REVISION SUMMARY REPORT

"Artificial Noisy MIMO Systems under Correlated Scattering Rayleigh Fading – A Physical Layer Security Approach"

(ISJ-RE-18-07334)

Dear Editor and Anonymous Reviewers:

We appreciate your time and effort to review our paper. Based on your suggestions, we have addressed all of your comments carefully. We believe that the quality of this paper has been improved by incorporating these changes. The corresponding changes and refinements we have made are summarized in the following paragraphs. For easy cross-reference, the reviewers' comments are marked in blue, our responses in black, and the changes made in the revised manuscript are highlighted in violet. Note that the reference numbers in this reply refer to the reference list in the revised manuscript, unless stated otherwise. Many thanks!

Authors: Yiliang Liu, Hsiao-Hwa Chen, Liangmin Wang, and Weixiao Meng

Date: March 14, 2019

AUTHORS' RESPONSES TO REVIEWER 1

The comments from Reviewer 1 can be divided into seven specific problems, and the detailed response is given as follows.

1. Reviewer's Comment:

Are the analytical and simulation results exact matching?

Authors' Responses:

Yes, the analytical results are consistent with the simulations.

At first, the exact theoretical results with Eqn. (20) are in a good agreement with the Monte Carlo simulations (10^5 independent runs) on Eqn. (10), as shown in all simulation figures. Eqn. (20) is the lower bound of the real ergodic secrecy rate, while Eqn. (10) is the

real ergodic secrecy rate. There are little difference between real ergodic secrecy rates and values from Eqn. (20), because AN signals make C_m be much larger than C_w with a high probability. As shown in Fig. R1. The 10^5 independent Monte Carlo simulations of Eqn. (10) for each curve indicate that C_m is smaller than C_w in only 662 runs among the total simulations of these four curves.

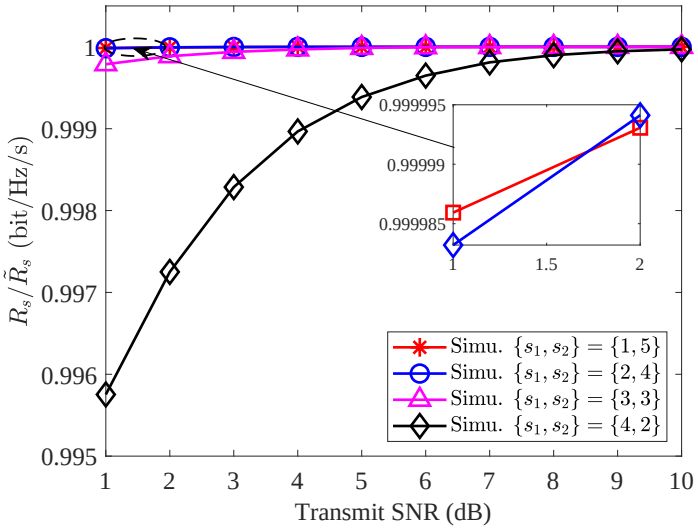

Fig. R1. The ratio between lower bound of ergodic secrecy rates, i.e., R_s, as shown in Eqn. (14) and the true ergodic secrecy rates, i.e., $\tilde{R}$, as shown in Eqn. (10).

Secondly, the approximate analytical results in TABLE I are consistent with simulation results, as shown in the trends of curves of Figs. 2-6 in the revised manuscript.

Due to the page limit of the IEEE System Journal, this test is only shown in the revision summary and https://github.com/yiliangliu1990/liugit_pub.

2. Reviewer's Comment:

The results should be obtained for the high value of SNR.

Authors' Responses:

Many thanks for the comment. We have added the simulation where the SNR is ranged from 30 to 60 dB. Without loss of generality, we find the ergodic secrecy rate grows lineally with SNR at high SNR regions, which is consistent with the result in our previous work [14] (The ergodic secrecy rate grows logarithmically with transmit power.). Specifically, we

have added the simulation figure, i.e., Fig. 2(b), in Section IV, on the page 7 of the revised manuscript.

3. Reviewer's Comment:

Why the plot of ergodic secrecy rate with $s_1 = 2$, is crossing the plot of ergodic secrecy at $s_1 = 3$ at a point of SNR.

Authors' Responses:

The crossing point is existed, because when SNR is low, the $s_1 = 2$ has a better performance than $s_1 = 3$, but in the high SNR regions, $s_1 = 3$ has a better performance. It means that the transmitter should use more eigen-subchannels to transmit messages in high SNR regions, whereas the transmitter should allocate eigen-subchannels of smaller eigenvalues to transmit AN signals in low SNR regions, which is consistent with Theorem 5 in our previous work [14] even if the investigation did not consider the correlation. We have explained this point in the 3rd paragraph of Section IV, on the page 6, 2nd column of the revised manuscript. Specifically, the added content is copied as follow.

"As shown in Fig. 2(a), the achievable ergodic secrecy rates increase almost exponentially with SNR, and $s_1 = 2$ is the best choice when SNR$<$ 16. There exists a crossing point between $s_1 = 2$ and $s_1 = 3$, because $s_1 = 3$ will have a better performance with increasing SNR, which is consistent with [14, Th. 5]."

4. Reviewer's Comment:

In Fig. 3, 4, the Goel scheme is outperforming the other considered cases except for $s_1 = 3$. Why?

Authors' Responses:

According to the Reviewer 2's comment, we replaced the "Goel scheme" by "$\{s_1, s_2\} = \{4, 2\}$" in all simulation figures because the our comparison is actually among the different numbers of eigen-subchannels for messages, whereas "Goel scheme" is a general AN scheme and not suitable for the name of comparisons.

We think the comment in Figs. 3 and 4 is: 1) why $s_1 = 3$ has the best performance? 2) why $s_1 = 4$ is outperforming the other schemes ($s_1 = 1$ and $s_1 = 2$)?

1) Why $s_1 = 3$ has the best performance?

Our previous conclusion in [14] shows that the ergodic secrecy rate will be improved if

always allocating eigen-subchannels of smallest gains (λ_4) for AN signals and allocating eigen-subchannels of larger gains (λ_1, λ_2, and λ_3) for messages, so $s_1 = 3$ has the better performance than $s_1 = 4$ that allocates all eigen-subchannels for messages. The conclusion is also consistent with the correlated fading scenarios as the λ_4 is too small whatever the degree of correlation. For the security purpose, if we use the eigen-subchannel of λ_4 for sending AN signals. The power of AN signals from Eve's perspective maybe large, thus, reducing wiretap rates with a large level.

2) Why $s_1 = 4$ is outperforming the other schemes?

As shown in Fig 3, $s_1 = 4$ is outperforming the other schemes ($s_1 = 1$ and $s_1 = 2$) only when the number of antennas at Bob is large enough. When the Bob has a lot of receive antennas, it can enlarge the channel gains, i.e., λ_1, λ_2, λ_3, and λ_4, of the message streams because Bob has enough antennas to decode them and gather the received power of each antennas. In this case, the channel gains of the third and forth eigen-suchannel (the eigen-suchannels of λ_3 and λ_4) will become larger, so if we use the eigen-suchannels of λ_3 and λ_4 to transmit AN signals and use the eigen-suchannels of λ_1 and λ_2 to transmit messages ($s_1 = 2$ and $s_2 = 2$), the secrecy rate will be smaller than using the all eigen-suchannels to transmit messages as all eigen-suchannels have large channel gains.

