A New Secure Transmission Scheme with Outdated Antenna Selection

Jianwei Hu, *Student Member, IEEE,* Yueming Cai, *Senior Member, IEEE,*
Nan Yang, *Member, IEEE,* and Weiwei Yang, *Member, IEEE*

***Abstract*—We propose a new secure transmission scheme in the multi-input multi-output multi-eavesdropper wiretap channel. In this channel, the N_A-antenna transmitter adopts transmit antenna selection (TAS) to choose the antenna that maximizes the instantaneous signal-to-noise ratio (SNR) at the receiver to transmit, while the N_B-antenna receiver and the N_E-antenna eavesdropper adopt maximal-ratio combining (MRC) to combine the received signals. We focus on the practical scenario where the channel state information (CSI) during the TAS process is outdated. In this scenario, we propose a new transmission scheme to prevent the detrimental effect of the outdated CSI on the wiretap codes design at the transmitter. To thoroughly assess the secrecy performance achieved by the proposed scheme, we derive new closed-form expressions for the exact secrecy outage probability and the probability of non-zero secrecy capacity for arbitrary SNRs. We also derive new compact expressions for the asymptotic secrecy outage probability at high SNRs. Notably, in the analysis we take spatial correlation at the receiver into consideration. Apart from the advantage of our scheme over the conventional TAS/MRC scheme, we demonstrate that the outdated TAS reduces the secrecy diversity order from $N_A N_B$ to N_B. We also demonstrate that antenna correlation improves the secrecy performance at low SNR but deteriorates the secrecy performance at medium and high SNRs, by affecting the secrecy array gain only.**

***Index Terms*—Secure transmission, outdated antenna selection, exponential antenna correlation, MIMOME wiretap channels.**

I. Introduction

THE BROADCAST nature of wireless communication makes it inherently vulnerable to potential eavesdropping by unauthorized receivers. As such, the need of confidential and secure transmission poses significant challenges in designing wireless communication systems. Traditionally, the confidentiality of data transmission has been addressed at higher layers using cryptographic protocols. However, these methods may not be suitable for large scale dynamic wireless networks, due to the high computational complexity caused by key distribution and management [1, 2]. Against this background, some efforts have been devoted to information-theoretic secrecy and revealed the possibility of ensuring confidentiality by exploiting the inherent randomness of physical channels in single-antenna wiretap channels, multi-antenna channels, and relay-aided channels (see [3–11] and the references therein). In particular, if the eavesdropper's observation is a degraded version of the legitimate user's observation, it is possible to provide secure communications between the legitimate users while keeping the eavesdropper completely ignorant of secure messages. Motivated by these studies, the physical layer security techniques are explored to offer an additional level of protection and to achieve perfect secrecy. The core philosophy of physical layer security is to exploit the characteristics of the wireless medium, such as fading, rather than applying the conventional cryptographic methods.

A. Related Work

Motivated by the potential of using multiple antennas in next generation wireless standards, physical layer security in multiple-input multiple-output (MIMO) wiretap channels has recently attracted a tremendous amount of research efforts. From the information-theoretic perspective, the secrecy capacity has been examined in multi-input, single-output, multi-eavesdropper (MISOME) channels [12] and multi-input, multi-output, multi-eavesdropper (MIMOME) channels [13]. In [12, 13] we note that the assumption that the perfect channel state information (CSI) of the main channel and the eavesdropper's channel is available at the transmitter may not be realistic. Particularly, the eavesdropper's CSI is difficult to obtain at the transmitter if the eavesdropper is a passive entity. Against this background, recent works designed secure transmission schemes for the realistic passive eavesdropping scenario [14–19]. In [14, 15], transmit beamforming in the direction of the legitimate receiver was recognized as an useful means to enhance security in MIMO wiretap channels.

It is mentioned that transmit beamforming requires high feedback overhead and high computational cost of signal processing, especially when the number of transmit antennas is large. As such, a low-cost and low-complexity alternative, referred to as transmit antenna selection (TAS), was proposed to capture the advantages of MIMO systems in security enhancement. In [16], TAS was introduced into the multi-input, single-output, single-eavesdropper (MISOSE) channels to boost physical layer security. In [17, 18], TAS was examined in MIMOME channels, together with maximal-ratio

This work of J. Hu, Y. Cai, and W. Yang was supported by the National Natural Science Foundation of China (No. 61371122) and Jiangsu provincial National Science Foundation (BK2013105). The work of N. Yang was supported by the Australian Research Council Discovery Project (DP150103905).

J. Hu, Y. Cai, and W. Yang are with the College of Communications Engineering, PLA University of Science and Technology, Nanjing 210007, China (e-mail: hujianwei1990@yeah.net; caiym@vip.sina.com; wwyang1981@163.com).

N. Yang is with the Research School of Engineering, Australian National University, Canberra, ACT 0200, Australia (email: nan.yang@anu.edu.au).

