1 + \rho \frac{|\mathbf{h}_{E,R}|^2 \left( |\mathbf{h}_{i^*}|^2 + |\mathbf{g}_{i^*}|^2 \right)}{|\mathbf{h}_{ER}|^2 + |\mathbf{h}_{i^*}|^2 + |\mathbf{g}_{i^*}|^2 + \frac{1}{\rho}} \right) \end{cases}. \quad (14)$$

The following lemma shows the asymptotic behavior of the probability to have zero secrecy rates.

**Lemma** *4:* For $N \to \infty$, the probability to have zero secrecy rates is zero, i.e. $P(\mathcal{I}_{1\to 2} > 0) \to 1$.

*Proof:* Without loss of generality, we still focus on the secrecy rate from the first source to the second one which can be lower bounded as shown in (15). Now the probability to have zero secrecy rates can be upper bounded as shown in (16). From the similar steps in the proof of Lemma 1, the extreme value theory can be applied and we can show the following

$$P \left( \min\{|\mathbf{h}_{i^*}|^2, |\mathbf{g}_{i^*}|^2\} \leq |\mathbf{h}_{E,R}|^2 \right) \to 0, \quad (17)$$

when $N \to \infty$. Note that $P \left( |\mathbf{h}_{i^*}|^2 + |\mathbf{g}_{i^*}|^2 < |\mathbf{h}_{E,R}|^2 \right) < P \left( \min\{|\mathbf{h}_{i^*}|^2, |\mathbf{g}_{i^*}|^2\} < |\mathbf{h}_{E,R}|^2 \right)$. Therefore the bound shown in (16) becomes zero, which means that the upper bound of the probability to have zero secrecy rates is also zero. The lemma is proved. ■

*1) Impact of different detection strategies:* In this section, we have used the capacity region of multiple access channels to obtain the lower bound of the secrecy rates as shown in (15). It is important to note that such a bound is quite loose. For example, if $\log \left( 1 + \rho \frac{|\mathbf{h}_{E,R}|^2 |\mathbf{h}_{i^*}|^2}{|\mathbf{h}_{ER}|^2 + |\mathbf{h}_{i^*}|^2 + |\mathbf{g}_{i^*}|^2 + \frac{1}{\rho}} \right)$ is used as the rate at which the eavesdropper can decode the first source's information, the rate related to the second source's information will be upper bounded by

$$\begin{aligned} \mathcal{I}_{E2} &\leq \log \left( 1 + \frac{\beta^2 |\mathbf{h}_{ER}|^4 |\mathbf{h}_{i^*}|^2}{\beta^2 |\mathbf{h}_{ER}|^4 |\mathbf{g}_{i^*}|^2 + \mathcal{E}\{\mathbf{h}_{E,R}^H \bar{\mathbf{n}}_E \bar{\mathbf{n}}_E^H \mathbf{h}_{E,R}\}} \right) \\ &\approx \log \left( 1 + \frac{|\mathbf{h}_{i^*}|^2}{|\mathbf{g}_{i^*}|^2} \right), \quad (18) \end{aligned}$$

a factor not even a function of the SNR, where the first inequality follows by treating the first source's messages as noise and the last one is following from the high SNR approximation. Actually when $M \to \infty$, we can find $\mathcal{I}_{E2} \leq \log \left( 1 + \frac{|\mathbf{h}_{i^*}|^2}{|\mathbf{g}_{i^*}|^2} \right) \approx 1$, a very low data rate. Therefore if the upper bound of the MAC individual rate constraints, i.e. $\log \left( 1 + \rho \frac{|\mathbf{h}_{E,R}|^2 |\mathbf{h}_{i^*}|^2}{|\mathbf{h}_{ER}|^2 + |\mathbf{h}_{i^*}|^2 + |\mathbf{g}_{i^*}|^2 + \frac{1}{\rho}} \right)$ is achievable, the achievable rate for the eavesdropper to intercept the other user's information becomes a small value constant. As can be seen from the above example, the bound based on the capacity region is quite loose, where the decoding capability of the eavesdropper has been exaggerated. On the other hand, the secrecy rates based on linear detection strategies, i.e. the ones shown in (4) and (9), yield the exact expressions of secrecy rates which are achievable to both two sources at the same time.

*2) Impact of the choice of $x$:* As can be observed from the signal model in (8), when increasing $x$ from 0 to $\lfloor \frac{M-1}{2} \rfloor$, the decoding capability of the eavesdropper will be reduced and the secrecy rate can be improved, since adding more interference is analog to reducing the number of antennas at the eavesdropper. Note that $\lfloor \cdot \rfloor$ denotes the floor operation.

When further increasing the value of $x$ from $\lfloor \frac{M-1}{2} \rfloor$ to $\lfloor \frac{M+1}{2} \rfloor$, the decoding capacity of the eavesdropper can be further reduced. For example, define $\mathcal{I}_{case1}^E$ as the sum rate obtained from (8) when $2x + 1 = M$,

$$\mathcal{I}_{case1}^E = \log\det \left( \mathbf{I}_{M+1} + \breve{\mathbf{H}} \breve{\mathbf{H}}^H \breve{\mathbf{C}}_n^{-1} \right),$$

and $\mathcal{I}_{case2}$ as the sum rate obtained from (12) when $2x = M$, i.e. $\mathcal{I}_{case2}^E = \log\det \left( \mathbf{I}_M + \hat{\mathbf{H}} \hat{\mathbf{H}}^H \bar{\mathbf{C}}_n^{-1} \right)$, where $\breve{\mathbf{H}}$ is the channel matrix shown in (8) and $\hat{\mathbf{H}}$ is defined in the appendix. Following the similar steps in the third part of the appendix, we can find

$$\mathcal{I}_{case1}^E = \log\det \left( \mathbf{I}_2 + \rho \breve{\mathbf{H}}_1^H \breve{\mathbf{H}}_1 + \hat{\mathbf{H}}^H \bar{\mathbf{C}}_n^{-1} \hat{\mathbf{H}} \right), \quad (19)$$

where $\breve{\mathbf{H}}_1$ is the $1 \times 2$ upper submatrix of $\breve{\mathbf{H}}$. Therefore $\mathcal{I}_{case1}^E - \mathcal{I}_{case2}^E > 0$ since the factor $\rho \breve{\mathbf{H}}_1^H \breve{\mathbf{H}}_1$ is dominant at high SNR. Therefore by increasing $2x$ from $(M-1)$ to $M$, the eavesdropping capability can be further reduced.

However, further adding interference by letting $2x > M$ will not affect the reception reliability at the eavesdropper due to the following reason. When $2x+1 > M$, the observations at the eavesdropper during the first time slot are so corrupted by the interference signals that the eavesdropper will simply drop these observations, and only focus on the second time slot. To such an eavesdropping strategy, further increasing $x$ has no impact, since the transmission during the second time slot becomes the weakest link in the system and further introducing interference to the first time slot is not helpful.

$$\begin{aligned}\mathcal{I}_{1\to 2} &\geq \log\left(\frac{\rho}{4}\min\{|\mathbf{h}_{i^*}|^2, |\mathbf{g}_{i^*}|^2\}\right) - \log\left(1+\rho\frac{|\mathbf{h}_{E,R}|^2|\mathbf{h}_{i^*}|^2}{|\mathbf{h}_{ER}|^2+|\mathbf{h}_{i^*}|^2+|\mathbf{g}_{i^*}|^2+\frac{1}{\rho}}\right) \\ &\geq \log\left(\frac{1}{4}\min\{|\mathbf{h}_{i^*}|^2, |\mathbf{g}_{i^*}|^2\}\right) - \log\left(\frac{|\mathbf{h}_{E,R}|^2\left(|\mathbf{h}_{i^*}|^2+|\mathbf{g}_{i^*}|^2\right)}{|\mathbf{h}_{ER}|^2+|\mathbf{h}_{i^*}|^2+|\mathbf{g}_{i^*}|^2}\right) \\ &\geq \log\left(\frac{1}{4}\min\{|\mathbf{h}_{i^*}|^2, |\mathbf{g}_{i^*}|^2\}\right) - \log\left(\min\{|\mathbf{h}_{E,R}|^2, |\mathbf{h}_{i^*}|^2+|\mathbf{g}_{i^*}|^2\}\right). \end{aligned} \tag{15}$$

$$\begin{aligned}P\left(\mathcal{I}_{1\to 2}<0\right) &\leq P\left(\frac{1}{4}\min\{|\mathbf{h}_{i^*}|^2, |\mathbf{g}_{i^*}|^2\} \leq |\mathbf{h}_{E,R}|^2, |\mathbf{h}_{E,R}|^2 < |\mathbf{h}_{i^*}|^2+|\mathbf{g}_{i^*}|^2\right) \\ &\quad +P\left(|\mathbf{h}_{E,R}|^2 > |\mathbf{h}_{i^*}|^2+|\mathbf{g}_{i^*}|^2\right) \\ &\leq P\left(\frac{1}{4}\min\{|\mathbf{h}_{i^*}|^2, |\mathbf{g}_{i^*}|^2\} \leq |\mathbf{h}_{E,R}|^2\right) + P\left(|\mathbf{h}_{E,R}|^2 > |\mathbf{h}_{i^*}|^2+|\mathbf{g}_{i^*}|^2\right). \end{aligned} \tag{16}$$

## IV. Secure Transmissions with Artificial Noise at Both Stages

In this section, we will study how to inject artificial noise during both time slots, which will increase the system complexity but yield a better secrecy rate. Following the similar steps in the previous section, the relay intends to broadcast the following message during the second time slot

$$x_R = \beta\left(|\mathbf{h}_{i^*}|s_1 + |\mathbf{g}_{i^*}|s_2 + n_R\right). \tag{20}$$

To reduce the system complexity, each destination selects a single antenna to receive such a mixture. By keeping the first time slot transmission strategy exactly the same as before, a straightforward strategy is following. Consider that the $n^*$-th antenna at the relay is selected to send $x_R$, and the $n_i^*$-th antenna at the $i$-th destination is used for receiving $x_R$, based on the following criterion

$$\begin{aligned}[n^*, n_1^*, n_2^*] = \arg\max\big\{&\min\{|h_{n,n_1}|^2, |g_{n,n_2}|^2\}, \\ &1\leq n\leq N, 1\leq n_1\leq M, 1\leq n_2\leq M\big\}.\end{aligned} \tag{21}$$

Surprisingly such a straightforward transmission strategy results in significant degradation of the outage performance. The exact reason for such a performance degradation is still unknown, and we suspect that outage events are more likely to happen when $n^*\neq i^*$, although we do not have a formal proof for this at this stage. In the following, we propose an alternative which can yield the full diversity gain of $MN$, and only require slight changes to the transmission strategy during the first time slot.

### A. An Antenna Selection Strategy with Full Diversity Gain

The antenna selection strategy consists of $N$ iterations. During each iteration, one antenna at the relay is chosen as the receiver during the first time slot and the transmitter during the second time slot. Beamforming will be used for source transmissions during the first time slot, and a single antenna is selected for receiving during the second time slot at each destinations respectively. The transmission strategy will be described in details as follows.