Fig. 4(a) has similar reason that the channel gains of the third and forth eigen-suchannel (the eigen-suchannels of λ_3 and λ_4) will become larger with increasing the antenna distance of Bob based on the characteristic of the eigenvalues of $\mathbf{W} \sim W_4(6, \mathbf{0}_4, \mathbf{R}_4)$.

5. Reviewer's Comment:

Why the author has assumed the channel through Rayleigh fading? Justify and can we use some other distribution for it?

Authors' Responses:

In this manuscript, our channel is based on the Rayleigh fading model. Rayleigh fading is a reasonable model for heavily built-up urban environments with many enough scattering, without dominant propagation along a line of sight between the transmitter and receiver.

The proposed scheme can be used in other fading model, such Rician and Nakagami. Recently, we find [14] has been extended to Rician fading channels via a non-central Wishart matrix in Ahmed's research [15]. However, it is mathematically nontrivial to derive the distributions of the Wishart matrix with correlation. Our work in this manuscript is to

extend the scheme in [14] to the correlated Rayleigh fading model. We have explained this point in the second paragraph of Section I, on the page 1, 2 column of the revised manuscript, which is copied as follow.

"The work in [14] was done based on a Rayleigh fading channel, as Rayleigh fading is a reasonable model for heavily built-up urban environments [12]. which has been extended to uncorrelated Rician fading channels via a non-central Wishart matrix in Ahmed's research [15]. "

6. Reviewer's Comment:

Is the amount of secrecy rate that we are getting in each case is sufficient to run the system?

Authors' Responses:

We only consider a general system model with a transmitter, a receiver, and an eavesdroppers, and analyze the achievable secrecy rate that is respect to bandwidth and time (bit/Hz/s). Our contribution is that, in this general model, if a system designer use the appropriate number of message streams and AN streams, and adjust the MIMO correlation via changing antenna distance in the manufacturing process or selecting appropriate device development based on angles of arrival (AoA) and receive angle spread (RAS), the secrecy rate will be improved. If considering real scenarios, this scheme can be easily extended into frequency and time systems, and the secrecy rate will be enlarged via allocating more frequency and time resources to the general model.

7. Reviewer's Comment:

Through some light on the motivation and novelty of the work.

Authors' Responses:

Many thanks for this comment.

At first, most of the AN schemes assumed the presence of uncorrelated fading in MIMO channels. Unfortunately, in most real applications, the correlation among antennas may exist due to poor-scattering environments or small spacing between antenna elements, as shown in 3GPP standard [17] and traditional MIMO research [24]-[26], [32], [33], [35]. It motivates us to study AN schemes in correlated fading environments.

Secondly, there are two mathematical challenges when considering receiver-side correlation

for AN schemes, including the properties of the correlated matrices in terms of spatial correlation parameters, and exact and simple expression for marginal probability density function (pdf) of the kth eigenvalues of receiver-side correlated Wishart matrices. This work provides some contributions on the basic mathematical investigations, which can be used for analyzing both ergodic secrecy rates of an AN scheme and channel capacities of traditional MIMO systems.

We have highlighted the motivation and novelty of the work in the 4-5 paragraphs of Section I, on the page 1, 2 column of the revised manuscript.

AUTHORS' RESPONSES TO REVIEWER 2

The comments from Reviewer 2 can be divided into seven specific problems, and the detailed response is given as follows.

1. Reviewer's Comment:

This paper is not much changed compared to their previous paper [9], which limits their contribution and innovation. Do they want to write another article that considers double-side correlation? According to their writing ideas, it is easy to draw a number of papers on this topic.

Authors' Responses:

Thanks for your comment. The main idea of this manuscript is to investigate the effect of spatial correlation in MIMO channels on the secure transmission design, which is an extension of [9] ([14] in the current version). However, such extension is nontrivial due to the following reasons:

At first, there is no appropriate research to describe the properties of the receiver-correlated matrix $\mathbf{R}_a$ in terms of AoA, RAS, and antenna distance, but it is useful for approximate analysis of ergodic secrecy rates. We use Theorem 1 to specify the properties of the correlated matrix $\mathbf{R}_a$ that can be used to deduce approximate analysis of ergodic secrecy rates in TABLE I.

Secondly, the properties of $\mathbf{H}_e\mathbf{F}\mathbf{F}^\dagger\mathbf{H}_e^\dagger$ is the mathematical challenge if $\mathbf{H}_e$ has receiver-side correlation. In traditional MIMO capacity research, the Wishart matrix usually focuses on $\mathbf{H}\mathbf{H}^\dagger$ form (or $\mathbf{H}^\dagger\mathbf{H}$), while in AN-aided MIMO, the Wishart matrix has $\mathbf{H}\mathbf{H}^\dagger$ and $\mathbf{H}_e\mathbf{F}\mathbf{F}^\dagger\mathbf{H}_e^\dagger$ forms, where $\mathbf{F}$ is an independent unitary matrix. It is hard to deduce the wiretap channel capacity via existing research of Wishart matrices. Hence, we provide the distribution formulation of $\mathbf{H}_e\mathbf{F}$ with receiver-side correlation in Theorem 2, and its simple and exact pdf functions of $\mathbf{H}_e\mathbf{F}\mathbf{F}^\dagger\mathbf{H}_e^\dagger$ in Theorem 3.

However, Theorems 2 and 3 are not appropriate for transmit-side correlation or double-side correlation. Hence, we are working on transmit-side correlation or double-side correlation in my thesis.

2. Reviewer's Comment:

This paper is untenable on the model. For MIMO systems, it is not practical to model the channels by considering only the correlation of one side, e.g., receiver-side correlation.

The assumption is unreasonable that there is correlation between the antennas on one side and no correlation on the other side. Reference [10] only considered receiver-side correlation, because their system is MISO-based system. It is recommended that the authors of this paper change receiver-side to double-side.

Authors' Responses:

We agree with the reviewer that double-side correlated MIMO is more general than one-side considerations. However, 3GPP standard [17, TABLE 4.2] provides reference values of the correlation scenarios in donwlinks when antenna distance at BS is large enough so that the correlation at BS side can be ignored for simplifying the analysis, while receiver-side correlation is considered at cellular users side because the short antenna distance or the poor scattering condition. Note that the single side correlation (only transmitter- or receiver-side correlation) to simplify the performance analysis of MIMO capacity is a common method in traditional MIMO research, such as in [R1]-[R7]. In this paper, we investigate the effect of receiver-side correlation on the achievable secrecy rate, which has not been considered before. We have highlighted the difference and contributions in the 4-5 paragraph of the introduction part.

[R1] L. G. Ordonez, D. P. Palomar, and J. R. Fonollosa, "Ordered eigenvalues of a general class of Hermitian random matrices with application to the performance analysis of MIMO systems," IEEE Trans. Signal Process., vol. 57, no. 2, pp. 672–689, 2009.

[R2] P. J. Smith, S. Roy, and M. Shafi, "Capacity of MIMO systems with semicorrelated flat fading," IEEE Trans. Inf. Theory, vol. 49, no. 10, pp. 2781–2788, Oct 2003.