Digital Object Identifier 10.1109/TIFS.2015.2464703

combining (MRC) and generalized selection combining at the legitimate receiver. Moreover, [19] proposed a new TAS scheme which selects two transmit antennas to examine the trade-off between feedback overhead and secrecy performance in MIMOME wiretap channels.

B. Motivation

We note that the application of TAS may pose a challenge. In practice, the signal-to-noise ratios (SNRs) of all branches need to be known for optimal antenna selection. However, it is indeed challenging to know these SNRs when there is only one radio frequency (RF) chain at the transmitter [20]. One solution to address this challenge is to use a training signal in a preamble of transmitted data packets [21]. During this preamble, the transmitter scans the transmit antennas to sequentially transmit pilot symbols. After performing the channel estimation based on the pilot symbols, the receiver determines the optimal transmit antenna with the maximum output SNR. Then the receiver uses a feedback link to inform the transmitter which transmit antenna is selected for data transmission.

It is worth noting that the pilot symbols in the aforementioned TAS scheme can be several milliseconds apart [22]. This leads to the fact that the CSI associated with the selected transmit antenna during the antenna selection process may not be the same as the CSI during the subsequent data transmission. Particularly, the CSI at different antennas during the antenna selection process may be outdated by different amounts [23, 24]. For example, the estimated CSI for the preceding antenna is probably more outdated than that for the subsequent antenna. Since outdated CSI leads to outdated antenna selection at the transmitter, some publications have examined its impact on the performance of MIMO systems without considering secrecy, e.g., [25–27].

When TAS is used for security enhancement, outdated antenna selection introduces a new set of problems. One problem is that the conventional TAS scheme uses outdated CSI to construct wiretap codes, which in turns leads to a connection outage such that the transmitter transmits but the receiver cannot decode the message. Needless to say, such an outage is detrimental to the throughput performance. Motivated by this, in this work we propose a new secure transmission scheme to avoid the occurrence of the connection outage in the presence of outdated antenna selection.

C. Novelties

In this paper, we consider that TAS/MRC is used in MIMOME channels where TAS is adopted at the N_A-antenna transmitter while MRC is adopted at the N_B-antenna receiver and the N_E-antenna eavesdropper. In such channels, we focus on the practical scenario with outdated antenna selection at the transmitter and exponential antenna correlation existing among N_B antennas at the receiver. The novelties of our work are summarized as follows:

1) We design a new secure transmission scheme in the presence of outdated TAS where the optimal transmit antenna at the selection time instant t may not be the optimal one at the secure transmission time instant $t+\tau$. The outdated TAS leads to the fact that the instantaneous CSI associated with the optimal transmit antenna obtained at time instant t may not be the same as that at time instant $t+\tau$. Our newly designed scheme requires the receiver to feed back the index of the optimal transmit antenna and the associated instantaneous CSI in different time slots. This ensures that the perfect instantaneous CSI associated with the selected transmit antenna is used for secure transmission, which in turns guarantees that the connection outage does not occur in the main channel.
2) We derive new statistics of bivariate generalized hyper-exponential distributions. This statistics allows us to precisely analyze the impact of exponential antenna correlation at the legitimate receiver on the secrecy performance. We note that the newly derived statistics have never been presented in the literature. We also note that they can serve as a powerful tool to examine the system performance in similar applications, e.g., exponentially correlated MIMO Rayleigh fading channels with outdated CSI.
3) We derive new closed-form expressions for the secrecy outage probability and the probability of non-zero secrecy capacity. These expressions offer us valuable insights into the joint impact of outdated antenna selection and exponential antenna correlation on the secrecy performance. To the best of our knowledge, these results have never been reported before. Moreover, we derive the asymptotic secrecy outage probability in order to examine the secrecy diversity order and the secrecy array gain at high SNRs. Furthermore, we highlight that the generality of our results lies in the fact that two special cases can be examined based on our results: 1. Outdated antenna selection only and 2. Exponential antenna correlation only.

Our results show that in low SNR regime, higher antenna correlation brings about a better secrecy performance, whereas in medium and high SNR regime, higher antenna correlation leads to a worse secrecy performance. These observations are due to the impact of antenna correlation on the secrecy array gain. Our results also show that the outdated antenna selection imposes a detrimental impact on the secrecy performance across the whole range of SNR. This impact is due to the fact that the outdated antenna selection reduces the secrecy diversity order from $N_A N_B$ to N_B. Moreover, our results show that the secrecy performance improvement provided by TAS becomes less profound when the selected antenna is more outdated. We further find that this improvement is almost not affected by the antenna correlation. In addition, we examine the impact of Eve's location on the secrecy performance.

Notation: Uppercase and lowercase bold symbols denote matrices and vectors, and italic symbols denote scalar variables. For a complex vector $\mathbf{x}$, $\|\mathbf{x}\|$ denotes the Euclidean norm and $(\mathbf{x})^H$ denotes the conjugate transpose. The $m \times m$ identity matrix is denoted by $\mathbf{I}_m$, and the expectation is denoted by $\mathrm{E}[\cdot]$.