- For the $n$-th iteration, select the $n$-th antenna at the relay as the receiver during the first time slot and the transmitter during the second time slot.
- During the first time slot, the same transmission strategy as (6) is used, i.e. each source sends $\mathbf{x}_i = \mathbf{p}_i s_i + \mathbf{P}_i\mathbf{w}_i$, $i\in\{1,2\}$. The mixture to be broadcasted during the second time slot is $x_{R,n} = \frac{(|\mathbf{h}_n|s_1+|\mathbf{g}_n|s_2+n_R)}{\sqrt{|\mathbf{h}_n|^2+|\mathbf{g}_n|+\frac{1}{\rho}}}$. During the second time slot, each destination selects one antenna as the intended receiver based on the following criterion

$$|h_{m_{nh}^*n}|^2 = \max\{|h_{1n}|^2, \ldots, |h_{Mn}|^2\},$$

and

$$|g_{m_{ng}^*n}|^2 = \max\{|g_{1n}|^2, \ldots, |g_{Mn}|^2\},$$

where $h_{mn}$ denotes the channel between the $m$-th antenna at the first destination and the $n$-th antenna at the relay, and $g_{mn}$ is defined similarly.
- To ensure the intended receivers free of interference, the relay transmits

$$\mathbf{x}_R = \bar{\mathbf{1}}_{N,n}x_R + \mathbf{Q}_{Rn}\mathbf{z}_R, \tag{22}$$

where $\bar{\mathbf{1}}_{N,n}$ is a $N\times 1$ vector whose elements are zero expect its $n$-th element being 1, $\mathbf{Q}_{Rn}$ is a $N\times(N-2)$ matrix containing $(N-2)$ eigenvectors of the orthogonal projection matrix

$$\mathbf{I}_N - \mathbf{G}_n\left(\mathbf{G}_n^H\mathbf{G}_n\right)^{-1}\mathbf{G}_n^H, \tag{23}$$

where $\mathbf{G}_n = \begin{bmatrix}\mathbf{e}_{m_{nh}^*} & \mathbf{f}_{m_{ng}^*}\end{bmatrix}$ corresponding to its non-zero eigenvalues, $\mathbf{e}_{m_{nh}^*}$ is the $N\times 1$ channel vector between the relay and the $m_{nh}^*$-th antenna at the first source, $\mathbf{f}_{m_{ng}^*}$ is defined similarly related to the second source, and $\mathbf{z}_R$ is a $(N-2)\times 1$ vector containing interference. Note that the dimension of $\mathbf{z}_R$ is determined by the rank of the project matrix, and the above equation requires $N>2$ in order to ensure the existence of such projection matrices.
- Consequently the first source observes

$$y_{1,m_n^*} = h_{m_{nh}^*n}^H\frac{|\mathbf{h}_n|s_1+|\mathbf{g}_n|s_2+n_R}{\sqrt{|\mathbf{h}_n|^2+|\mathbf{g}_n|^2+\frac{1}{\rho}}} + n_{1,m_n^*} \tag{24}$$

After removing the self-interference,we can find the SNR at the first destination as

$$SNR_{1,n} = \frac{\rho|h_{m_{nh}^*n}|^2|\mathbf{g}_n|^2}{|\mathbf{h}_n|^2+|\mathbf{g}_n|^2+|h_{m_{nh}^*n}|^2+\frac{1}{\rho}}, \tag{25}$$

conditioned on the use of the $n$-th antenna at the relay.
- After $N$ iterations, select the $n^*$-th antenna which maximizes $\min\{SNR_{1,n}, SNR_{2,n}\}$.

As can be seen from the above description, during the first time slot, the two sources will inject the artificial noise $\mathbf{P}_i\mathbf{w}_i$ which will not be received at the selected relay antenna. However, at the eavesdropper the useful messages will be buried by the introduced artificial noise. A similar phenomenon can be observed during the second time slot. In the following section, the performance at the eavesdropper will be evaluated with details.

### *B. Performance at the eavesdropper*

In this section, we will only consider the case that maximum interference is added during both phases. For example, each source introduces $(M-1)$ interference signals during the first time slot, and $(N-2)$ interference signals are injected into the system during the second time slot, where $(N-2)\geq M$ is assumed to ensure that there are more than $M$ incoming signals at the eavesdropper during the second time slot. The performance of other cases can be obtained following the similar steps from the previous section. Since the dimension of interference signals is larger than the number of receiving antennas at the eavesdropper, interference signals will be treated as noise, which yields the following

$$\begin{aligned}\mathbf{y}_E &= \begin{bmatrix}\mathbf{H}_{E,1}^H\mathbf{p}_1 & \mathbf{H}_{E,2}^H\mathbf{p}_2\\ \beta_{n^*}\mathbf{h}_{E,R}|\mathbf{h}_{n^*}| & \beta_{n^*}\mathbf{h}_{E,R}|\mathbf{g}_{n^*}|\end{bmatrix}\begin{bmatrix}s_1\\ s_2\end{bmatrix}\\ &+\begin{bmatrix}\mathbf{H}_{E,1}^H\mathbf{P}_1 & \mathbf{H}_{E,2}^H\mathbf{P}_2 & \mathbf{0}_{M,N-2}\\ \mathbf{0}_{M\times(M-1)} & \mathbf{0}_{M\times(M-1)} & \mathbf{H}_{ER}\mathbf{Q}_{Rn^*}\end{bmatrix}\begin{bmatrix}\mathbf{w}_1\\ \mathbf{w}_2\\ \mathbf{z}_R\end{bmatrix}+\mathbf{n}_E\\ &=\begin{bmatrix}\hat{\mathbf{H}}_{E1}\\ \hat{\mathbf{H}}_{E2}\end{bmatrix}\begin{bmatrix}s_1\\ s_2\end{bmatrix}+\begin{bmatrix}\hat{\mathbf{G}}_{E1} & \mathbf{0}_{M,N-2}\\ \mathbf{0}_{M,2(M-1)} & \hat{\mathbf{G}}_{E2}\end{bmatrix}\begin{bmatrix}\mathbf{w}_1\\ \mathbf{w}_2\\ \mathbf{z}_R\end{bmatrix}+\mathbf{n}_E \quad (26)\end{aligned}$$

where the channel matrices have been denoted by a compact form in the second equation. In the following, we can show that the mutual information at the eavesdropper will be always bounded by a constant no matter whether linear detection strategies or the capacity region of multiple access channels is used.

*1) Zero forcing detection:* Given the signal model in (26), multiplying the observations by $\left(\hat{\mathbf{H}}_{E1}^H\hat{\mathbf{H}}_{E1}+\hat{\mathbf{H}}_{E2}^H\hat{\mathbf{H}}_{E2}\right)^{-1}\begin{bmatrix}\hat{\mathbf{H}}_{E1}^H & \hat{\mathbf{H}}_{E2}^H\end{bmatrix}$, the corresponding noise-interference covariance matrix can be shown in (27), where the noise part has been omitted due to the high SNR assumption. When $M$ becomes large, we can have the following approximations

$$\hat{\mathbf{H}}_{E1}^H\hat{\mathbf{H}}_{E1}\to M\mathbf{I}_2,\hat{\mathbf{H}}_{E2}^H\hat{\mathbf{H}}_{E2}\to\frac{M}{2}\mathbf{1}_{2,2}, \quad (28)$$

where $\mathbf{1}_{m,n}$ is an $m\times n$ all one matrix. To find the asymptotic behavior of $\left(\hat{\mathbf{H}}_{E1}^H\hat{\mathbf{G}}_{E1}\hat{\mathbf{G}}_{E1}^H\hat{\mathbf{H}}_{E1}+\hat{\mathbf{H}}_{E2}^H\hat{\mathbf{G}}_{E2}\hat{\mathbf{G}}_{E2}^H\hat{\mathbf{H}}_{E2}\right)$, we first study the following eigenvalue decomposition

$$\hat{\mathbf{H}}_{E1}^H\hat{\mathbf{G}}_{E1}\hat{\mathbf{G}}_{E1}^H\hat{\mathbf{H}}_{E1} \quad = \quad \hat{\mathbf{H}}_{E1}^H\hat{\mathbf{U}}_{G,E1}\hat{\mathbf{\Lambda}}_{G,E1}\hat{\mathbf{U}}_{G,E1}^H\hat{\mathbf{H}}_{E1},$$

where $\hat{\mathbf{U}}_{G,E1}$ is an $M\times M$ matrix containing the eigenvectors of $\hat{\mathbf{G}}_{E1}\hat{\mathbf{G}}_{E1}^H$, and denote $\lambda_{min,G1}$ as its smallest eigenvalue. Recall that $\hat{\mathbf{G}}_{E1}$ is an $M\times 2(M-1)$ complex Gaussian matrix, we can find that its smallest eigenvalue has the following asymptotic behavior [23]

$$\frac{1}{M}\lambda_{min,G1}\to 2\left(1-\sqrt{\frac{1}{2}}\right)^2,$$

since $\lim\limits_{M\to\infty}\frac{M}{2(M-1)}=\frac{1}{2}$. Note that $\hat{\mathbf{H}}_{E1}^H\hat{\mathbf{U}}_{G,E1}$ is still complex Gaussian distributed since $\hat{\mathbf{H}}_{E1}$ and $\hat{\mathbf{G}}_{E1}$ are independent, and therefore the approximation in (28) can be applied similarly. Therefore the SNR for the first source's information at the eavesdropper can be bounded as

$$SNR_{E1}=\frac{1}{[\hat{\mathbf{C}}_n]_{1,1}}\leq \frac{1}{\left[\left(M\mathbf{I}_2+\frac{M}{2}\mathbf{1}_{22}\right)^{-1}\left(\varrho_1M^2\mathbf{I}_2+\varrho_2M^2\mathbf{1}_{22}\right)\left(M\mathbf{I}_2+\frac{M}{2}\mathbf{1}_{22}\right)^{-1}\right]_{11}},$$

where $\varrho_1=2\left(1-\sqrt{\frac{1}{2}}\right)^2$ and $\varrho_2=2\left(1-\sqrt{\lim\limits_{M\to\infty}\frac{M}{N-2}}\right)^2$. Without the need to know $\lim\limits_{M\to\infty}\frac{M}{N-2}$, we can further upper bound the above SNR as

$$SNR_{E1} \quad\leq\quad \frac{1}{\varrho_1M\left[\left(\mathbf{I}_2+\frac{1}{2}\mathbf{1}_{22}\right)^{-2}\right]_{11}}\leq\frac{9}{4\varrho_1M}.$$

which means that the mutual information at the eavesdropper has the following approximation

$$\mathcal{I}_{E1}=\log(1+SNR_{E1})\leq\log\left(1+\frac{9}{4\varrho_1M}\right)\to 0, \quad (29)$$

when $M$ and $N$ is large enough. Therefore when linear detection methods are used, the rate at which the eavesdropper can intercept the source information goes to zero, even if the SNR becomes infinity. It is worth pointing out that the above asymptotic studies are obtained in the high SNR regime.