[R3] M. Chiani, M. Z. Win, and A. Zanella, "On the capacity of spatially correlated MIMO Rayleigh-fading channels," IEEE Trans. Inf. Theory, vol. 49, no. 10, pp. 2363–2371, Oct 2003.

[R4] A. Zanella, M. Chiani, and M. Z. Win, "On the marginal distribution of the eigenvalues of Wishart matrices," IEEE Trans. Commun., vol. 57, no. 4, pp. 1050–1060, 2009.

[R5] T. Ratnarajah, "Topics in complex random matrices and information theory," Master's thesis, Mathematics and Statistics of University of Ottawa, May 2003.

[R6] Q. T. Zhang, X. W. Cui and X. M. Li, "Very tight capacity bounds for MIMO-correlated Rayleigh-fading channels," in IEEE Trans. Wireless Commun., vol. 4, no. 2, pp.

681-688, March 2005.

[R7] X. W. Cui, Q. T. Zhang and Z. M. Feng, "Generic procedure for tightly bounding the capacity of MIMO correlated Rician fading channels," in IEEE Trans. Commun., vol. 53, no. 5, pp. 890-898, May 2005.

3. Reviewer's Comment:

Zero-forcing beamforming is a very common method, but the authors do not fully explain it. Although they cite their own published paper [9], the published paper is also wrong. With the assumption that Eve know $\mathbf{H}$ and $\mathbf{B}$, if it is guaranteed that Eve cannot eliminate the AN signal, then t must be greater than e. In [9], the authors gave such an explanation that Eve can eliminate the AN signal by $\mathbf{y} = [\mathbf{HB}]^{\dagger}\mathbf{H}\mathbf{H}_e^{-1}\mathbf{y}_e$. However, this is completely wrong, because $\mathbf{H}_e$ is not a square matrix in the case of $t < e$, i.e., the inverse matrix of $\mathbf{H}_e$ does not exist. Therefore, it is necessary to introduce a concept that the author does not know, the generalized inverse matrix. Eve can eliminate the AN signal by $\mathbf{y} = [\mathbf{HB}]^{\dagger}(\mathbf{H}_e^{\dagger}\mathbf{H}_e)^{-1}\mathbf{H}_e^{\dagger}\mathbf{y}_e$. It is recommended that the authors find relevant references for verification of my comments.

Authors' Responses:

Sorry for our mistakes, and we are agree with you that Eve can can eliminate the AN signal by $[\mathbf{HB}]^{\dagger}(\mathbf{H}_e^{\dagger}\mathbf{H}_e)^{-1}\mathbf{H}_e^{\dagger}\mathbf{y}_e$ when $t < e$.

Secondly, we think your comment on the "zero-forcing" is about Eqn. (9), as a receiver design, on the page 4, 1st column as follow,

$$\tilde{\mathbf{y}} = [\mathbf{HB}]^{\dagger}\mathbf{y} = \mathbf{\Lambda}_{s_1}\mathbf{x} + \tilde{\mathbf{n}}, \tag{9}$$

where $\mathbf{\Lambda}_{s_1} \in \mathbb{R}^{s_1 \times s_1}$ is a diagonal matrix formed by the first to the s_1th eigenvalues of $\mathbf{H}^{\dagger}\mathbf{H}$, and $\mathbf{x}$ is the transmitted signal. We do not use the traditional zero-forcing form $(\mathbf{H}^{\dagger}\mathbf{H})^{-1}\mathbf{H}^{\dagger}$ to eliminate the interference between antennas due to the limitation of $t > r$ [R8]. And we use $[\mathbf{HB}]^{\dagger}$ to eliminate the interference among antennas and AN-incurred interference, simultaneously, as shown in Eqn. (9).

Here, we provide a simple proof of Eqn. (9).

Proof: We have

$$\begin{aligned}[\mathbf{HB}]^{\dagger}\mathbf{HB} &= \mathbf{B}^{\dagger}\mathbf{H}^{\dagger}\mathbf{HB} \\ &= \mathbf{B}^{\dagger}\mathbf{U}\mathbf{\Lambda}\mathbf{U}^{\dagger}\mathbf{B},\end{aligned} \tag{R1}$$

where $\mathbf{\Lambda} \in \mathbb{R}^{t\times t}$ is a diagonal matrix, $\mathbf{U} \in \mathbb{C}^{t\times t}$ and $\mathbf{U}^{\dagger} \in \mathbb{C}^{t\times t}$ are unitary matrices. Since the $t \times s_1$ matrix $\mathbf{B} = [\mathbf{U}]_{(1\sim t),(1\sim s_1)}$ denotes a sub-matrix of $\mathbf{U}$, including the first to the tth rows and the first to the s_1th columns of $\mathbf{U}$, according to the property of a unitary matrix, different columns of $\mathbf{U}$ are complex orthogonal with each other such that

$$[[\mathbf{U}]_{(1\sim t),j}]^{\dagger}[\mathbf{U}]_{(1\sim t),i} = 0, \quad j \neq i, \tag{R2}$$

and $[[\mathbf{U}]_{(1\sim t),i}]^{\dagger}[\mathbf{U}]_{(1\sim t),i} = 1$. Then, we have $\mathbf{B}^{\dagger} = [[\mathbf{U}]_{(1\sim t),(1\sim s_1)}]^{\dagger}$, and get a $s_1 \times t$ matrix as

$$\begin{aligned} \mathbf{B}^{\dagger}\mathbf{U}\mathbf{\Lambda} &= [\mathbf{I}_{s_1}; \mathbf{0}_{s_1\times s_2}]\mathbf{\Lambda} \\ &= [\mathbf{\Lambda}_{s_1}; \mathbf{0}_{s_1\times s_2}], \end{aligned} \tag{R3}$$

where $\mathbf{I}_{s_1}$ is a $s_1 \times s_1$ identity matrix, $\mathbf{0}_{s_1\times s_2}$ is a $s_1 \times s_2$ zero matrix, $\mathbf{\Lambda}_{s_1} \in \mathbb{R}^{s_1\times s_1}$ is a diagonal matrix formed by the first to the s_1th eigenvalues of $\mathbf{H}^{\dagger}\mathbf{H}$. Similarly, we have a $t \times s_2$ matrix

$$\mathbf{U}^{\dagger}\mathbf{B} = \begin{bmatrix} \mathbf{I}_{s_1} \\ \mathbf{0}_{s_1\times s_2} \end{bmatrix}. \tag{R4}$$

Obviously, we get

$$\begin{aligned} [\mathbf{HB}]^{\dagger}\mathbf{HB} &= [\mathbf{\Lambda}_{s_1}; \mathbf{0}_{s_1\times s_2}] \times \begin{bmatrix} \mathbf{I}_{s_1} \\ \mathbf{0}_{s_1\times s_2} \end{bmatrix} \\ &= \mathbf{\Lambda}_{s_1}. \end{aligned} \tag{R5}$$

$[\mathbf{HB}]^{\dagger}\mathbf{HZ} = \mathbf{0}$ is proved in [14, Le. 1].

The proof is completed. ■

The proof is shown in https://github.com/yiliangliu1990/liugit_pub.

[R8] C. -J. Chen, and L. C. Wang, "Performance analysis of scheduling in multiuser MIMO systems with zero-forcing receivers." IEEE J. Selected Areas in Commun. vol. 25, no. 7, pp. 1435-1445, 2007.