II. A New Transmission Scheme with Outdated TAS

We consider a MIMOME wiretap channel, where the transmitter Alice, the receiver Bob, and the eavesdropper Eve are equipped with N_A, N_B, and N_E antennas, respectively. We assume that Eve is a passive eavesdropper such that the instantaneous CSI between Alice and Eve is not available at Alice and Bob. The channel between Alice and Bob is referred to as the main channel and the channel between Alice and Eve is referred to as the eavesdropper's channel. We assume independent but non-identical distributions between the main channel and the eavesdropper's channel such that they have different average SNRs. We also assume spatial correlation among the N_B antennas at Bob. In practise, spatial correlation among antennas arises due to the increase in the number of antennas and the reduction of inter-element spacing. We further assume no spatial correlation among the N_E antennas at Eve.

In the MIMOME wiretap channel, we consider that TAS is adopted at Alice to perform secure transmission. We focus on the practical scenario where the CSI associated with the selected antenna during the antenna selection process may be outdated for the subsequent data transmission. Outdated CSI is often caused by the long processing time and the long feedback propagation time between Alice and Bob during the TAS process. As such, outdated CSI leads to outdated antenna selection at the transmitter. We note that in the conventional TAS scheme for secure transmission, the CSI associated with the selected antenna is directly fed back from Bob to Alice during TAS process for wiretap codes construction [17–19]. Therefore, if the conventional TAS scheme is used for secure transmission in the presence of outdated antenna selection, a connection outage may occur in the main channel such that the transmitter transmits but the receiver cannot decode the message. In order to avoid this outage, we propose a new secure transmission scheme to guarantee that the perfect CSI is used for secure transmission. We next detail the frame structure and signaling procedures of our scheme as follows.

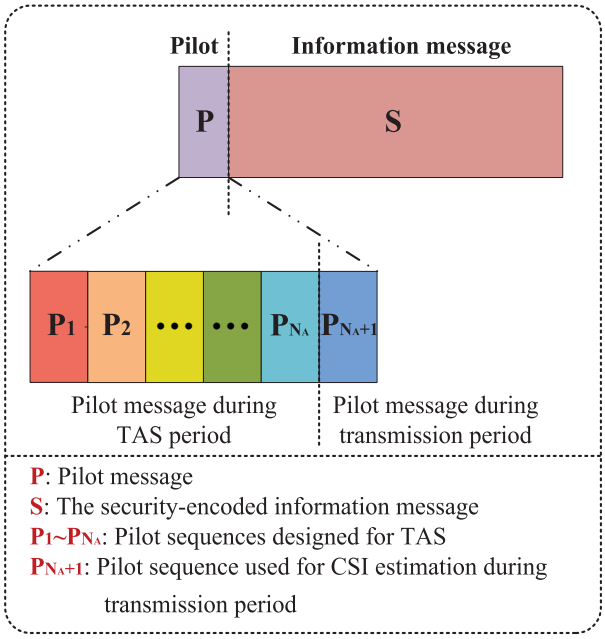

Fig. 1. The frame structure of TAS and secure transmission.

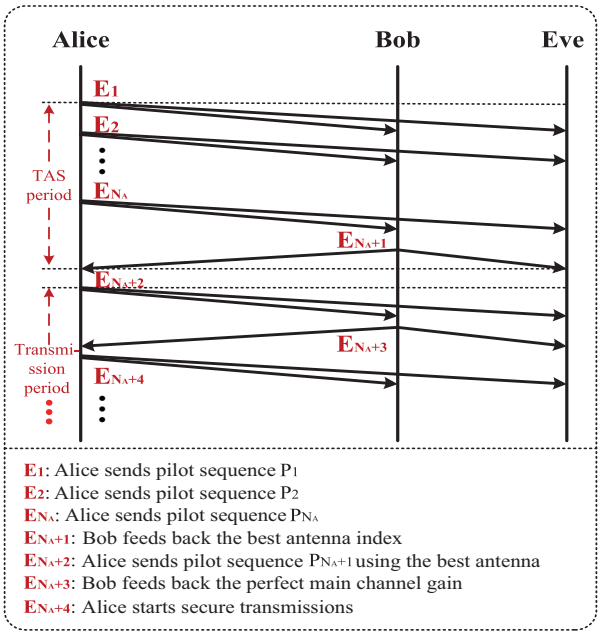

Fig. 2. Signaling procedure of TAS and secure transmission.

A. A New Secure Transmission Scheme

1) TAS Process: TAS is conducted based on the transmission and reception of the pilot sequences from P_1 to P_{N_A}, as illustrated in Fig. 1. The signaling procedure of the TAS process is performed via the operations from E_1 to E_{N_A+1}, as illustrated in Fig. 2. We next detail the steps of TAS.