*2) Based on the capacity region of multiple access channels:* As discussed before, the use of the capacity region of multiple access channels can help us to obtain an upper bound of the eavesdropper capability. Without loss of generality, take the first source's information as an example. The rate at which the eavesdropper can intercept such a message is bounded as

$$\begin{aligned}\mathcal{I}_{E1} \quad&\leq\quad \log\left(1+\begin{bmatrix}\hat{\mathbf{h}}_{E1}\\ \hat{\mathbf{h}}_{E2}\end{bmatrix}^H\right. \quad (30)\\ &\qquad\left.\times\begin{bmatrix}\hat{\mathbf{G}}_{E1}\hat{\mathbf{G}}_{E1}^H & \mathbf{0}_{M,M}\\ \mathbf{0}_{M,M} & \hat{\mathbf{G}}_{E2}\hat{\mathbf{G}}_{E2}^H\end{bmatrix}^{-1}\begin{bmatrix}\hat{\mathbf{h}}_{E1}\\ \hat{\mathbf{h}}_{E2}\end{bmatrix}\right)\\ &=\quad \log\left(1+\left(\hat{\mathbf{h}}_{E1}^H\left[\hat{\mathbf{G}}_{E1}\hat{\mathbf{G}}_{E1}^H\right]^{-1}\hat{\mathbf{h}}_{E1}\right.\right.\\ &\qquad\left.\left.+\hat{\mathbf{h}}_{E2}^H\left[\hat{\mathbf{G}}_{E2}\hat{\mathbf{G}}_{E2}^H\right]^{-1}\hat{\mathbf{h}}_{E2}\right)\right).\end{aligned}$$

$$\begin{aligned}\hat{\mathbf{C}}_n &\approx \left(\hat{\mathbf{H}}_{E1}^H\hat{\mathbf{H}}_{E1}+\hat{\mathbf{H}}_{E2}^H\hat{\mathbf{H}}_{E2}\right)^{-1}\begin{bmatrix}\hat{\mathbf{H}}_{E1}\\ \hat{\mathbf{H}}_{E2}\end{bmatrix}^H\begin{bmatrix}\hat{\mathbf{G}}_{E1}\hat{\mathbf{G}}_{E1}^H & \mathbf{0}_{M,M}\\ \mathbf{0}_{M,M} & \hat{\mathbf{G}}_{E2}\hat{\mathbf{G}}_{E2}^H\end{bmatrix}\begin{bmatrix}\hat{\mathbf{H}}_{E1}\\ \hat{\mathbf{H}}_{E2}\end{bmatrix}\left(\hat{\mathbf{H}}_{E1}^H\hat{\mathbf{H}}_{E1}+\hat{\mathbf{H}}_{E2}^H\hat{\mathbf{H}}_{E2}\right)^{-1} \quad (27)\\ &= \left(\hat{\mathbf{H}}_{E1}^H\hat{\mathbf{H}}_{E1}+\hat{\mathbf{H}}_{E2}^H\hat{\mathbf{H}}_{E2}\right)^{-1}\left(\hat{\mathbf{H}}_{E1}^H\hat{\mathbf{G}}_{E1}\hat{\mathbf{G}}_{E1}^H\hat{\mathbf{H}}_{E1}+\hat{\mathbf{H}}_{E2}^H\hat{\mathbf{G}}_{E2}\hat{\mathbf{G}}_{E2}^H\hat{\mathbf{H}}_{E2}\right)\left(\hat{\mathbf{H}}_{E1}^H\hat{\mathbf{H}}_{E1}+\hat{\mathbf{H}}_{E2}^H\hat{\mathbf{H}}_{E2}\right)^{-1},\end{aligned}$$

Again applying the eigenvalue decomposition for $\hat{\mathbf{G}}_{Ei}\hat{\mathbf{G}}_{Ei}^H$, we can further bound the rate as

$$\begin{aligned}\mathcal{I}_{E1} &\leq \log\left(1+\left(\hat{\mathbf{h}}_{E1}^H\left[\lambda_{min,G1}\hat{\mathbf{U}}_{G,E1}\hat{\mathbf{U}}_{G,E1}^H\right]^{-1}\hat{\mathbf{h}}_{E1}\right.\right.\\ &\qquad \left.\left.+\hat{\mathbf{h}}_{E2}^H\left[\lambda_{min,G2}\hat{\mathbf{U}}_{G,E2}\hat{\mathbf{U}}_{G,E2}^H\right]^{-1}\hat{\mathbf{h}}_{E2}\right)\right)\\ &\to \log\left(1+\left(\frac{1}{\varrho_1 M}\hat{\mathbf{h}}_{E1}^H\hat{\mathbf{U}}_{G,E1}^H\hat{\mathbf{U}}_{G,E1}\hat{\mathbf{h}}_{E1}\right.\right.\\ &\qquad \left.\left.+\frac{1}{\varrho_2 M}\hat{\mathbf{h}}_{E2}^H\hat{\mathbf{U}}_{G,E2}^H\hat{\mathbf{U}}_{G,E2}\hat{\mathbf{h}}_{E2}\right)\right)\\ &\to \log\left(1+\frac{1}{\varrho_1}+\frac{1}{\varrho_2}\right),\end{aligned}$$

which means that the mutual information at the eavesdropper is bounded as

$$\mathcal{I}_{E1} \leq \log\left(1+\frac{1}{\varrho_1}+\frac{1}{\varrho_2}\right), \quad (31)$$

which is again not a function of the SNR. Different to the zero forcing case, $\lim\limits_{M\to\infty}\frac{M}{N-2}$ is needed to evaluate the upper bound. Take $N=2M$ as an example, which means $\varrho_2 = 0.1716$ and the use of the MAC capacity region yields an upper bound of 3.6618, no matter how large the SNR is.

*Remark 1:* To evaluate the inverse of the matrix in the above equation, we have used the minimum eigenvalue to obtain the upper bound, and one can imagine that such an upper bound based on the minimum eigenvalue is quite loose, and the actual rate at which the eavesdropper can intercept the source messages will be less than the one shown in (31).

*Remark 2:* Consider that $\mathcal{I}(x_1; y_E|x_2)$ is achievable for the eavesdropper to intercept the first source's information, i.e. $\mathcal{I}_{E1} = \mathcal{I}(x_1; y_E|x_2)$, as in (30). It is important to point out that the rate at which the eavesdropper can intercept the second source will become zero, as discussed at the end of the previous section. Therefore, an achievable symmetrical rate will be less than the one in (31), and the performance difference between the use of linear methods and the MAC capacity region can be further reduced.

### C. Achievable Secrecy Rate

The secrecy rate achieved by the proposed transmission protocol can be expressed as

$$\begin{aligned}\mathcal{I}_{1\to 2} &= \log(1+SNR_{1,n^*})-\mathcal{I}_{E1} \quad (32)\\ &\approx \log\left(1+\rho\frac{|h_{m^*_{n^*h}n^*}|^2|\mathbf{g}_{n^*}|^2}{|\mathbf{h}_{n^*}|^2+|\mathbf{g}_{n^*}|^2+|h_{m^*_{n^*h}n^*}|^2+\frac{1}{\rho}}\right),\end{aligned}$$

where $\mathcal{I}_{E1}$ is removed since it is a constant not related to SNR as shown previously. The following lemma shows the diversity gain achieved by the proposed secure transmission.

**Lemma 5:** The proposed secure transmission protocol can achieve the full diversity gain of $MN$, i.e. $P(\mathcal{I}_{1\to 2} < R) \doteq \frac{1}{\rho^{MN}}$, where $R$ is a targeted data rate and $f(\rho)$ is said to be exponentially equal to $\rho^d$, denoted as $f(\rho) \doteq \rho^d$, when $\lim\limits_{\rho\to\infty}\frac{\log[f(\rho)]}{\log\rho} = d$.

*Proof:* Recall that the antenna selection strategy consists of $N$ iterations. First consider the $n$-th iteration when the $n$-th antenna at the relay has been used. To simplify the notation, denote $x_{mn}$ as $x_{mn} = |h_{mn}|^2$. Order these $M$ variables and denote the ordered ones as $x_{(m)n}$, $1 \leq m \leq M$, i.e. $x_{(1)n} \leq \cdots \leq x_{(M)n}$. Similarly the channels related to the second source can also be ordered as $y_{(m)n}$. Therefore, the SNR can be expressed as

$$\begin{aligned}SNR_{1,n} &\approx \frac{\rho x_{(M)n}\sum_{m=1}^M y_{(m)n}}{2x_{(M)n}+\sum_{m=1}^{M-1}x_{(m)n}+\sum_{m=1}^M y_{(m)n}}\\ &\geq \frac{\rho x_{(M)n}\sum_{m=1}^M y_{(m)n}}{(M+1)x_{(M)n}+\sum_{m=1}^M y_{(m)n}}. \quad (33)\end{aligned}$$

Define $\omega = \frac{2^R-1}{\rho}$ and $\epsilon = 2^R-1$. Since the upper bound of the outage probability is of interest, we can have

$$\begin{aligned}P_e &\leq P\left(\frac{x_{(M)n}\sum_{m=1}^M y_{(m)n}}{x_{(M)n}+\sum_{m=1}^M y_{(m)n}} < (M+1)\omega\right) \quad (34)\\ &\leq P\left(\sum_{m=1}^M y_{(m)n} < (M+1)\omega\right)\\ &\quad +P\left(x_{(M)n} < (M+1)\omega\right),\end{aligned}$$

where $P_e$ denotes $(SNR_{1,n} < \epsilon)$ for simplicity. Recall that the CDF of $x_{(M)n}$ is $F_{x_{(M)n}}(x) = \left(1-e^{-x}\right)^M$, and the pdf of $\sum_{m=1}^M y_{(m)n}$ is $f_{\sum_{m=1}^M y_{(m)n}}(y) = \frac{y^{M-1}}{(M-1)!}e^{-y}$. So the upper bound of the outage probability can be expressed as

$$\begin{aligned}P_e &\leq \left(1-e^{-(M+1)\omega}\right)^M \quad (35)\\ &\quad +\int_0^{(M+1)\omega}\frac{y^{M-1}}{(M-1)!}e^{-y}dy\\ &\approx (M+1)^M\omega^M+\int_0^{(M+1)\omega}\frac{y^{M-1}}{(M-1)!}dy \doteq \rho^M,\end{aligned}$$

where the integral about $y$ has been simplified by using the fact that $e^{-y} \approx 1$ since $y \leq (M+1)\omega \to 0$. The lower bound of the outage probability can be easily obtained as follows

$$\begin{aligned}SNR_{1,n} &\leq \frac{\rho\sum_{m=1}^M x_{(m)n}\sum_{m=1}^M y_{(m)n}}{2\sum_{m=1}^M y_{(m)n}+\sum_{m=1}^M y_{(m)n}} \quad (36)\\ &\leq \rho\min\left\{\sum_{m=1}^M x_{(m)n}, \sum_{m=1}^M y_{(m)n}\right\}.\end{aligned}$$

By using the fact that $\sum_{m=1}^M x_{(m)n}$ and $\sum_{m=1}^M y_{(m)n}$ are independently identically Chi-square distributed, we can find that the lower bound of $P(SNR_{1,n} < \epsilon)$ is also decaying as $\rho^M$, the same as the upper bound. Therefore we have

$P(SNR_{i,n} < \epsilon) \doteq \rho^M$, $i \in \{1,2\}$, which leads to $P(\min\{SNR_{i,n}, i \in \{1,2\}\} < \omega) \doteq \rho^M$. Note that the $n^*$-th antenna at the relay is selected due to the criterion

$$n^* = \arg\max\{\min\{SNR_{1,n}, SNR_{2,n}\}, 1 \leq n \leq N\}.$$

Using the fact that any pair of channels $h_{mn}$ and $h_{li}$ are independent if $n \neq i$, the lemma is proved. ■

Comparing Lemma 5 to Lemma 1 and 2, the performance gains by adding artificial noise to both time slots are significant, where the outage probability, not just the probability to have zero secrecy rates, is going to zero for any targeted data rate. However, the transmission protocol proposed in this section causes the largest system complexity compared to the previous two schemes. Specifically the antennas at the source need to perform beamforming for the source signals, and carry out the transmissions of interference signals simultaneously. In addition, the protocol with interference at both stages requires all antennas at the relay to be used, where the transmission protocols introduced in the previous sections only need to use one single antenna at the relay.