4. Reviewer's Comment:

As commented 2, the author's scheme is only valid when Eve's antenna number e is less than the transmitter's antenna number t, which limits its practicality. In practice, it is not always guaranteed that $t > e$.

Authors' Responses:

We agree with the reviewer that the scheme is only valid when the number of Eve's antennas e is less than that of transmitter's antennas t, which is also the fundamental drawback of the AN schemes without Eve's CSI . If $t < e$, the Eve is much more powerful than Bob, and thus the AN schemes may not be applicable. At the moment, researchers only focus on the case $t > e$ to optimize the transmission strategy to optimize the secrecy rate, such as [6-13], and the secure transmission design for $t < e$ still remains an open problem that deserves more research efforts in the future.

5. Reviewer's Comment:

The language of this paper is not refined enough and there is too much nonsense. For example, the so-called "Eigen-subchannel Allocation Algorithm" is actually an ergodic process to find the maximum value, which does not need to be expressed so complicated. It only needs a brief introduction of how to find the maximum, and does not need a specific solution process.

Authors' Responses:

We have removed the eigen-subchannel allocation algorithm, and briefly introduce how to find the maximum value in Remark 2 of Section III, on page 5, 1st column of the revised manuscript. Specifically, we have added the following content.

"Remark 2: We can use Eqn. (20), as a theoretical ergodic secrecy rate expression of Eqn. (14), to maximize the ergodic secrecy rates via a one-dimensional search, which takes the number of eigen-subchannels of message streams, i.e., s_1, as the search direction. Although the results from the search are not globally optimal and the achieved ergodic secrecy rates are the lower bounds of ergodic secrecy capacities, the search with its complexity $O(n)$ avoids complicated convex optimization processes. "

6. Reviewer's Comment:

I wonder if the channel of "Goel scheme" reported in [6] and [7] is the same as that in this paper. If not, how to compare the performance? The author should explain it further. For example, whether there is correlation of the channel in "Goel scheme".

Authors' Responses:

Many thanks for this comment. The channel of "Goel scheme" reported in [6] and [7]

are not the same with ours, where [6] that assumed a MISO system, and [7] assumed a MIMO system. Both [6] and [7] do not consider correlation. Other papers, such as [8-11], are based on Goel's work, but they consider different MIMO models, i.e., [8-10] assume Rayleigh MIMO channels while [11] assumes Rician MIMO channels. All of works in [8-11] do not consider correlation, and they use all eigen-subchannels to transmit messages with $t > r$. In the proposed scheme, the number of eigen-subchannels for messages, i.e., s_1, is a variable that can be adjusted. Hence, the comparison is between the variable s_1 and $s_1 = n$ where the channel models are the same in our simulations based on receiver-side Rayleigh correlated model. In order to pay our respects to Mr. Goel who first presented this AN scheme, we name the schemes in [8-11] as "Goel scheme". To clarify the statement, we have modified the confusing name from "Goel scheme" as "$s_1 = n$ and $s_2 = t - s_1$" in below simulation figures.

We have explained this point in the 2nd paragraph of Section IV, on the page 6, 2nd column of the revised manuscript. Specifically, the added content is copied as follow.

"The ergodic secrecy rates of our scheme are compared to the traditional AN schemes [8]-[11] without the correlation consideration that use all eigen-subchannels to transmit messages, i.e., $s_1 = n$. In the proposed scheme, the number of eigen-subchannels for messages, i.e., s_1, is a variable that can be adjusted. The channel model in simulations is receiver-side correlated Rayleigh fading channel. "

7. Reviewer's Comment:

There are also some minor mistakes in the paper. For example, in Section III-B, the sentence "We can simplify the expression to an approximate form, to show the impacts of correlated matrices $\mathbf{R}_r$ and $\mathbf{R}_r$ (a function of..." should be "$\mathbf{R}_r$ and $\mathbf{R}_e$".

Authors' Responses:

Thanks for the comment. We have tried our best to improve the writing presentation throughout this paper.

AUTHORS' RESPONSES TO REVIEWER 3

The comments from Reviewer 3 can be divided into five specific problems, and the detailed response is given as follows.

1. Reviewer's Comment:

As mentioned in the paper, this work is an extension of the previously published work, i.e., reference [9]. Could the author emphasize how mathematical difficulty it is to include the receiver-side correlated nature compared to the previous work in [9]? What is the main challenging to cope with the correlated nature in the formulation?

Authors' Responses:

There are two mathematical challenges when considering receiver-side correlation.

At first, there is no appropriate research to describe the properties of the receiver-correlated matrix $\mathbf{R}_a$ in terms of AoA, RAS, and antenna distance, but it is useful for approximate analysis of ergodic secrecy rates. We use Theorem 1 to specify the properties of the correlated matrix $\mathbf{R}_a$ that can be used to deduce approximate analysis of ergodic secrecy rates in TABLE I.

Secondly, the properties of $\mathbf{H}_e\mathbf{F}\mathbf{F}^\dagger\mathbf{H}_e^\dagger$ is the mathematical challenge if $\mathbf{H}_e$ has receiver-side correlation. In traditional MIMO capacity research, the Wishart matrix usually focuses on $\mathbf{H}\mathbf{H}^\dagger$ form (or $\mathbf{H}^\dagger\mathbf{H}$), while in AN-aided MIMO, the Wishart matrix has $\mathbf{H}\mathbf{H}^\dagger$ and $\mathbf{H}_e\mathbf{F}\mathbf{F}^\dagger\mathbf{H}_e^\dagger$ forms, where $\mathbf{F}$ is an independent unitary matrix. It is hard to deduce the wiretap channel capacity via existing research of Wishart matrices. Hence, we provide the distribution formulation of $\mathbf{H}_e\mathbf{F}$ with receiver-side correlation in Theorem 2, and its simple and exact version pdf functions of $\mathbf{H}_e\mathbf{F}\mathbf{F}^\dagger\mathbf{H}_e^\dagger$ in Theorem 3.

We have highlighted the contribution of the work in the 5 paragraph of Section I, on the page 2, 1st column of the revised manuscript.

2. Reviewer's Comment:

The author takes the lower bound of ergodic secrecy rate for the further analysis, as shown in Eqn. (12), due to the lack of knowing $\mathbf{H}_e$. Then, it would be wondering how much different the performance will be compared to the case considering the true ergodic secrecy

rate, as shown in Eqn. (11). This can be tested in the Monte Carlo simulations by checking the scenarios of a negative instantaneous secrecy rate.

Authors' Responses:

We are sorry for our mistake that using Eqn. (12) (Eqn. (14) in the current revision) for Monte Carlo simulations, and we should use Eqn. (11) (Eqn. (10) in the current revision), which is true ergodic secrecy rate, to verify the theoretical results from Eqn. (20). Hence, we have changed all simulation results via Eqn. (10) in this new manuscript. We find that the results of the true ergodic secrecy rate is very similar with the lower bound Eqn. (20), because it seems that C_m is lager than C_w with a high probability, as shown in Fig. R2. The 10^5 independent Monte Carlo simulations for each curve indicate that C_m is smaller than C_w in only 662 runs among the total simulations of these four curves.