1) Since there is only a RF chain at Alice, Alice transmits pilot sequences P_k, $1 \leq k \leq N_A$, from each transmit antenna at different time slots, starting with the transmission of P_1 from the first transmit antenna and ending with the transmission of P_{N_A} from the N_A-th transmit antenna.
2) With the aid of the pilot sequences, Bob estimates the channel vector between each transmit antenna and N_B receive antennas. As per the rule of TAS/MRC, Bob selects the optimal transmit antenna that maximizes the instantaneous SNR of the main channel.
3) Bob feeds back the index of the optimal transmit antenna, k^*, to Alice, which is determined as

$$k^* = \underset{1\leq k\leq N_A}{\operatorname{argmax}} \left\| \mathbf{\Phi}^{1/2}\mathbf{h}_{k,B} \right\|, \tag{1}$$

where $\mathbf{\Phi}$ denotes the $N_B \times N_B$ antenna correlation matrix at Bob and $\mathbf{h}_{k,B}$ denotes the $N_B \times 1$ channel vector between the kth transmit antenna and N_B antennas at Bob.

2) Secure Transmission: To perform secure transmission with the optimal transmit antenna k^*, Alice is required to

obtain the accurate instantaneous CSI of the main channel to facilitate the design of wiretap codes in the passive eavesdropping scenario. We note that it is not wise for Alice to use the instantaneous CSI associated with the k^*th transmit antenna during the TAS process to design wiretap codes since this CSI may be outdated due to the time delay of TAS. If Alice uses this CSI, Bob may not be able to decode the secure messages sent by Alice. Therefore, prior to secure data transmission, another pilot sequence P_{N_A+1} is transmitted from the k^*th transmit antenna at Alice to Bob for accurate channel estimation, as depicted in Fig. 1. The steps of secure transmission through the operations from E_{N_A+2} to E_{N_A+4}, as depicted in Fig. 2, are explained as follows.

1) Alice transmits the pilot sequence P_{N_A+1} from the k^*th transmit antenna that allows Bob to accurately estimate the channel vector between the k^*th transmit antenna and N_B receive antennas.
2) With the aid of P_{N_A+1}, Bob accurately estimates the channel vector between the k^*th transmit antenna and N_B receive antennas. Then Bob feeds back the instantaneous CSI of the main channel to Alice.
3) Alice encodes information messages into codewords using the instantaneous CSI fed back by Bob.

There are two feedback operations in our proposed transmission scheme, i.e., the optimal antenna index in time slot E_{N_A+1} and the accurate instantaneous CSI associated with the selected transmit antenna in time slot E_{N_A+3}. We find that this feedback design is different from the conventional TAS scheme which feeds back the optimal antenna index and the CSI associated with the selected transmit antenna together. Therefore, our newly designed transmission scheme only incurs an additional time slot as the added overhead but no extra information bit. The additional time slot guarantees that our proposed TAS scheme avoids using the outdated CSI.

B. Channel Knowledge with Outdated TAS

After the operations from E_1 to E_{N_A+4}, Alice performs secure transmission using the k^*th transmit antenna. The received signal vector at Bob is written as

$$\mathbf{y} = \sqrt{d_{AB}^{-\mu}}\mathbf{\Phi}^{1/2}\tilde{\mathbf{h}}_{k^*,B}x + \mathbf{n}_B, \tag{2}$$

where $\tilde{\mathbf{h}}_{k^*,B}$ denotes the τ_d time-delayed version of $\mathbf{h}_{k^*,B}$, $\mathbf{n}_B$ denotes the $N_B \times 1$ additive white Gaussian noise (AWGN) vector at Bob satisfying $\mathrm{E}\left[\mathbf{n}_B\mathbf{n}_B^H\right] = \mathbf{I}_{N_B}\sigma_B^2$, and σ_B^2 denotes the noise variance at each receive antenna of Bob. Moreover, we incorporate the path loss between Alice and Bob in (2) where d_{AB} is the distance between Alice and Bob and μ is the path-loss exponent. Using a generalization of outdated CSI model, known as a Gauss-Markov process [29], we formulate the relationship between $\tilde{\mathbf{h}}_{k^*,B}$ and $\mathbf{h}_{k^*,B}$ as

$$\tilde{\mathbf{h}}_{k^*,B} = \rho_d\mathbf{h}_{k^*,B} + \sqrt{1-\rho_d^2}\mathbf{e}_B, \tag{3}$$

where $\mathbf{e}_B$ is a random vector, the entries of which are i.i.d. zero-mean complex Gaussian random variables. In (3), the degree of "outdated CSI" is captured using ρ_d, the correlation coefficient between the CSI used for antenna selection and the CSI used for wiretap codes construction. In the literature, ρ_d is generally expressed using the Jake's autocorrelation model, given by $\rho_d = J_0\left(2\pi f_d\tau_d\right)$, where $J_0\left(\cdot\right)$ is the zeroth-order Bessel function of the first kind and f_d is the maximum Doppler frequency.