## V. Numerical Results

In this section, the computer simulations will be used to verify the performance of the described secure transmission schemes. To simplify the notations, we denote the three schemes described in Sections II, III and IV, by Scenario I, II and III, respectively.

In Fig. 1, the performance achieved by the transmission schemes described in Section II and III is compared. Specifically, in Fig. 1.a, the probability to have zero secrecy rates is shown as a function of the number of the relay antennas. Recall from Lemma 1 and 2 that the probability to have a zero secrecy rate approaches zero, i.e. $P(\mathcal{I}_{1\to 2} > 0) \to 1$, when $\frac{N}{M} \to \infty$. As can be seen from the figure, by increasing the number of the relay antennas, the probability to have zero secrecy rates is decreasing, which confirms the analytical results developed in Lemma 1 and 2. In addition, it can be easily observed that Scenario II can achieve a better secure performance than Scenario I, which is due to the fact that artificial noise has been added into the multiple access stage. By increasing the value of $x$, the performance of the scheme shown in Section III can be further improved. Recall that Lemma 3 states that the eavesdropping capability will be decreased by introducing more interference, i.e. increasing the value of $x$. The observation from Fig. 1 is consistent to this lemma. To better demonstrate the accuracy of Lemma 3, Fig. 2 is provided to consider the performance of the transmission scheme shown in Section III with different choices of $M$ and $x$, constrained by $2x + 1 \leq M$. As can be observed from this figure, while keeping $M$ fixed, increasing $x$ is helpful to damage the eavesdropping capability and improve the secrecy rate, which confirms Lemma 3.

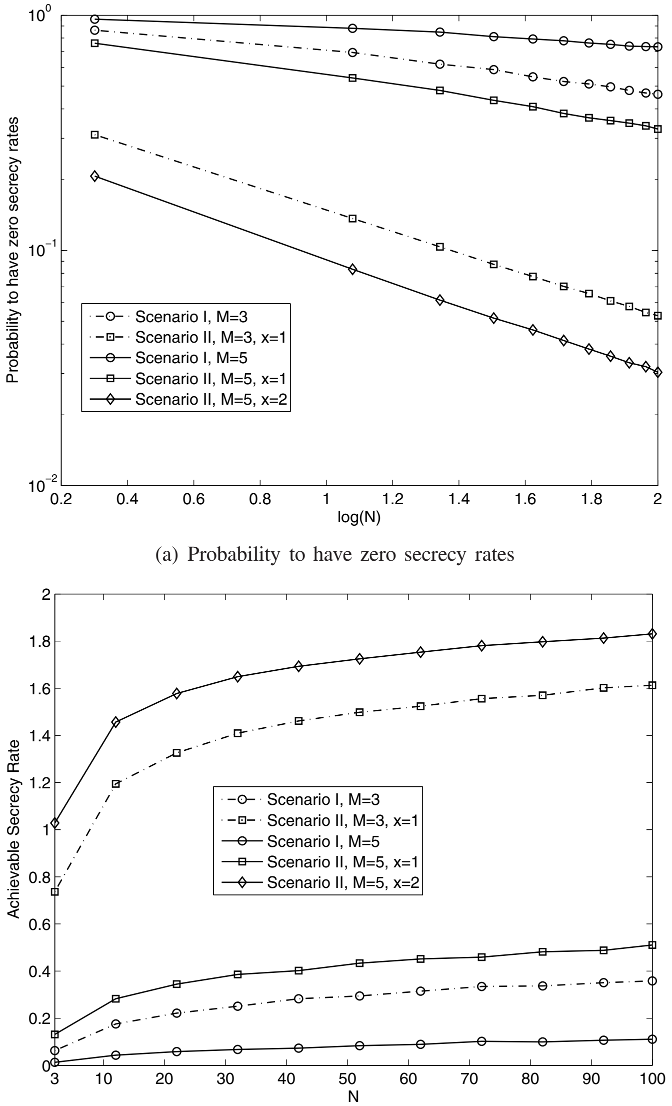
As discussed in Section III, when there is too much interference injected during the first phase, the eavesdropper may simply drop these observations, and the performance of such a strategy is studied in the following three figures. In Fig. 3, the MAC individual rate constraint shown in (14), $\mathcal{I}_{E1} \leq \log\left(1 + \rho\frac{|\mathbf{h}_{E,R}|^2|\mathbf{h}_{i^*}|^2}{|\mathbf{h}_{ER}|^2+|\mathbf{h}_{i^*}|^2+|\mathbf{g}_{i^*}|^2+\frac{1}{\rho}}\right)$, is used to obtain the lower bounds of the achievable secrecy rates. As can be observed from Fig. 3, the secure performance of Scenario II will still be improved by increasing the number of the relay antennas. For example, the use of more relay antennas can reduce the probability to have zero secrecy rates, and this observation confirms Lemma 4 which states that the probability to have non-zero secrecy rates approaches one when $N \to \infty$. Similarly, the achievable secrecy rate will be increased by using more antennas at the relay, since the use of extra relay antennas can increase the diversity gain at the legitimate receivers, but not helpful to the eavesdropper.

However, the use of such individual rate constraints will exaggerate the eavesdropping capability, as discussed in Section III. For example, if the eavesdropping rate for one source's information is $\mathcal{I}_{E1} = \log\left(1 + \rho\frac{|\mathbf{h}_{E,R}|^2|\mathbf{h}_{i^*}|^2}{|\mathbf{h}_{ER}|^2+|\mathbf{h}_{i^*}|^2+|\mathbf{g}_{i^*}|^2+\frac{1}{\rho}}\right)$, it is easy to show that the eavesdropping rate for the other source is $\mathcal{I}_{E2} \leq \log\left(1 + \frac{|\mathbf{h}_{i^*}|^2}{|\mathbf{g}_{i^*}|^2}\right) \approx 1$, not even a function of the SNR. Such a phenomenon can also be observed by comparing Fig. 3.b and Fig. 4. Specifically Fig. 3.b could lead a wrong conclusion that adding more interference will reduce the achievable secrecy rate, which is due to the fact that the eavesdropping capability is exaggerated. The use of the MAC sum rate constraint is considered in Fig. 4 which yields a more reasonable observation that more added interference yields the improvement of the achievable secrecy rates. In addition, the huge gap between the curves with the sum rate and individual rate constraints also demonstrates the fact that the use of the individual ones will underestimate the achievable secrecy rate.

In Fig. 5, the performance of the secure transmission scheme with artificial noise added to both stages is studied. Given the fact that the use of the MAC capacity region can only yield a loose lower bound of the secrecy rate, we only focus on the use of the zero forcing method. In Fig. 5.a, the outage probability is shown as a function of SNR. Recall that Lemma 5 states that the diversity order achieved by the proposed scheme is proportional to the number of the relay and source antennas. As can be observed from the figure, using more antennas at the sources and the relay, i.e. increasing $M$ or $N$, will ensure that the slope of the outage probability curves is increased, which means that the diversity order is increased by using more source and relay antennas. And therefore such an observation confirms the analytical results shown in Lemma 5. In Fig. 5.b, the achievable secrecy rate is shown as a function of the number of the relay antennas. By increasing the number of the relay antennas, a larger secrecy rate can be achieved. In addition, it can also be observed from Fig. 5.b that the curves for Scenario III are growing with $N$ at a larger slope, which means that the gap between the two scenarios will be further enlarged.

## VI. Conclusions

In this paper, we have studied two-way relaying transmissions with various tradeoff between the security and complexity. When antenna selection is applied at the relay and no interference is added to both stages, the secure performance is worst, where the probability to have zero secrecy rates will be decreased by using more relay antennas, but not by increasing the SNR. When adding artificial noise during the



(a) Probability to have zero secrecy rates

(b) Achievable secrecy rates

Fig. 1. Performance of the secure transmission protocols described in Section II and III. The transmit SNR is 5dB, i.e. $\rho = 5$.

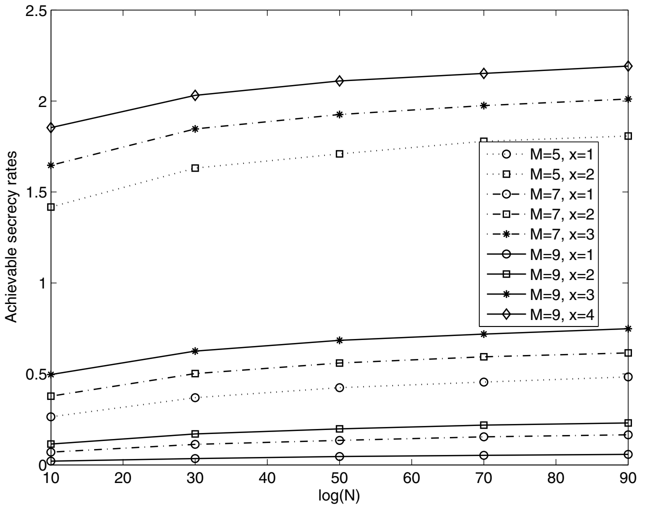
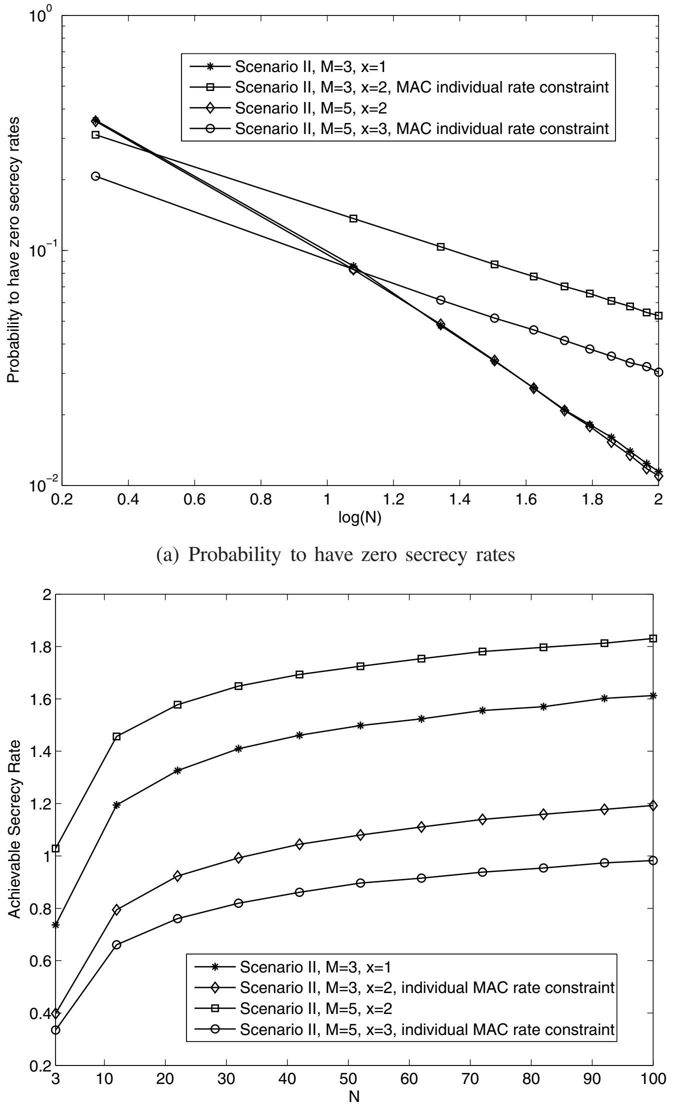