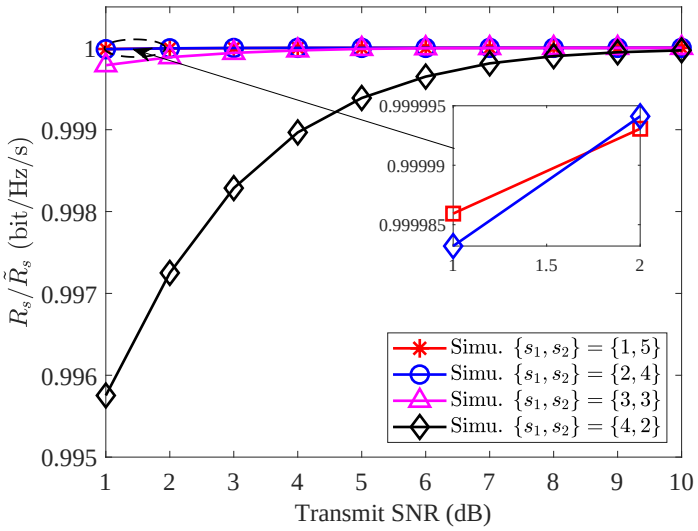

Fig. R2. The ratio between lower bound of ergodic secrecy rates, i.e., R_s, as shown in Eqn. (14) and the true ergodic secrecy rates, i.e., $\tilde{R}$, as shown in Eqn. (10).

Due to the page limit of the IEEE System Journal, this test is only shown in the revision summary and https://github.com/yiliangliu1990/liugit_pub, which is shown as a footnote in the 3rd paragraph of Section III, page 4, 2nd column of the revised manuscript as follow.

"With a large s_2, i.e., more eigen-subchannels are allocated for AN signals, it seems that

C_m is much larger than C_w with a high probability[1]. ”

3. Reviewer's Comment:

The proposed scheme is based on the analysis of the statistical information of the channels. What if the instantaneous channel state information of all channels are known, in that case, is it possible to optimize the precoding matrix $\mathbf{B}$ and $\mathbf{Z}$ by solving an optimization problem? In that way, the global optimum may be achievable, and it would also be interesting that how much difference it would be compared to the result of the proposed scheme in this work, since the current scheme does not guarantee the globally optimal solution, especially considering the lower bound problem mentioned in point 2.

Authors' Responses:

Many thanks for your valuable comment. In our scheme, we chose s_1 and s_2 based on the ergodic secrecy rates via Eqn. (20), then use the eigenvalue decomposition of $\mathbf{H}^{\dagger}\mathbf{H}$ to obtain $\mathbf{B}$ and $\mathbf{Z}$. Hence, this scheme can be regarded as statistically optimal. It has a lower complexity than optimization schemes. For the case with instantaneous CSI, global optimal solution can be obtained at every CSI state through optimization schemes, such as semidefinite programming (SDP) relaxation, Now, we are studying SDP relaxation to optimize information and AN beamforming vectors.

4. Reviewer's Comment:

In Section IV, the proposed scheme is compared to the 'Goel scheme' which uses all eigen-subchannels to transmit messages and is not aware of the receiver-side correlated channels. Then, I wonder the performance of a scheme with the consideration of the eigen-subchannel optimization, but without the awareness of the correlated fading nature. By adding this into the comparison in the simulation, the gain of a channel-correlation-aware design is verified.

Authors' Responses:

We have added the simulations without the awareness of the correlated fading nature in Fig. 2(a) in Section IV, on the page 7 of the revised manuscript. We think this scenario is common because if Alice does not have the knowledge of correlation parameters at Eve

[1]The test is shown in https://github.com/yiliangliu1990/liugit_pub.

side, it will just do the eigen-subchannel optimization assuming there is no correlation at Eve side, i.e., Eve's channel is an uncorrelated Rayleigh fading channel.

5. Reviewer's Comment:

Minor issues:

The paper contains some typos and improper expressions, please correct them and recheck the paper for the potential typos.

1. In the beginning of Section III.B., a typo of $\mathbf{R}_r$ should be $\mathbf{R}_e$.

2. In Algorithm 1 line 5, it is better to replace 'max' by other symbols or letters, since 'max' could be confused with maximization.

3. In page 9 line 38, i.e, should be i.e.,

Authors' Responses:

Thanks for the comment. We have tried our best to improve the writing presentation throughout this paper.

AUTHORS' RESPONSES TO REVIEWER 4

The comments from Reviewer 4 can be divided into seven specific problems, and the detailed response is given as follows.

1. Reviewer's Comment:

In the introduction section, reference related to correlation among antennas should be provided to support the statement "in most real applications, the correlation among antennas may exist due to scattering channels or small spacing between antenna...".

Authors' Responses:

Thanks for your comment. We have added a 3GPP standard [17] and some research papers [18] [19] related to the statement. Specifically, we have added the following content in the 3rd paragraph of Section I, on the page 1, 2nd column of the revised manuscript.

"Unfortunately, in most real applications, the correlation among antennas may exist due to poor-scattering environments or small spacing between antenna elements [17]-[19]."

2. Reviewer's Comment:

The authors assume that Alice knows $\mathbf{R}_e$ and Eve knows $\mathbf{H}$ and $\mathbf{R}_r$. Are they practical assumptions? Further discussions are needed.

Authors' Responses:

Based on the research of existing communication systems, we think it is practical.

At first, Alice can get the knowledge of $\mathbf{R}_e$ and the CDI of Eve, because Eve may be a common receiver in the same communication systems with Alice, and exchanges messages without security consideration. Hence, Alice can obtain $\mathbf{R}_e$ via historical CSI of $\mathbf{H}_e$, i.e., $\mathbf{R}_e = \mathrm{E}(\mathbf{H}_e\mathbf{H}_e^{\dagger}/t)$ or statistical AoA information as shown in Definition 2. Otherwise, Alice should assume that there is no correlation at Eve side, i.e., $\mathbf{R}_e = \mathbf{I}_e$, which is the worst assumption because $\mathbf{R}_e = \mathbf{I}_e$ will maximize the ergodic wiretap channel capacity among all realizations of $\mathbf{R}_e$.

Secondly, CSI is usually revealed to Eve in feedback-based CSI estimation, where Alice emits the training signal to Bob and Bob uses feedback channels to inform Alice of CSI, which allows Bob and Alice to obtain accurate knowledge of $\mathbf{H}$. However, Eve can obtain $\mathbf{H}$ due to the broadcasting nature of feedback channels, and Eve can intercept training signals

to get $\mathbf{H}_e$ of himself. In addition, Eve can obtain the $\mathbf{R}_r = \mathrm{E}(\mathbf{H}\mathbf{H}^\dagger/t)$ and $\mathbf{R}_e = \mathrm{E}(\mathbf{H}_e\mathbf{H}_e^\dagger/t)$ according long-term realizations of $\mathbf{H}$ and $\mathbf{H}_e$, or statistical AoA information as shown in Definition 2.

We explained the CSI assumptions in the 3-4 paragraphs of Section II. B, on the page 3, 2nd column of the revised manuscript.

3. Reviewer's Comment:

More explanation on how to obtain (22) is needed.

Authors' Responses:

Eqn. (22) (Eqn. (20) in the current revision) is the most important equation, because we will use it to choose s_1 and s_2 for information and AN precoding, which is the theoretical ergodic secrecy rate expression of Eqn. (14).