Bob applies MRC to process the received signal using a MRC weight $\mathbf{w}_B = \mathbf{\Phi}^{1/2}\tilde{\mathbf{h}}_{k^*,B}^H \Big/ \left\|\mathbf{\Phi}^{1/2}\tilde{\mathbf{h}}_{k^*,B}\right\|$. As such, the received signal at Bob after MRC is expressed as

$$y = \sqrt{d_{AB}^{-\mu}}\left\|\mathbf{\Phi}^{1/2}\tilde{\mathbf{h}}_{k^*,B}\right\| x + \mathbf{w}_B\mathbf{n}_B. \tag{4}$$

Based on (4), the instantaneous SNR of the main channel is written as

$$\tilde{\gamma}_B = \left\|\mathbf{\Phi}^{1/2}\tilde{\mathbf{h}}_{k^*,B}\right\|^2 P d_{AB}^{-\mu}/\sigma_B^2, \tag{5}$$

where P is the transmit power.

Since Alice has no knowledge about the eavesdropper's channel, we consider the worst-case scenario where perfect channel estimation is performed by Eve and no correlation exists among N_E antennas. Therefore, the received signal vector at Eve is given by

$$\mathbf{z} = \sqrt{d_{AE}^{-\nu}}\mathbf{h}_{k^*,E}x + \mathbf{n}_E, \tag{6}$$

where $\mathbf{h}_{k^*,E}$ denotes the $N_E \times 1$ channel vector between the k^* transmit antenna at Alice and N_E antennas at Eve, $\mathbf{n}_E$ denotes the $N_E \times 1$ AWGN vector at Eve satisfying $\mathrm{E}\left[\mathbf{n}_E\mathbf{n}_E^H\right] = \mathbf{I}_{N_E}\sigma_E^2$ and σ_E^2 denotes the noise variance at each receive antenna of Eve. Similar to (2), we incorporate the path loss between Alice and Eve into (6) where d_{AE} is the distance between Alice and Eve and ν is the path-loss exponent. In this worst-case scenario, Eve performs MRC to combine the received signals in order to maximize the probability of successful eavesdropping. Using the MRC weight given by $\mathbf{w}_E = \mathbf{h}_{k^*,E}^H \Big/ \left\|\mathbf{h}_{k^*,E}\right\|$, the received signal symbol at Eve after MRC is expressed as

$$z = \sqrt{d_{AE}^{-\nu}}\left\|\mathbf{h}_{k^*,E}\right\| x + \mathbf{w}_E\mathbf{n}_E. \tag{7}$$

Based on (7), the instantaneous SNR of the eavesdropper's channel is written as

$$\gamma_E = \left\|\mathbf{h}_{k^*,E}\right\|^2 P d_{AE}^{-\nu}/\sigma_E^2. \tag{8}$$

C. Wiretap Codes Design

Since Bob feeds back the instantaneous CSI to Alice prior to secure data transmission, Alice knows the instantaneous capacity of the main channel given by $\tilde{C}_B = \log_2\left(1+\tilde{\gamma}_B\right)$. Then Alice uses $\tilde{C}_B$ to construct wiretap codes such that Bob is always able to decode the transmitted signals. In the passive eavesdropping scenario, Alice does not have the knowledge of the instantaneous capacity of the eavesdropper's channel given by $C_E = \log_2\left(1+\gamma_E\right)$. Therefore, Alice assumes the instantaneous capacity of the eavesdropper's channel as $\hat{C}_E = \tilde{C}_B - R_s$ to perform secure data transmission [6], where R_s is a constant secrecy rate selected by Alice. Then Alice constructs the wiretap codes using $\tilde{C}_B$ and $\hat{C}_E$. If $\hat{C}_E \geq C_E$, the codewords guarantee perfect secrecy. If $\hat{C}_E < C_E$, Eve can eavesdrop on the transmitted data and the secrecy is

compromised. This mandates the use of the secrecy outage probability as a useful and well-accepted secrecy performance metric.

III. Secrecy Performance

In this section, we evaluate the secrecy performance of the TAS system with outdated antenna selection at Alice and exponential antenna correlation at Bob. In particular, we first focus on the exponential antenna correlation model and derive the joint statistics of bivariate generalized hyper-exponential distributions. We then derive new closed-form expressions for the exact cumulative density functions (CDFs) and probability density functions (PDFs) of $\tilde{\gamma}_B$ and γ_E. Based on these results, we analyze the exact and asymptotic secrecy performance of outdated antenna selection with exponential antenna correlation in MIMOME wiretap channels. In addition, valuable insights are gained to examine the individual impact of outdated antenna selection and exponential antenna correlation on the secrecy performance.