Fig. 2. Achievable rates for the secure transmission protocols described in Section III. The transmit SNR is 5dB, i.e. $\rho = 5$.



(a) Probability to have zero secrecy rates

(b) Achievable secrecy rates

Fig. 3. Performance of the secure transmission protocols described in Section III. The transmit SNR is 5dB, i.e. $\rho = 5$.

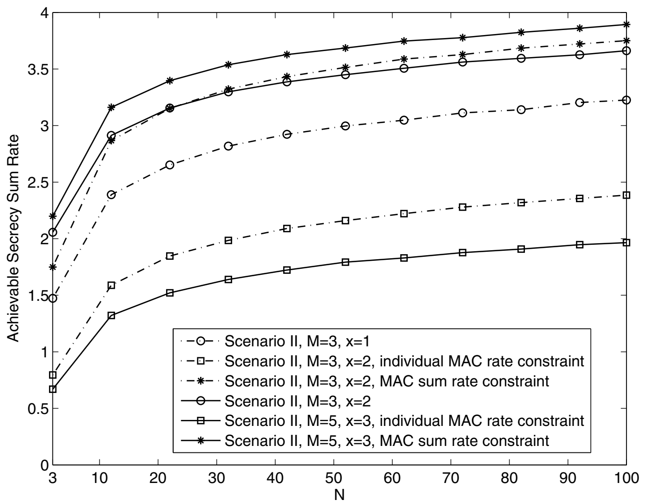
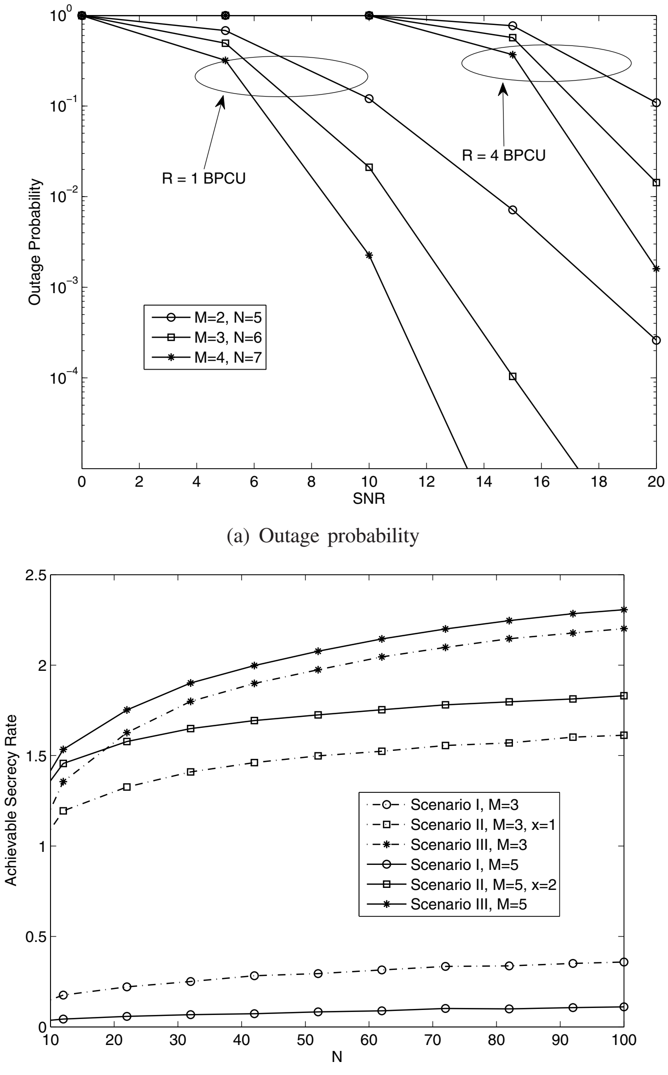


Fig. 4. Performance of the secure transmission protocols described in Section III. The transmit SNR is 5dB, i.e. $\rho = 5$.



(a) Outage probability

(b) Achievable secrecy rates ($\rho = 5$)

Fig. 5. Performance of the secure transmission protocols described in Section IV.

first phase, the reception reliability at the eavesdropper can be decreased, however, there is a threshold for the amount of the interference, above which more interference does not cause much performance degradation at the eavesdropper. The secure performance of the third scenario is the best, where the outage probability for any targeted data rate can be decreased to zero by increasing the SNR. But such a scheme will impose the most complexity on the system, since all the relay antennas will be used for cooperative jamming. In this paper, we have considered two types of detection strategies at the eavesdropper. One is based on linear detection methods, as shown in Section III-A and Section IV-B1. The other is based on the capacity region, as shown in Section III-B and Section IV-B2. The capacity region forms an upper bound for the eavesdropping capability, whereas the use of linear detection methods gives us an achievable performance at the eavesdropper. It is a promising future direction to study how to select $n$ best antennas $n > 1$, which may not increase the diversity gain, but yield a constant outage performance gain [24]. However, it is worth pointing out that there are two difficulties to use multiple antennas in the addressed two-way secure scenario. One is to design a sophisticated relaying beamformer which is to serve two source nodes simultaneously. And the other is to maintain security risk, since the amount of artificial noise injected to the system is inversely promotional to the number of the used relay antennas, as can be seen from (6).

## Appendix

*Proof of Proposition 1 :* We first focus on the matrix $\mathbf{A}$, and $\mathbf{A}^H\mathbf{A}$ can be expressed as

$$\mathbf{A}^H\mathbf{A} = \begin{bmatrix} |\mathbf{a}|^2+|\mathbf{c}|^2 & \mathbf{a}^H\mathbf{b}+\mathbf{c}^H\mathbf{d} \\ \mathbf{b}^H\mathbf{a}+\mathbf{d}^H\mathbf{a} & |\mathbf{b}|^2+|\mathbf{d}|^2 \end{bmatrix}. \tag{37}$$

And therefore $\left[\mathbf{A}^H\mathbf{A}\right]^{-1}_{1,1}$ can be obtained as

$$\frac{1}{\left[\mathbf{A}^H\mathbf{A}\right]^{-1}_{1,1}} = |\mathbf{a}|^2+|\mathbf{c}|^2 - \frac{|\mathbf{a}^H\mathbf{b}+\mathbf{c}^H\mathbf{d}|^2}{|\mathbf{b}|^2+|\mathbf{d}|^2}. \tag{38}$$

Similarly $\left[\mathbf{B}^H\mathbf{B}\right]^{-1}_{1,1}$ can be expressed as

$$\frac{1}{\left[\mathbf{B}^H\mathbf{B}\right]^{-1}_{1,1}} = |\mathbf{a}|^2+|\mathbf{c}|^2 - \frac{|\mathbf{a}^H\mathbf{b}+\mathbf{c}^H\mathbf{c}|^2}{|\mathbf{b}|^2+|\mathbf{c}|^2}. \tag{39}$$

The addressed probability can be rewritten as

$$\begin{aligned} &P\left(\frac{1}{\left[\mathbf{A}^H\mathbf{A}\right]^{-1}_{i,i}} > \frac{1}{\left[\mathbf{B}^H\mathbf{B}\right]^{-1}_{i,i}}\right) \\ &= P\left(\frac{|\mathbf{a}^H\mathbf{b}+\mathbf{c}^H\mathbf{c}|^2}{|\mathbf{b}|^2+|\mathbf{c}|^2} > \frac{|\mathbf{a}^H\mathbf{b}+\mathbf{c}^H\mathbf{d}|^2}{|\mathbf{b}|^2+|\mathbf{d}|^2}\right). \end{aligned} \tag{40}$$

The right hand side of the inequality can be written as

$$\frac{|\mathbf{a}^H\mathbf{b}+\mathbf{c}^H\mathbf{d}|^2}{|\mathbf{b}|^2+|\mathbf{d}|^2} = \left|\frac{\mathbf{b}^H}{\sqrt{|\mathbf{b}|^2+|\mathbf{d}|^2}}\mathbf{a} + \frac{\mathbf{d}^H}{\sqrt{|\mathbf{b}|^2+|\mathbf{d}|^2}}\mathbf{c}\right|^2. \tag{41}$$