Recalling the Eqn. (14), we have

$$R_s(P, \mathbf{H}, \mathbf{R}_r, \mathbf{R}_e; s_1, s_2) \tag{R6}$$

$$= [\mathrm{E}_{\mathbf{H}}[C_m] - \mathrm{E}_{\mathbf{H}_e,\mathbf{H}}[C_w]]^+$$

$$= \left[\mathrm{E}\big[\log_2\det(\mathbf{I}_r + \rho\mathbf{H}_1\mathbf{H}_1^\dagger)\big] - \mathrm{E}\big[\log_2\det\big(\mathbf{I}_e + \frac{\rho\mathbf{H}_2\mathbf{H}_2^\dagger}{\rho\mathbf{H}_3\mathbf{H}_3^\dagger + \mathbf{I}_e}\big)\big]\right]^+, \tag{R7}$$

where $\rho = P/t$. We definite the first term in the above expression as

$$\mathrm{E}\big[\log_2\det(\mathbf{I}_r + \rho\mathbf{H}_1\mathbf{H}_1^\dagger)\big] = C_{\mathbf{H}}(\mathbf{R}_r, \rho, s_1). \tag{R8}$$

The second term in Eqn. (R7) can be rewritten as

$$\mathrm{E}\left[\log_2\det\left(\mathbf{I}_e + \frac{\rho\mathbf{H}_2\mathbf{H}_2^\dagger}{\rho\mathbf{H}_3\mathbf{H}_3^\dagger + \mathbf{I}_e}\right)\right] \tag{R9}$$

$$= \mathrm{E}\left[\log_2\det\left(\frac{\rho\mathbf{H}_3\mathbf{H}_3^\dagger + \rho\mathbf{H}_2\mathbf{H}_2^\dagger + \mathbf{I}_e}{\rho\mathbf{H}_3\mathbf{H}_3^\dagger + \mathbf{I}_e}\right)\right]$$

$$= \mathrm{E}_{\mathbf{H}_4}\big[\log_2\det\big(\mathbf{I}_e + \rho\mathbf{H}_4\mathbf{H}_4^\dagger\big)\big] - \mathrm{E}_{\mathbf{H}_3}\big[\log_2\det\big(\mathbf{I}_e + \rho\mathbf{H}_3\mathbf{H}_3^\dagger\big)\big]$$

$$= C_{\mathbf{H}_4,}(\mathbf{R}_e, \rho, e) - C_{\mathbf{H}_3}(\mathbf{R}_e, \rho, n_1),$$

where $n_1 = \min(s_2, e)$, $\mathbf{H}_1 = \mathbf{H}\mathbf{B} \in \mathbb{C}^{r\times s_1}$, $\mathbf{H}_2 = \mathbf{H}_e\mathbf{B} \in \mathbb{C}^{e\times s_1}$, $\mathbf{H}_3 = \mathbf{H}_e\mathbf{Z} \in \mathbb{C}^{e\times s_2}$, and $\mathbf{H}_4 = [\mathbf{H}_2, \mathbf{H}_3] = \mathbf{H}_e\mathbf{U} \in \mathbb{C}^{e\times t}$. Thus, we get

$$R_s(P, \mathbf{R}_r, \mathbf{R}_e; s_1, s_2) \tag{R10}$$

$$= \big[C_{\mathbf{H}}(\mathbf{R}_r, \rho, s_1) + C_{\mathbf{H}_3}(\mathbf{R}_e, \rho, n_1) - C_{\mathbf{H}_4}(\mathbf{R}_e, \rho, e)\big]^+,$$

As an arbitrary MIMO channel ($\mathbf{H}$, $\mathbf{H}_3$, or $\mathbf{H}_4$) can be effectively decomposed into multiple parallel SISO eigen-subchannels, we can obtain $C_{\mathbf{H}}(\mathbf{R}_r, \rho, s_1)$, $C_{\mathbf{H}_3}(\mathbf{R}_e, \rho, n_1)$, and $C_{\mathbf{H}_4}(\mathbf{R}_e, \rho, e)$ via the pdf of the kth eigenvalue of complex Wishart matrices as

$$C_{\mathbf{A}}(\mathbf{R}_a, \rho, \eta) = \sum_{k=1}^{\eta} \int_0^{\infty} \log_2(1+\rho x) f_{\lambda_k}(x) dx, \tag{R11}$$

in which $\mathbf{A} \in \mathbb{C}^{a \times b}$, $\mathbf{R}_a$ is an $a \times a$ matrix, λ_k is the kth largest eigenvalue of $\mathbf{A}\mathbf{A}^{\dagger}$(or $\mathbf{A}^{\dagger}\mathbf{A}$), and $f_{\lambda_k}(x)$ is given in Theorem 3.

The proof is completed. ■

Due to the page limit of the IEEE System Journal, this proof is only shown in the revision summary and https://github.com/yiliangliu1990/liugit_pub

4. Reviewer's Comment:

In the simulation section, the reviewer observes that simulated results are exactly the same as the analytic ones. However, in common sense, it is not possible. Can the authors explain this?

Authors' Responses:

At first, we should state the theoretical (theo.) results are from Eqn. (20), while the simulation (simu.) results are from Eqn. (10) rather than Eqn. (14). Eqn. (20) is the theoretical expression of Eqn. (14), so they are exactly the same with enough runs of the Monte Carlo procedure.

Then, we will explain why Eqn. (20) is also so matching with Eqn. (10). Eqn. (20) or (14) can not represent the real ergodic secrecy rate. In fact, Eqn. (10) is the real ergodic secrecy rate. Based on the comment of Reviewer 3, we rework all simulations where results of Monte Carlo simulation is from Eqn. (10) assuming all CSIs is obtained at Eve, and find there are little difference between real ergodic secrecy rates and values from Eqn. (20), because AN signals make C_m be much larger than C_w with a high probability. We upload our matlab code and corresponding test of this probability in https://github.com/yiliangliu1990/liugit_pub, and the test results are also shown in the responses of Reviewer 1's 1st and Reviewer 3's 2nd comments.

5. Reviewer's Comment:

The authors compared their results with that presented in [6] and [7]. However, these two papers are quite old. In addition, they have a lot of citations. So the reviewer believes that there are more recent references which the authors should compare their results with.

Authors' Responses:

Many thanks for the valuable comment. We replaced [6] [7] by [8]-[11], which used all eigen-subchannels to transmit messages with the limitation of $t > r$. In the proposed scheme, the number of eigen-subchannels for messages, i.e., s_1, is a variable that can be adjusted. Hence, the comparison is between the variable s_1 and the $s_1 = n$ scenarios. In addition, we have modify the name from "Goel scheme" as "$s_1 = n$ and $s_2 = t - s_1$" in all simulation figures according to the Reviewer 2's second comment. Corresponding content is in the 2nd paragraph of Section IV, on the page 6, 2nd column of the revised manuscript, which is copied as follow.

"The ergodic secrecy rates of our scheme are compared to the traditional AN schemes [8]-[11] without the correlation consideration that use all eigen-subchannels to transmit messages, i.e., $s_1 = n$. In the proposed scheme, the number of eigen-subchannels for messages, i.e., s_1, is a variable that can be adjusted. The channel model in simulations is receiver-side correlated Rayleigh fading channel. "

6. Reviewer's Comment:

When t is large enough, the reviewer curious about the behavior of the secrecy rate when r increases and approaches to t. Can the authors provide this simulation?