A. Statistics of $\tilde{\gamma}_B$ and γ_E

To commence our derivation of the statistical properties of $\tilde{\gamma}_B$, we first examine the CDFs and the PDFs of $\gamma_k = \left\|\mathbf{\Phi}^{1/2}\mathbf{h}_{k,B}\right\|^2 P d_{AB}^{-\mu}/\sigma_B^2$ and $\gamma_B = \left\|\mathbf{\Phi}^{1/2}\mathbf{h}_{k^*,B}\right\|^2 P d_{AB}^{-\mu}/\sigma_B^2$. We adopt the exponential correlation model since it is widely used to describe the scenario where multichannel reception is conducted over equal-spaced diversity antennas [30, 31]. The correlation matrix of this model is $\mathbf{\Phi} = \left[\rho_a^{|i-j|}\right]$, where $\rho_a \in (0,1)$ denotes the degree of correlation between antennas. In this case, the PDF of γ_k is obtained as [32, Eq. (11)]

$$f_{\gamma_k}(\gamma) = \sum_{u=1}^{N_B} \frac{\alpha_u}{\varphi_u \overline{\gamma}_B} \exp\left(-\frac{\gamma}{\varphi_u \overline{\gamma}_B}\right), \tag{9}$$

where $\overline{\gamma}_B = P d_{AB}^{-\mu}/\sigma_B^2$, $\varphi_1, \varphi_2, \cdots, \varphi_{N_B}$ denotes the distinct real eigenvalues of $\mathbf{\Phi}$ and

$$\alpha_u = \varphi_u^{N_B-1} \prod_{k=1,k\neq u}^{N_B} (\varphi_u - \varphi_k)^{-1}. \tag{10}$$

Based on (10), it is easy to find that α_u is a real number which satisfies $\sum_{u=1}^{N_B} \alpha_u = 1$. As such, we treat γ_k as a generalized hyper-exponential-distributed random variable (RV). Using $F_{\gamma_k}(\gamma) = \int_0^\gamma f_{\gamma_k}(\gamma)\, d\gamma$, the CDF of γ_k is obtained as

$$F_{\gamma_k}(\gamma) = 1 - \sum_{u=1}^{N_B} \alpha_u \exp\left(-\frac{\gamma}{\varphi_u \overline{\gamma}_B}\right). \tag{11}$$

Based on (5), we express $\tilde{\gamma}_k = \left\|\mathbf{\Phi}^{1/2}\tilde{\mathbf{h}}_{k,B}\right\|^2 P d_{AB}^{-\mu}/\sigma_B^2$ as the time-delayed version of γ_k. Since $\tilde{\mathbf{h}}_{k,B}$ has the same distribution as $\mathbf{h}_{k,B}$, $\tilde{\gamma}_k$ is also a generalized hyper-exponential distributed RV. We next derive the joint statistics of the bivariate generalized hyper-exponential distributions in the following lemma.

Lemma 1: The joint pdf of $\tilde{\gamma}_k$ and γ_k with correlation parameter ρ_d is derived as

$$f_{\tilde{\gamma}_k,\gamma_k}(x,y) = \sum_{u=1}^{N_B} \frac{\alpha_u \beta_u^2}{1-\rho_d^2} \exp\left(-\frac{\beta_u (x+y)}{1-\rho_d^2}\right) I_0\left(\frac{2\beta_u \rho_d \sqrt{xy}}{1-\rho_d^2}\right), \tag{12}$$

where $\beta_u = (\varphi_u \overline{\gamma}_B)^{-1}$ and $I_0(\cdot)$ denotes the zeroth-order modified Bessel function of the first kind.

Proof: The proof is given in Appendix A. ∎

Using the CDF and the PDF of γ_k, the PDF of γ_B is written as

$$f_{\gamma_B}(\gamma) = N_A \left[F_{\gamma_k}(\gamma)\right]^{N_A-1} f_{\gamma_k}(\gamma). \tag{13}$$

Based on the knowledge of probability theory, we formulate $f_{\tilde{\gamma}_B}(x)$ as

$$f_{\tilde{\gamma}_B}(x) = \int_0^\infty f_{\tilde{\gamma}_B|\gamma_B}(x|y) f_{\gamma_B}(y)\, \mathrm{d}y, \tag{14}$$

where

$$f_{\tilde{\gamma}_B|\gamma_B}(x|y) = \frac{f_{\tilde{\gamma}_k,\gamma_k}(x,y)}{f_{\gamma_k}(y)}. \tag{15}$$

We next present the PDF of $\tilde{\gamma}_B$ in the following lemma.

Lemma 2: The PDF of $\tilde{\gamma}_B$ is derived as

$$\begin{aligned} f_{\tilde{\gamma}_B}(x) =& N_A \sum_{n=0}^{N_A-1} \binom{N_A-1}{n} (-1)^n n! \sum_{\sum_{i=1}^{N_B} k_i = n} \\ &\times \left(\prod_{i=1}^{N_B} \frac{\alpha_i^{k_i}}{k_i!}\right) \sum_{i=1}^{N_B} \frac{\alpha_i \beta_i^2}{\beta_i + (1-\rho_d^2)\sum_{l=1}^{N_B} k_l \beta_l} \\ &\times \exp\left(-\frac{\left(\beta_i + \sum_{l=1}^{N_B} k_l \beta_l\right)\beta_i x}{\beta_i + (1-\rho_d^2)\sum_{l=1}^{N_B} k_l \beta_l}\right), \end{aligned} \tag{16}$$

where k_i, $i = 1, \cdots, N_B$ are nonnegative integers.