$\frac{\mathbf{b}^H}{\sqrt{|\mathbf{b}|^2+|\mathbf{d}|^2}}\mathbf{a}$ is still complex Gaussian distributed, i.e. its $i$-th element has the distribution $CN\left(0, \frac{|b_i|^2}{|\mathbf{b}|^2+|\mathbf{d}|^2}\right)$, where $b_i$ is the $i$-th element of $\mathbf{b}$. A similar observation can be made for $\frac{\mathbf{d}^H}{\sqrt{|\mathbf{b}|^2+|\mathbf{d}|^2}}\mathbf{c}$. Since $\mathbf{a}$ and $\mathbf{c}$ are independent, the factor in (41) is exponentially distributed with mean 1, no matter how large the value of $M$ is. The left hand side of the inequality can be approximated as

$$\begin{aligned} \frac{|\mathbf{a}^H\mathbf{b}+\mathbf{c}^H\mathbf{c}|^2}{|\mathbf{b}|^2+|\mathbf{c}|^2} &= \left|\frac{\mathbf{b}^H}{\sqrt{|\mathbf{b}|^2+|\mathbf{c}|^2}}\mathbf{a} + \frac{|\mathbf{c}|^2}{\sqrt{|\mathbf{b}|^2+|\mathbf{c}|^2}}\right|^2 \\ &\approx \left|\frac{|\mathbf{c}|^2}{\sqrt{|\mathbf{b}|^2+|\mathbf{c}|^2}}\right|^2 \approx \frac{M}{2} \to \infty, \end{aligned} \tag{42}$$

where the approximation follows from $\frac{\mathbf{b}^H}{\sqrt{|\mathbf{b}|^2+|\mathbf{c}|^2}}\mathbf{a} \to M\mathcal{E}\left\{\frac{b_i^* a_i}{\sqrt{|\mathbf{b}|^2+|\mathbf{c}|^2}}\right\} \to 0$ and $\frac{|\mathbf{c}|^2}{\sqrt{|\mathbf{b}|^2+|\mathbf{c}|^2}} \to \frac{M\mathcal{E}\{|c|_i^2\}}{\sqrt{M\mathcal{E}\{|b|_i^2\}+M\mathcal{E}\{|c|_i^2\}}} \to \frac{\sqrt{M}}{\sqrt{2}}$, given $M \to \infty$. The addressed probability can now be approximated as

$$P\left(\frac{1}{\left[\mathbf{A}^H\mathbf{A}\right]^{-1}_{i,i}} > \frac{1}{\left[\mathbf{B}^H\mathbf{B}\right]^{-1}_{i,i}}\right) \approx 1 - e^{-\frac{M}{2}} \approx 1, \tag{43}$$

when $M \to \infty$. And the proposition is proved. ■

*Proof for Lemma 1 :* At high SNR, the receive SNR expression in (3) can be approximated as $\frac{\rho|\mathbf{h}_{i*}|^2|\mathbf{g}_{i*}|^2}{|\mathbf{h}_{i*}|^2+2|\mathbf{g}_{i*}|^2}$ which can be first lower bounded as $\frac{\rho|\mathbf{h}_{i*}|^2|\mathbf{g}_{i*}|^2}{2(|\mathbf{h}_{i*}|^2+|\mathbf{g}_{i*}|^2)}$. Then by using a property of the harmonic mean, i.e. $\frac{ab}{a+b} > \frac{1}{2}\min\{a,b\}$, we can lower bound the data rate at the legitimate receivers as $\log\left(\frac{\rho}{4}\min\{|\mathbf{h}_{1^*}|^2, |\mathbf{h}_{2^*}|^2\}\right)$.

On the other hand, recall that the noise covariance matrix at the eavesdropper is $\mathbf{C}_n = \begin{bmatrix}\mathbf{I}_M & \mathbf{0}_M \\ \mathbf{0}_M & \mathbf{I}_M + \beta^2\mathbf{h}_{ER}\mathbf{h}_{ER}^H\end{bmatrix}$. To obtain an upper bound for the mutual information at the eavesdropper, we will reduce its noise power by removing $\beta^2\mathbf{h}_{ER}\mathbf{h}_{ER}^H$ from its noise covariance matrix, i.e. the new covariance matrix becomes an identity matrix $\mathbf{I}_{2M}$. Such steps yield the following lower bound of the achievable secrecy rate at high SNR:

$$\mathcal{I}_{1\to 2} \geq \log\left(\frac{1}{4}\min\{|\mathbf{h}_{1^*}|^2, |\mathbf{h}_{2^*}|^2\}\right) - \log\left(\frac{1}{[(\mathbf{H}_E^H\mathbf{H}_E)^{-1}]_{1,1}}\right).$$

The density function of $\frac{1}{\left[(\mathbf{H}_E^H\mathbf{H}_E)^{-1}\right]_{1,1}}$ is still difficult to be found. We first construct two matrices, $\bar{\mathbf{H}}_E = \begin{bmatrix}\mathbf{H}_{E1}^H\mathbf{p}_1 & \mathbf{H}_{E2}^H\mathbf{p}_2 \\ \mathbf{h}_{ER} & \mathbf{h}_{ER}\end{bmatrix}$ and $\tilde{\mathbf{H}}_E = \begin{bmatrix}\mathbf{H}_{E1}^H\mathbf{p}_1 & \mathbf{H}_{E2}^H\mathbf{p}_2 \\ \mathbf{h}_{ER} & \tilde{\mathbf{h}}_{ER}\end{bmatrix}$, where $\tilde{\mathbf{h}}_{ER}$ is an auxiliary Gaussian vector which is independent to $\mathbf{h}_{ER}$. When $M \to \infty$, we observe $\beta|\mathbf{h}_{i^*}| \to \frac{1}{\sqrt{2}}$ and $\beta|\mathbf{g}_{i^*}| \to \frac{1}{\sqrt{2}}$. By using this observation and following similar steps in the proof for Proposition 1, we can obtain $\frac{1}{\left[(\mathbf{H}_E^H\mathbf{H}_E)^{-1}\right]_{1,1}} < \frac{1}{\left[(\bar{\mathbf{H}}_E^H\bar{\mathbf{H}}_E)^{-1}\right]_{1,1}}$ with probability one, when $M \to \infty$. Furthermore, each element of the auxiliary vector $\tilde{\mathbf{h}}_{ER}$ is identically and independent complex Gaussian distributed with zero mean and unit variance. By using Proposition 1, we have $\frac{1}{\left[(\bar{\mathbf{H}}_E^H\bar{\mathbf{H}}_E)^{-1}\right]_{1,1}} < \frac{1}{\left[(\tilde{\mathbf{H}}_E^H\tilde{\mathbf{H}}_E)^{-1}\right]_{1,1}}$ with probability one. With the above arguments, the secrecy rate can be further lower bounded as follows:

$$\begin{aligned}\mathcal{I}_{1\to 2} \geq\ & \log\left(\frac{1}{4}\min\{|\mathbf{h}_{1^*}|^2, |\mathbf{h}_{2^*}|^2\}\right) \qquad (44)\\ & - \log\left(\frac{1}{\left[(\tilde{\mathbf{H}}_E^H\tilde{\mathbf{H}}_E)^{-1}\right]_{1,1}}\right).\end{aligned}$$

where Note that the above bound is obtained by using the assumption $M \to \infty$. The rationale behind this new channel matrix is that $\tilde{\mathbf{H}}_E$ is a classical $2M \times 2$ complex Gaussian matrix, which makes it easy to evaluate the value of $\left[(\tilde{\mathbf{H}}_E^H\tilde{\mathbf{H}}_E)^{-1}\right]_{1,1}$.

The probability to have zero secrecy rates can be upper bounded by

$$P\left(\frac{1}{4}\min\{|\mathbf{h}_{i^*}|^2, |\mathbf{g}_{i^*}|^2\} \leq \frac{1}{\left[(\tilde{\mathbf{H}}_E^H\tilde{\mathbf{H}}_E)^{-1}\right]_{1,1}}\right). \qquad (45)$$

Define $z_i = \min\{|\mathbf{h}_i|^2, |\mathbf{g}_i|^2\}$. Since both $|\mathbf{h}_i|^2$ and $|\mathbf{g}_i|^2$ are independently Chi-square distributed, the probability density function (pdf) of $z_i$ will be $f_{z_i}(x) = \frac{2x^{M-1}}{(M-1)!}e^{-x}\left(1 - \frac{\gamma(M,x)}{(M-1)!}\right)$, where $\gamma(m,x)$ is the incomplete Gamma function. So the cumulative distribution function (CDF) of the largest $z_i$ is $F_{z_{i^*}}(x) = \left(\int_0^\theta \frac{2x^{M-1}}{(M-1)!}e^{-x}\left(1 - \frac{\gamma(M,x)}{(M-1)!}\right)dx\right)^N$, from which its probability density function (pdf) $f_{z_{i^*}}(x)$ can be obtained. On the other hand, as shown in [25], [26], $\frac{1}{\left[(\tilde{\mathbf{H}}_E^H\tilde{\mathbf{H}}_E)^{-1}\right]_{1,1}}$ is also Chi-square distributed with the pdf of $f_e(y) = \frac{y^{2M-2}}{(2M-2)!}e^{-y}$. Therefore the zero secrecy probability is upper bounded as

$$\begin{aligned}P(\mathcal{I}_{1\to 2} < 0) &\leq \int_0^\infty \int_0^{4y} f_{z_{i^*}}(x)dx f_e(y)dy \qquad (46)\\ &= \int_0^\infty F_{z^*}(4y)\frac{y^{2M-2}}{(2M-2)!}e^{-y}dy.\end{aligned}$$

The above integral could be directly evaluated by first applying the series representation of $\gamma(M,x)$, and then using binomial expansion, where the resultant expression is very complicated due to the sum of sums and therefore offers no more insights compared to the original integral.

In the following, the extreme value theory [27], [28] will be used to evaluate the upper bound. Different to [27] the addressed variable is not a simple Chi-square variable, but the minimum of two Chi-square variables. First rewrite the cumulative distributive function (CDF) of $z_i$ as

$$F_{z_i}(\theta) = 1 - (1 - F_\chi(\theta))^2,$$

where $F_\chi(x) = \frac{1}{(M-1)!}\gamma(M,x)$ is the CDF of a Chi-square distribution with $2M$ degrees of freedom. To ensure those extreme value results applicable, it is important to verify that the growth function, defined as $g(x) = \frac{1-F_{z_i}(x)}{f_{z_i}(x)}$, becomes a constant when $x \to \infty$. This is indeed true for the addressed distribution $F_\chi(x)$, as shown in the following

$$g(x) = \frac{1 - \frac{\gamma(M,x)}{(M-1)!}}{\frac{2x^{M-1}}{(M-1)!}e^{-x}} = \frac{e^{-x}\sum_{k=0}^{M-1}\frac{x^k}{k!}}{\frac{2x^{M-1}}{(M-1)!}e^{-x}} \to \frac{1}{2}, \qquad (47)$$

when $x \to \infty$. An interesting observation is that the growth function in the above equation is quite similar to the one shown in [27], although the addressed CDF, $F_{z_i}(\theta)$, is different. Given the existence of the limit of the growth function, we need to find $\theta_N$, the root for the equation $1 - F_{z_i}(\theta_N) = \frac{1}{N}$, which will be used to bound the value of $z_{i^*}$. Such a root can be found as

$$\begin{aligned}\frac{1}{N} &= 1 - F_{z_i}(\theta_N) \qquad (48)\\ &= \left(1 - \frac{\gamma(M,\theta_N)}{(M-1)!}\right)^2 = \left(\frac{\Gamma(M,\theta_N)}{(M-1)!}\right)^2.\end{aligned}$$