Authors' Responses:

We tested the AN scheme in massive MIMO systems in this response letter, and we added a simulation with $t = 64$, and $r = \{59, 60, 61, 62, 63, 64\}$. We set $s_1 = \{1, 2, 3, 4\}$ and $s_2 = t - s_1$, because it is hard to exhaustively test all s_1 from 1 to t. The theoretical expression, i.e., Eqn. (20), is not available for massive MIMO systems, because we need $2^n - 1$ memory spaces to record $2^n - 1$ matrices $\mathbf{\Omega}(\cdot)$ for $f_{\lambda_k}(x), k = 1, ..., n$, in Eqn. (20). However, matlab can only support maximum 2^{14} memory spaces. Hence, the below figure only shows the Monte Carlo simulations.

From Fig. R3, we can find that the ergodic secrecy rate increases with the number of Bob's antennas. In addition, the increasing ratio is larger with a larger s_1, because no

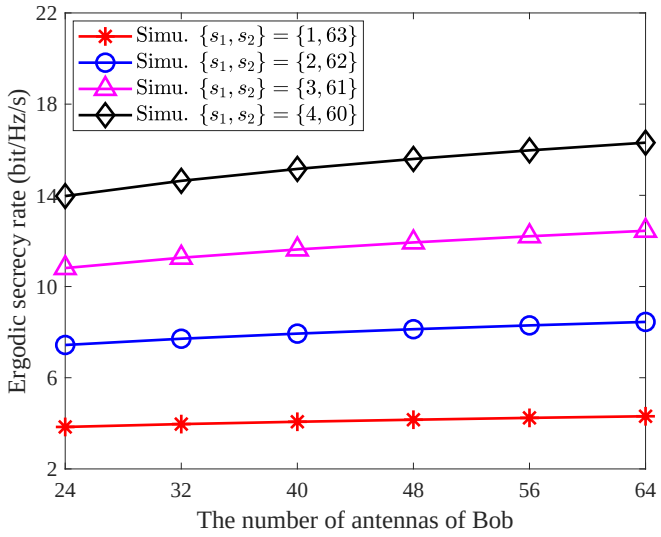

Fig. R3. Ergodic secrecy rates of a massive MIMO system, where $t = 64$, $e = 4$, transmit SNR=5 dB, $d_{\text{Bob}} = d_{\text{Eve}} = 0.8$, $\bar{\theta}_{\text{Bob}} = \bar{\theta}_{\text{Eve}} = 30^\circ$, and $\delta_{\text{Bob}} = \delta_{\text{Eve}} = 10^\circ$.

matter $r = 24$ or $r = 64$, that is enough for Bob to decode these confidential message streams. Bob can gather the received power of each antennas, so more receive antennas means a larger power gain. We upload our matlab code and corresponding content in https://github.com/yiliangliu1990/liugit_pub

7. Reviewer's Comment:

Minor comments: references should be in the form [x]-[y]. However, throughout the paper, references are [x][y]. In addition, several typos are found. Please carefully proofread the paper before submitting.

Authors' Responses:

We have modified the citation format according to the IEEE standard citation style, and have tried our best to correct all the typos throughout this paper.

AUTHORS' RESPONSES TO REVIEWER 5

The comments from Reviewer 5 can be divided into seven specific problems, and the detailed response is given as follows.

1. Reviewer's Comment:

In the abstract, the author said "extend our previous AN scheme to spatially correlated Rayleigh fading channels at receiver-sides". However, according to the contents of this paper, we find that spatially correlation at both receiver-side and eavesdropper-side has be considered. Hence, please modify the corresponding statements.

Authors' Responses:

Thanks for your comment. We found our previous statement is confusing, so we have modified the statements of Abstract and Introduction, which are copied as follows.

In Abstract,

"In this paper, we extend our previous AN scheme to spatially correlated Rayleigh fading channels at both legitimate receiver- and eavesdropper-sides."

In Introduction, on the page 1, 2nd column of the revised manuscript

"This paper focuses on receiver-side correlation scenarios (at both legitimate receiver- and eavesdropper-sides).".

2. Reviewer's Comment:

In the introduction. The reviewer would suggest the authors (1) to cite and discuss recent AN-based physical layer security papers published in the IEEE System Journal, or other outstanding journals and magazines. (2) the researches on the correlated channel model in MIMO system without physical layer security.

Authors' Responses:

(1) We found a recent paper [13] on the AN-based physical layer security that published in IEEE System Journal, and we have added a discussion about it in the 2nd paragraph of Introduction on the page 1, 2nd column of the revised manuscript, which is copied as follow.

"These AN schemes achieve a null space for AN signals only under the condition that the number of transmit antennas is larger than that of receivers [6]–[13]."

(2) In addition, we also added some papers on the correlated channel model in MIMO system without physical layer security when introducing the correlated fading and correlated matrices [24]-[26], [32] [33] [35]. They have been published for many years.

3. Reviewer's Comment:

In the system model, we can find the statements that $t > e$, however, not any assumption on the number of Bob's antennas is provided. The simulation section only shows the $r = e$ scenarios. Please specify the condition of Bob' antennas, and provide some simulations in terms of the number of Bob's antennas.

Authors' Responses:

At first, we specified that r is arbitrary in the first paragraph of Section II. A, on the page 2, 2nd column of the revised manuscript, which is copied as follow.

"We assume $t > e$ and r is arbitrary. "

Then, we have added the simulations in terms of the number of Bob's antennas in Fig. 3, where $t = 5$, $e = 3$, and r is a variable in the x axis, which is in Section IV, on page 7, 1st column of the revised manuscript.

4. Reviewer's Comment:

Please add some simulations to show if there still is a positive ergodic secrecy rate if Eve has uncorrelated antennas, but Bob has correlated ones, because we always consider the worst condition where Eve is superior. In addition, please specify How many realizations for Monte Carlo simulations.

Authors' Responses:

We have added the simulations without the awareness of the correlated fading nature in Fig. 2(a) on the page 7 of the revised manuscript. We think this scenario is usual because if Alice does not have the knowledge of correlation parameters at Eve side, it will just do the eigen-subchannel optimization assuming there is no correlation at Eve side, i.e., Eve's channel is an uncorrelated Rayleigh fading channel.

In addition, we specified the number of realizations for Monte Carlo simulations in the 1st paragraph of Section IV, on the page 6, 2nd column of the revised manuscript as follow.

"The theoretical results (theo.) from Eqn. (20) are in a good agreement with the Monte Carlo simulations (simu.) of 10^5 independent runs on Eqn. (10)"

5. Reviewer's Comment:

The equation (61) is not clear, please add more explanation, proof process, or corresponding references.