Proof: The proof is given in Appendix B. ∎

Using $F_{\tilde{\gamma}_B}(x) = \int_0^x f_{\tilde{\gamma}_B}(y)\, dy$, the CDF of $\tilde{\gamma}_B$ is obtained as

$$\begin{aligned} F_{\tilde{\gamma}_B}(x) =& 1 - N_A \sum_{n=0}^{N_A-1} \binom{N_A-1}{n} (-1)^n \sum_{\sum_{i=1}^{N_B} k_i = n} \\ &\times n! \left(\prod_{i=1}^{N_B} \frac{\alpha_i^{k_i}}{k_i!}\right) \sum_{i=1}^{N_B} \frac{\alpha_i \beta_i}{\beta_i + \sum_{l=1}^{N_B} k_l \beta_l} \\ &\times \exp\left(-\frac{\left(\beta_i + \sum_{l=1}^{N_B} k_l \beta_l\right)\beta_i x}{\beta_i + (1-\rho_d^2)\sum_{l=1}^{N_B} k_l \beta_l}\right). \end{aligned} \tag{17}$$

We next present the PDF of γ_E. It is worthwhile to note that the preselected transmit antenna at Alice corresponds to a random transmit antenna for Eve since it is entirely determined by the CSI of the main channel [16]. As such, we express the PDF of γ_E as [18]

$$f_{\gamma_E}(x) = \frac{x^{N_E-1}}{\Gamma(N_E)\, \overline{\gamma}_E^{N_E}} \exp\left(-\frac{x}{\overline{\gamma}_E}\right), \tag{18}$$

where $\overline{\gamma}_E = P d_{AE}^{-\nu}/\sigma_E^2$ is the average SNR of the eavesdropper's channel.

B. Secrecy Performance

1) Exact Secrecy Performance: The secrecy outage probability is defined as the probability that the achievable secrecy rate is less than a predetermined secrecy transmission rate R_s, below which the secure transmission is not guaranteed. According to this definition, we formulate the secrecy outage probability as $P_{out}(R_s) = \Pr\{C_s < R_s\}$, where $C_s = \max\left\{\tilde{C}_B - C_E, 0\right\}$.

We find that two outage events occur when $C_s < R_s$. The first outage event is that Alice does not transmit. This event occurs when $\tilde{C}_B \leq R_s$. The second outage event is that Alice transmits but the message is decodable at Eve and thus secrecy is compromised. This event occurs when $\tilde{C}_B > R_s$ and $C_s < R_s$. Therefore, the secrecy outage probability is expressed as

$$P_{out}(R_s) = \underbrace{\Pr\left\{\tilde{C}_B < R_s\right\}}_{\lambda_1} + \underbrace{\Pr\left\{C_s < R_s \middle| \tilde{C}_B > R_s\right\} \Pr\left\{\tilde{C}_B > R_s\right\}}_{\lambda_2}, \tag{19}$$

where λ_1 characterizes the probability of the first outage event and λ_2 characterizes the probability of the second outage event. Based on the probability theory, we simplify (19) as

$$P_{out}(R_s) = \int_0^\infty f_{\gamma_E}(\gamma_E) F_{\tilde{\gamma}_B}\left(2^{R_s}(1+\gamma_E) - 1\right) d\gamma_E. \tag{20}$$

Substituting (17) and (18) into (20) and solving the resultant integrals with the aid of [33, Eq. (3.381.1)], we derive $P_{out}(R_s)$ as

$$\begin{aligned} P_{out}(R_s) =& 1 - N_A \sum_{n=0}^{N_A-1} \binom{N_A-1}{n} \sum_{\sum_{i=1}^{N_B} k_i = n} n! \\ &\times (-1)^n \left(\prod_{i=1}^{N_B} \frac{\alpha_i^{k_i}}{k_i!}\right) \sum_{i=1}^{N_B} \frac{\alpha_i \beta_i}{\beta_i + \sum_{l=1}^{N_B} k_l \beta_l} \\ &\times \exp\left(-\vartheta\left(2^{R_s}-1\right)\right) \left(1 + \vartheta 2^{R_s} \overline{\gamma}_E\right)^{-N_E}, \end{aligned} \tag{21}$$

where $\vartheta = \frac{\left(\beta_i + \sum_{l=1}^{N_B} k_l \beta_l\right)\beta_i}{\beta_i + \left(1-\rho_d^2\right)\sum_{l=1}^{N_B} k_l \beta_l}$.

We highlight that (21) is derived in closed form and applies to the realistic scenario with exponential correlation at N_B antennas and outdated antenna selection in the main channel.