Following Eq. 8.357 in [29], we can have

$$\frac{1}{N^{\frac{1}{2}}} = \frac{\Gamma(M,\theta_N)}{(M-1)!} \approx \frac{\theta_N^{M-1}e^{-\theta_N} + O\left(\frac{1}{\theta_N}\right)}{(M-1)!}, \qquad (49)$$

when $\theta_N$ is large. Therefore the solution will be

$$\theta_N = \frac{1}{2}\log N + (M-1)\log\log N^{\frac{1}{2}} + O(\log\log\log N), \qquad (50)$$

which is obtained following Eq. (A9) in [27] by applying the fact of $\log \frac{N^{\frac{1}{2}}}{(M-1)!} \rightarrow \log N^{\frac{1}{2}}$ which is due to $\frac{N}{M} \rightarrow \infty$. By using Corollary A.1 in [27], we can obtain

$$P\left(\frac{1}{2}\log N + (M-2)\log\log N^{\frac{1}{2}} + O(\log\log\log N)\right. \tag{51}$$
$$\left. \leq z_{i^*} \leq \frac{1}{2}\log N + M\log\log N^{\frac{1}{2}} + O(\log\log\log N)\right)$$
$$> 1 - O\left(\frac{1}{\log N}\right),$$

for $M \rightarrow \infty$ and $\frac{N}{M} \rightarrow \infty$. Such extreme value results can be used to bound the zero rate probability as follows. First divide the upper bound of the zero rate probability into two integrals as follows

$$P(\mathcal{I}_{1\rightarrow 2} < 0) \leq \int_0^a F_{z_{i^*}}(4y)\frac{y^{2M-2}}{(2M-2)!}e^{-y}dy + \int_a^\infty F_{z_{i^*}}(4y)\frac{y^{2M-2}}{(2M-2)!}e^{-y}dy,$$

where $a = \frac{1}{2}\log N + (M-2)\log\log N^{\frac{1}{2}} + O(\log\log\log N)$. The first integral can be approximated as

$$\int_0^a F_{z_{i^*}}(4y)\frac{y^{2M-2}}{(2M-2)!}e^{-y}dy \rightarrow O\left(\frac{1}{\log N}\right) \times \int_0^a \frac{y^{2M-2}}{(2M-2)!}e^{-y}dy. \tag{52}$$

Since $\int_0^a \frac{y^{2M-2}}{(2M-2)!}e^{-y}dy \leq 1$, we can have

$$\int_0^a F_{z_{i^*}}(4y)\frac{y^{2M-2}}{(2M-2)!}e^{-y}dy \rightarrow 0, \tag{53}$$

when $N \rightarrow 0$. The second integral can be simplified as

$$\begin{aligned}\int_a^\infty F_{z_{i^*}}(4y)\frac{y^{2M-2}}{(2M-2)!}e^{-y}dy &\leq \int_a^\infty \frac{y^{2M-2}}{(2M-2)!}e^{-y}dy\\ &= e^{-a}\sum_{k=0}^{2M-2}\frac{a^k}{k!} \rightarrow 0,\end{aligned}$$

since $a$ becomes infinity when $N \rightarrow \infty$. So the upper bound of the zero secrecy rate probability becomes zero for $N \rightarrow \infty$, and the lemma is proved. ■

*Proof for Lemma 3 :*To prove the lemma, the lower bound of the eavesdropping data rate shown (10) cannot be use. Instead, the exact expression of the eavesdropping rate needs to be studied. Following the signal mode in (8), the data rate $\mathcal{I}_{1,x}^E$ can be re-written as

$$\mathcal{I}_{1,x}^E = \log\left(1 + \rho\frac{1}{\left[(\breve{\mathbf{H}}_x^H\breve{\mathbf{H}}_x)^{-1}\breve{\mathbf{H}}_x^H\breve{\mathbf{C}}_{n,x}\breve{\mathbf{H}}_x(\breve{\mathbf{H}}_x^H\breve{\mathbf{H}}_x)^{-1}\right]_{1,1}}\right),$$

when the amount of artificial noise is $x$. When $M \rightarrow \infty$, $\beta^2\mathbf{h}_{ER}\mathbf{h}_{ER}^H = \frac{\mathbf{h}_{ER}\mathbf{h}_{ER}^H}{|\mathbf{h}_{i^*}|^2+|\mathbf{g}_{i^*}|^2+\frac{1}{\rho}} \rightarrow \mathbf{I}_M$, which means $\breve{\mathbf{C}}_{n,x} \rightarrow \mathbf{I}_M$. By using such an approximation, the addressed probability can be written as

$$P(\mathcal{I}_{1,x-1}^E > \mathcal{I}_{1,x}^E) \approx P\left(\frac{1}{\left[(\breve{\mathbf{H}}_{x-1}^H\breve{\mathbf{H}}_{x-1})^{-1}\right]_{1,1}} > \frac{1}{\left[(\breve{\mathbf{H}}_x^H\breve{\mathbf{H}}_x)^{-1}\right]_{1,1}}\right).$$

For simplicity, denote the channel matrix as the following form, $\breve{\mathbf{H}}_x = \begin{bmatrix}\mathbf{h} & \mathbf{g}\\ \frac{\mathbf{h}_{ER}}{\sqrt{2}} & \frac{\mathbf{h}_{ER}}{\sqrt{2}}\end{bmatrix}$, where the dimension of $\mathbf{h}$ and $\mathbf{g}$ is $(M-2x)\times 1$, and the approximations $\frac{|\mathbf{h}_{i^*}|^2}{|\mathbf{h}_{i^*}|^2+|\mathbf{g}_{i^*}|^2+\frac{1}{\rho}} \rightarrow \frac{1}{2}$ and $\frac{|\mathbf{g}_{i^*}|^2}{|\mathbf{h}_{i^*}|^2+|\mathbf{g}_{i^*}|^2+\frac{1}{\rho}} \rightarrow \frac{1}{2}$ are used. $\breve{\mathbf{H}}_{x-1}$ is constructed by adding the following row, $\begin{bmatrix}h_x & g_x\end{bmatrix}$, on the top of $\breve{\mathbf{H}}_x$. With such simplified notations, the determinant of $\breve{\mathbf{H}}_x^H\breve{\mathbf{H}}_x$ is

$$\begin{aligned}\det(\breve{\mathbf{H}}_x^H\breve{\mathbf{H}}_x) &= |\mathbf{h}|^2|\mathbf{g}|^2 + \frac{1}{2}|\mathbf{h}_{ER}|^2(|\mathbf{h}|^2+|\mathbf{g}|^2\\ &\quad -\mathbf{h}^H\mathbf{g} - \mathbf{g}^H\mathbf{h}) - |\mathbf{h}^H\mathbf{g}|^2\\ &= |\mathbf{h}|^2|\mathbf{g}|^2 + \frac{1}{2}|\mathbf{h}_{ER}|^2|\mathbf{h}-\mathbf{g}|^2 - |\mathbf{h}^H\mathbf{g}|^2.\end{aligned} \tag{54}$$

And the term $\frac{1}{\left[(\breve{\mathbf{H}}_x^H\breve{\mathbf{H}}_x)^{-1}\right]_{1,1}}$ can be expressed as

$$\frac{1}{\left[(\breve{\mathbf{H}}_x^H\breve{\mathbf{H}}_x)^{-1}\right]_{1,1}} = \frac{|\mathbf{h}|^2|\mathbf{g}|^2 + \frac{1}{2}|\mathbf{h}_{ER}|^2|\mathbf{h}-\mathbf{g}|^2 - |\mathbf{h}^H\mathbf{g}|^2}{|\mathbf{g}|^2 + \frac{1}{2}|\mathbf{h}_{ER}|^2}. \tag{55}$$

To proof the lemma, it is equivalent to show that increasing $x$ will decrease the value of $\frac{1}{\left[(\breve{\mathbf{H}}_x^H\breve{\mathbf{H}}_x)^{-1}\right]_{1,1}}$. With a fixed $x$ and $M \rightarrow \infty$, both $M$ and $M-2x$ become infinity. Therefore it is straightforward to show that $|\mathbf{h}_{ER}|^2 \rightarrow M$, $|\mathbf{h}|^2 \rightarrow (M-2x)$, and $|\mathbf{g}|^2 \rightarrow (M-2x)$. Furthermore, to find the approximation of $|\mathbf{h}-\mathbf{g}|^2$, denote the $n$-th element of $\mathbf{h}$ as $h_n$, and $g_n$ is defined similarly. It is easy to show that $h_n - g_n$ is still complex Gaussian distributed with zero mean and variance 2, which means $|h_n - g_n|^2$ is exponentially distributed with the parameter $\frac{1}{2}$. Applying the large number theorem, we can find $|\mathbf{h}-\mathbf{g}|^2 \rightarrow \frac{M-x}{2}$. Following similar arguments, we can have $\frac{\mathbf{h}^H\mathbf{g}}{M-2x} \rightarrow 0$. Therefore we can find the term shown in (55) can be approximated as

$$\frac{1}{\left[(\breve{\mathbf{H}}_x^H\breve{\mathbf{H}}_x)^{-1}\right]_{1,1}} \rightarrow \frac{(M-2x)^2 + \frac{M}{4}(M-x)}{\frac{3}{2}M - 2x}. \tag{56}$$

It is straightforward to show that the right side of (56) is an decreasing function of $x$, with a fixed $x$ and $M \rightarrow \infty$. And the proof for the lemma is completed. ■

*Justification to remove the observations from the first time slot:* According to the signal model in (7), the sum rate available at the eavesdropper is

$$\mathcal{I}_{E,sum} = \log\det\left(\mathbf{I}_{2M} + \bar{\mathbf{H}}\bar{\mathbf{H}}^H\bar{\mathbf{C}}_n^{-1}\right). \tag{57}$$

where $\bar{\mathbf{H}} = \begin{bmatrix}\mathbf{H}_{E,1}^H\mathbf{p}_1 & \mathbf{H}_{E,2}^H\mathbf{p}_2\\ \beta\mathbf{h}_{E,R}h_1^* & \beta\mathbf{h}_{E,R}h_2^*\end{bmatrix}$ and the noise-interference covariance matrix is $\bar{\mathbf{C}}_n = diag[\mathbf{H}_{E,1}^H\mathbf{P}_1\mathbf{P}_1^H\mathbf{H}_{E,1} + \mathbf{H}_{E,2}^H\mathbf{P}_2\mathbf{P}_2^H\mathbf{H}_{E,2} + \frac{1}{\rho}\mathbf{I}_M, \frac{1}{\rho}\mathbf{I}_M + \frac{\beta^2}{\rho}\mathbf{h}_{ER}\mathbf{h}_{ER}^H]$. Rewrite the sum rate as shown in (58), where $\bar{\mathbf{C}}_n = \frac{1}{\rho}\mathbf{I}_M + \frac{\beta^2}{\rho}\mathbf{h}_{ER}\mathbf{h}_{ER}^H$ and $\bar{\mathbf{H}} = \begin{bmatrix}\hat{\mathbf{H}}_1^H & \hat{\mathbf{H}}^H\end{bmatrix}^H$. At high SNR, we can have the approximation shown in (59). The first factor is a constant not a function of $\rho$, and the second term can be expressed as in (60). For a large $M$ and $N$, we can have $\frac{\mathbf{h}_{ER}\mathbf{h}_{ER}^H}{|\mathbf{h}_{i^*}|^2+|\mathbf{g}_{i^*}|^2+\frac{1}{\rho}} \rightarrow 0$ and the factor can be approximated as