Authors' Responses:

Here, we provide the proof as follow. Due to the page limit of the IEEE System Journal, this proof is only shown in the revision summary and our GitHub.

https://github.com/yiliangliu1990/liugit_pub

$$\det[\mathbf{E}^{\boldsymbol{\kappa}}(\boldsymbol{\lambda})]\prod_{i<j}^{n}(\lambda_i-\lambda_j) \tag{1}$$

$$= \det\begin{bmatrix} 1 & \dots & 1 \\ \lambda_1 & \dots & \lambda_n \\ \vdots & & \vdots \\ \lambda_1^{n-1} & \dots & \lambda_n^{n-1} \end{bmatrix} \times \det\begin{bmatrix} \sigma_{\kappa_{r-n+1}}^{r-n-1}\exp(-\frac{\lambda_1}{\sigma_{\kappa_{r-n+1}}}) & \sigma_{\kappa_{r-n+2}}^{r-n-1}\exp(-\frac{\lambda_1}{\sigma_{\kappa_{r-n+2}}}) & \dots & \sigma_{\kappa_r}^{r-n-1}\exp(-\frac{\lambda_1}{\sigma_{\kappa_r}}) \\ \sigma_{\kappa_{r-n+1}}^{r-n-1}\exp(-\frac{\lambda_2}{\sigma_{\kappa_{r-n+1}}}) & \sigma_{\kappa_{r-n+2}}^{r-n-1}\exp(-\frac{\lambda_2}{\sigma_{\kappa_{r-n+2}}}) & \dots & \sigma_{\kappa_r}^{r-n-1}\exp(-\frac{\lambda_2}{\sigma_{\kappa_r}}) \\ & \vdots & & \vdots \\ \sigma_{\kappa_{r-n+1}}^{r-n-1}\exp(-\frac{\lambda_n}{\sigma_{\kappa_{r-n+1}}}) & \sigma_{\kappa_{r-n+2}}^{r-n-1}\exp(-\frac{\lambda_n}{\sigma_{\kappa_{r-n+2}}}) & \dots & \sigma_{\kappa_r}^{r-n-1}\exp(-\frac{\lambda_n}{\sigma_{\kappa_r}}) \end{bmatrix}$$

$$= \prod_{i=1}^{n}\sigma_{\kappa_{r-n+i}}^{r-n-1}\det\begin{bmatrix} \sum_{q=1}^{n}\lambda_q^0\exp(-\frac{\lambda_q}{\sigma_{\kappa_{r-n+1}}}) & \sum_{q=1}^{n}\lambda_q^0\exp(-\frac{\lambda_q}{\sigma_{\kappa_{r-n+2}}}) & \dots & \sum_{q=1}^{n}\lambda_q^0\exp(-\frac{\lambda_q}{\sigma_{\kappa_r}}) \\ \sum_{q=1}^{n}\lambda_q^1\exp(-\frac{\lambda_q}{\sigma_{\kappa_{r-n+1}}}) & \sum_{q=1}^{n}\lambda_q^1\exp(-\frac{\lambda_q}{\sigma_{\kappa_{r-n+2}}}) & \dots & \sum_{q=1}^{n}\lambda_q^1\exp(-\frac{\lambda_q}{\sigma_{\kappa_r}}) \\ & \vdots & & \vdots \\ \sum_{q=1}^{n}\lambda_q^{n-1}\exp(-\frac{\lambda_q}{\sigma_{\kappa_{r-n+1}}}) & \sum_{q=1}^{n}\lambda_q^{n-1}\exp(-\frac{\lambda_q}{\sigma_{\kappa_{r-n+2}}}) & \dots & \sum_{q=1}^{n}\lambda_q^{n-1}\exp(-\frac{\lambda_q}{\sigma_{\kappa_r}}) \end{bmatrix}$$

$$= \prod_{i=1}^{n}\sigma_{\kappa_{r-n+i}}^{r-n-1}\sum_{q}^{\sim}\det\begin{bmatrix} \lambda_{q_1}^0\exp(-\frac{\lambda_{q_1}}{\sigma_{\kappa_{r-n+1}}}) & \lambda_{q_2}^0\exp(-\frac{\lambda_{q_2}}{\sigma_{\kappa_{r-n+2}}}) & \dots & \lambda_{q_n}^0\exp(-\frac{\lambda_{q_n}}{\sigma_{\kappa_r}}) \\ \lambda_{q_1}^1\exp(-\frac{\lambda_{q_1}}{\sigma_{\kappa_{r-n+1}}}) & \lambda_{q_2}^1\exp(-\frac{\lambda_{q_2}}{\sigma_{\kappa_{r-n+2}}}) & \dots & \lambda_{q_n}^1\exp(-\frac{\lambda_{q_n}}{\sigma_{\kappa_r}}) \\ & \vdots & & \vdots \\ \lambda_{q_1}^{n-1}\exp(-\frac{\lambda_{q_1}}{\sigma_{\kappa_{r-n+1}}}) & \lambda_{q_2}^{n-1}\exp(-\frac{\lambda_{q_2}}{\sigma_{\kappa_{r-n+2}}}) & \dots & \lambda_{q_n}^{n-1}\exp(-\frac{\lambda_{q_n}}{\sigma_{\kappa_r}}) \end{bmatrix}$$

$$= \prod_{i=1}^{n}\sigma_{\kappa_{r-n+i}}^{r-n-1}\sum_{q}^{\sim}\sum_{\iota}^{\sim}(-1)^{\mathrm{per}(\iota_1,\dots,\iota_n)}\prod_{i=1}^{n}\lambda_{q_i}^{\iota_i-1}\exp(-\frac{\lambda_{q_i}}{\sigma_{\kappa_{r-n+i}}}).$$

---

6. Reviewer's Comment:

In the system model, the authors claimed that Alice knows "the channel distribution information (CDI) of Eve". As the eavesdropper's CSI is not known to Alice, how does Alice obtain the information on the CDI of Eve? If this assumption conforms to practical scenarios?

Authors' Responses:

We explained the CSI assumptions in Section II, on the page 3, 2nd column of the revised manuscript, which is copied as follow.

"Alice can get the knowledge of $\mathbf{R}_e$ and the CDI of Eve, because Eve may be a common receiver in the same communication systems with Alice, and exchanges messages without security consideration. Hence, Alice can obtain $\mathbf{R}_e$ via historical CSI of $\mathbf{H}_e$, i.e., $\mathbf{R}_e = \mathrm{E}(\mathbf{H}_e\mathbf{H}_e^{\dagger}/t)$ or statistical AoA information as shown in Definition 2. Otherwise, Alice should assume that there is no correlation at Eve side, i.e., $\mathbf{R}_e = \mathbf{I}_e$, which is the worst assumption because $\mathbf{R}_e = \mathbf{I}_e$ will maximize the ergodic wiretap channel capacity among all realizations of $\mathbf{R}_e$. "

7. Reviewer's Comment:

P.4 Line 20, 1st column, the author said "In the AN elimination process, the received signal with noise multiplied by a given matrix will not change its capacity." This sentence is hard to understand. If $\mathbf{B}$ does not include all eigenvector of $\mathbf{H}^{\dagger}\mathbf{H}$. The capacity will be reduced via the AN elimination process.

Authors' Responses:

Thanks a lot, we made a mistake on this statement. As you said, if $\mathbf{B}$ does not include all eigenvector of $\mathbf{H}^{\dagger}\mathbf{H}$, the main capacity will be reduced. We have modified the statement in the last paragraph of Section II. B, on the page 3, 2nd column of the revised manuscript, which is copied as follow.

"In the AN elimination process, the channel where the received signal is left multiplied by a given matrix $[\mathbf{HB}]^{\dagger}$ will not change its capacity if $\mathbf{B}$ includes all eigenvectors of $\mathbf{H}^{\dagger}\mathbf{H}$."