$$\mathcal{I}_{E,sum} = \log\det\left(\mathbf{I}_4 + \begin{bmatrix} \hat{\mathbf{H}}_1^H\left(\mathbf{H}_{E,1}^H\mathbf{P}_1\mathbf{P}_1^H\mathbf{H}_{E,1} + \mathbf{H}_{E,2}^H\mathbf{P}_2\mathbf{P}_2^H\mathbf{H}_{E,2} + \frac{1}{\rho}\mathbf{I}_M\right)^{-1}\hat{\mathbf{H}}_1 & \mathbf{0}_{2\times 2} \\ \mathbf{0}_{2\times 2} & \hat{\mathbf{H}}^H\bar{\mathbf{C}}_n^{-1}\hat{\mathbf{H}} \end{bmatrix}\right). \tag{58}$$

$$\begin{aligned} \mathcal{I}_{E,sum} &\approx \log\det\left(\mathbf{I}_4 + \begin{bmatrix} \hat{\mathbf{H}}_1^H\left(\mathbf{H}_{E,1}^H\mathbf{P}_1\mathbf{P}_1^H\mathbf{H}_{E,1} + \mathbf{H}_{E,2}^H\mathbf{P}_2\mathbf{P}_2^H\mathbf{H}_{E,2}\right)^{-1}\hat{\mathbf{H}}_1 & \mathbf{0}_{2\times 2} \\ \mathbf{0}_{2\times 2} & \hat{\mathbf{H}}^H\bar{\mathbf{C}}_n^{-1}\hat{\mathbf{H}} \end{bmatrix}\right) \\ &= \log\det\left(\mathbf{I}_2 + \hat{\mathbf{H}}_1^H\left(\mathbf{H}_{E,1}^H\mathbf{P}_1\mathbf{P}_1^H\mathbf{H}_{E,1} + \mathbf{H}_{E,2}^H\mathbf{P}_2\mathbf{P}_2^H\mathbf{H}_{E,2}\right)^{-1}\hat{\mathbf{H}}_1\right) + \log\det\left(\mathbf{I}_2 + \hat{\mathbf{H}}^H\bar{\mathbf{C}}_n^{-1}\hat{\mathbf{H}}\right). \end{aligned} \tag{59}$$

$$\begin{aligned} \log\det\left(\mathbf{I}_2 + \hat{\mathbf{H}}^H\bar{\mathbf{C}}_n\hat{\mathbf{H}}\right) &= \log\det\left(\mathbf{I}_2 + \hat{\mathbf{H}}^H\left(\frac{1}{\rho}\mathbf{I}_M + \frac{\beta^2}{\rho}\mathbf{h}_{ER}\mathbf{h}_{ER}^H\right)^{-1}\hat{\mathbf{H}}\right) \\ &= \log\det\left(\mathbf{I}_M + \rho\hat{\mathbf{H}}^H\left(\mathbf{I}_M + \frac{\mathbf{h}_{ER}\mathbf{h}_{ER}^H}{|\mathbf{h}_{i^*}|^2 + |\mathbf{g}_{i^*}|^2 + \frac{1}{\rho}}\right)^{-1}\hat{\mathbf{H}}\right). \end{aligned} \tag{60}$$

$$\log\det\left(\mathbf{I}_2 + \hat{\mathbf{H}}^H\bar{\mathbf{C}}_n\hat{\mathbf{H}}\right) = \log\det\left(\mathbf{I}_2 + \rho\hat{\mathbf{H}}^H\hat{\mathbf{H}}\right) \rightarrow \infty, \tag{61}$$

at high SNR. So the second factor is dominant in the sum rate, which is the reason to only consider the observations from the second time slot. ■

## References

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 8, pp. 1355–1387, 1975.

[2] M. Bloch, J. Barros, M. R. D. Rodriques, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2515–2534, June 2008.

[3] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4687–4698, Oct. 2008.

[4] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4005–4019, Sept. 2008.

[5] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2735–2751, June 2008.

[6] Y. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[7] Y. Liang, H. V. Poor, and S. Shamai (Shitz), *Information Theoretic Security*. Foundations and Trend in Commun. and Inform. Theory, vol. 5, nos. 4–5, pp 355–580. Now Publishers, 2008.

[8] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[9] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 10, pp. 2067–2076, Dec. 2011.

[10] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans Inf. Forensics Security*, vol. 7, pp. 310–320, Feb. 2012.

[11] Z. Ding, K. Leung, D. L. Goeckel, and D. Towsley, "Opportunistic relaying for secrecy commun.: cooperative jamming vs relay chatting," *IEEE Trans. Wireless Commun.*, vol. 10, pp. 1725–1729, June 2011.

[12] J. Huang and A. Swindlehurst, "Cooperative jamming for secure commun. in MIMO relay networks," *IEEE Trans Signal Process*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[13] Z. Ding, M. Peng, and H. Chen, "A general relaying transmission protocol for MIMO secrecy communications," *IEEE Trans Commun.*, vol. 60, no. 11, pp. 3461–3471, 2012.

[14] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3693–3704, 2012.

[15] A. Gorokhov, D. Gore, and A. Paulraj, "Receive antenna selection for MIMO flat-fading channels: theory and algorithms," *IEEE Trans Inf. Theory*, vol. 49, no. 10, pp. 2687–2696, Oct. 2003.

[16] A. F. Molisch and M. Z. Win, "MIMO systems with antenna selection," *IEEE Microwave Mag.*, vol. 5, no. 1, pp. 45–46, Jan. 2004.

[17] S. Sanayei and A. Nosratinia, "Antenna selection in MIMO systems," *IEEE Commun. Mag.*, vol. 42, no. 10, pp. 68–73, 2004.

[18] R. Cao, T. Lv, H. Gao, S. Yang, and J. Cioffi, "Achieving full diversity in multi-antenna two-way relay networks via symbol-based physical-layer network coding," *IEEE Trans. Wireless Commun.*, vol. 12, no. 7, pp. 3445–3457, 2013.

[19] H. Gao, T. Lv, S. Zhang, C. Yuen, and S. Yang, "Zero-forcing based MIMO two-way relay with relay antenna selection: transmission scheme and diversity analysis," *IEEE Trans. Wireless Commun.*, vol. 11, no. 12, pp. 4426–4437, 2012.

[20] N. Yang, P. Yeoh, M. Elkashlan, R. Schober, and J. Yuan, "MIMO wiretap channels: secure transmission using transmit antenna selection and receive generalized selection combining," *IEEE Commun. Lett.*, no. 99, pp. 1–4, 2013.

[21] I. Krikidis, J. Thompson, S. McLaughlin, and N. Goertz, "Max-min relay selection for legacy amplify-and-forward systems with interference," *IEEE Trans. Wireless Commun.*, vol. 51, pp. 3016–3027, June 2009.

[22] A. Bletsas, H. Shin, and M. Win, "Cooperative communications with outage-optimal opportunistic relaying," *IEEE Trans. Wireless Commun.*, vol. 6, no. 9, pp. 3450–3460, 2007.

[23] A. Edelman, "Eigenvalues and condition numbers of random matrices," Ph.D. dissertation, Massachusetts Institute of Technology, 1989.

[24] Z. Ding and H. V. Poor, "The use of spatially random base stations in cloud radio access networks," *IEEE Signal Process. Lett.*, to appear. Preprint available: http://www.staff.ncl.ac.uk/z.ding/CRANdraft.pdf.

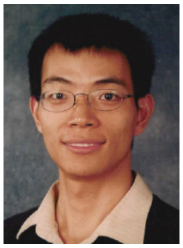
[25] M. Rupp, C. Mecklenbrauker, and G. Gritsch, "High diversity with simple space time block codes and linear receivers," in *Proc. 2003 IEEE Global Commun. Conf.*, vol. 2, pp. 302–306.

[26] Z. Ding, M. Zheng, and K. Leung, "Impact of network coding on system delay for multisource—multidestination scenarios," *IEEE Trans. Veh. Technol.*, vol. 59, pp. 831–841, Feb. 2010.

[27] M. Sharif and B. Hassibi, "On the capacity of MIMO broadcast channels with partial side information," *IEEE Trans. Inf. Theory*, vol. 51, no. 2, pp. 506–522, Feb. 2005.

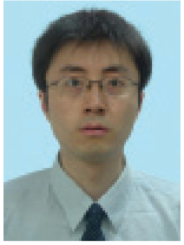
[28] H. A. David and H. N. Nagaraja, *Order Statistics*, 3rd ed. John Wiley, 2003.

[29] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 6th ed. Academic Press, 2000.



**Zhiguo Ding** (S'03-M'05) received his B.Eng in Electrical Engineering from the Beijing University of Posts and Telecommunications in 2000, and the Ph.D degree in Electrical Engineering from Imperial College London in 2005. From Jul. 2005 to Jun. 2010, he was working in Queens University Belfast, Imperial College and Lancaster University. Since Oct. 2010, he has been with Newcastle University, currently as a Reader.

Dr Dings research interests are game theory, cooperative and energy harvesting networks and statistical signal processing. He was Co-chair for the WCNC-2013 Workshop on New Advances for Physical Layer Network Coding, and is serving as an Editor for IEEE WIRELESS COMMUNICATION LETTERS, IEEE COMMUNICATIONS LETTERS, and *Journal of Wireless Communications and Mobile Computing*. He received the best paper award at the IET Comm. Conf. on Wireless, Mobile and Computing, 2009, IEEE COMMUNICATIONS LETTERS Exemplary Reviewer 2012, and the EU Marie Curie Fellowship 2012-2014.



**Zheng Ma** received his Bsc and PhD degree in communications and information system in 2000 and 2006 respectively from Southwest Jiaotong University. Dr. Ma was a visiting scholar of University of Leeds, University of Hull and St.Martin College in UK in 2003. In 2003 and 2005, he was a visiting scholar in Hong Kong University of Science and Technology. From 2008, he is a visiting research fellow in department of communication systems, Lancaster university, United Kingdom. He is currently a professor in Southwest Jiaotong University. Dr Mas research interests include: information theory & coding, signal design & applications, FPGA/DSP Implementation, and professional mobile radio (PMR). He has published more than twenty research papers in high quality journals and conferences such as IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, and IEEE COMMUNICATIONS LETTERS, etc.

**Pingzhi Fan** received his M.S. degree in Computer Science from the Southwest Jiaotong University, PRC, in 1987, and Ph.D. degree in Electronic Engineering from the Hull University, U.K., in 1994. He is currently a professor and director of the institute of mobile communications, Southwest Jiaotong University, PRC. He also serves as a chief scientist of China 973 program, a guest professor of Leeds University, UK (1997-), and a guest professor Shanghai Jiaotong University (1999-). He was a recipient of the UK ORS Award (1992), and the NSFC Outstanding Young Scientist Award (1998). He is the inventor of 22 patents, and the author of over 350 research papers and eight books, including six books published by John Wiley & Sons Ltd, RSP (1996), IEEE Press (2003, 2006) and Springer (2004) and Nova Science (2007), respectively. His research interests include high mobility wireless communications, spread-spectrum and CDMA techniques, information theory & coding, etc.