We next use (21) to evaluate the probability of non-zero secrecy capacity. The probability of non-zero secrecy capacity is defined as the probability that the achievable secrecy rate is positive. According to this definition, we formulate it as $\Pr\{C_s > 0\} = 1 - P_{out}(R_s)|_{R_s=0}$. Utilizing (21), we derive $\Pr\{C_s > 0\}$ as

$$\begin{aligned} \Pr\{C_s > 0\} =& N_A \sum_{n=0}^{N_A-1} \binom{N_A-1}{n} \sum_{\sum_{i=1}^{N_B} k_i = n} (-1)^n \\ &\times n! \left(\prod_{i=1}^{N_B} \frac{\alpha_i^{k_i}}{k_i!}\right) \sum_{i=1}^{N_B} \frac{\alpha_i \beta_i}{\beta_i + \sum_{l=1}^{N_B} k_l \beta_l} \left(1 + \vartheta \overline{\gamma}_E\right)^{-N_E}. \end{aligned} \tag{22}$$

2) Asymptotic Secrecy Performance: In this subsection, we provide valuable insights into the system design by evaluating the secrecy performance at high SNRs with $\overline{\gamma}_B \to \infty$. Here, $\overline{\gamma}_B \to \infty$ corresponds to the scenario where Bob is located much closer to Alice than Eve. The asymptotic result allows us to quantify the diversity loss induced by exponential correlation and outdated antenna selection.

At high SNRs, the asymptotic secrecy outage probability can be expressed as

$$P_{out}^{\infty}(R_s) = G\left(\overline{\gamma}_B\right)^{-d} + o\left(\overline{\gamma}_B^{-d}\right), \tag{23}$$

where d denotes the secrecy diversity order and describes how fast the secrecy outage probability decreases with increasing $\overline{\gamma}_B$, G denotes the secrecy array gain and characterizes the SNR advantage of the asymptotic outage probability relative to the reference curve $\overline{\gamma}_B^{-d}$, and $o(\cdot)$ denotes higher order terms [18]. We next present the secrecy diversity order and the secrecy array gain in the following theorem.

***Theorem** 1:* The secrecy diversity order is derived as

$$d = N_B, \tag{24}$$

and the secrecy array gain is derived as

$$\begin{aligned} G =& N_A \frac{(-1)^{N_B+1}}{\Gamma(N_B+1)} \sum_{n=0}^{N_A-1} \binom{N_A-1}{n} \sum_{\sum_{i=1}^{N_B} k_i = n} (-1)^n n! \\ &\times \left(\prod_{i=1}^{N_B} \frac{\alpha_i^{k_i}}{k_i!}\right) \sum_{i=1}^{N_B} \frac{\left(\varphi_i^{-1} + \sum_{l=1}^{N_B} k_l \varphi_l^{-1}\right)^{N_B-1}}{\left(\varphi_i^{-1} + (1-\rho_d^2)\sum_{l=1}^{N_B} k_l \varphi_l^{-1}\right)^{N_B}} \\ &\times \frac{\alpha_i}{\varphi_i^{N_B+1}} \sum_{t=0}^{N_B} \binom{N_B}{t} \frac{\Gamma(t+N_E) 2^{tR_s} \overline{\gamma}_E^t}{\Gamma(N_E)\left(2^{R_s}-1\right)^{t-N_B}}. \end{aligned} \tag{25}$$

Proof: The proof is given in Appendix C. ∎

Based on (24) we find that the outdated antenna selection reduces the secrecy diversity order from $N_A N_B$ to N_B. We highlight that it is possible to improve the secrecy diversity order if a subset of antennas, rather than a single antenna, out of all antennas at the transmitter are selected [34]. The effective design required by this improvement will be a potential extension of this work in future. The asymptotic result also reveals that the secrecy array gain in high SNRs, indicated by (25), is detrimentally influenced by antenna correlation and outdated antenna selection.

C. Special Case 1: Outdated Antenna Selection Only

In this section, we consider the independent fading case to merely examine the impact of the outdated antenna selection in the main channel. In this special case, no spatial correlation exists at N_B antennas, which means that the correlation matrix $\mathbf{\Phi} = \mathbf{I}_{N_B}$. Under this circumstance, the PDF of γ_k is easily obtained as

$$f_{\gamma_k}(x) = \frac{x^{N_B-1}}{\Gamma(N_B)\overline{\gamma}_B^{N_B}} \exp\left(-\frac{x}{\overline{\gamma}_B}\right), \tag{26}$$

We denote the accurate instantaneous SNR of the main channel in this case by γ_{B_1}. To derive the CDF of γ_{B_1}, we

need to resort to the bivariate gamma distribution, which has been given in [35]

$$f_{\tilde{\gamma}_k,\gamma_k}(x,y) = \frac{\left(xy/\rho_d^2\right)^{\frac{N_B-1}{2}}}{\left(1-\rho_d^2\right)\Gamma(N_B)\,\overline{\gamma}_B^{N_B+1}} \exp\left(\frac{-(x+y)}{\left(1-\rho_d^2\right)\overline{\gamma}_B}\right) \times I_{N_B-1}\left(\frac{2\rho_d\sqrt{xy}}{\left(1-\rho_d^2\right)\overline{\gamma}_B}\right), \quad (27)$$

where $\tilde{\gamma}_k$ is the τ_d time-delayed version of γ_k. Using (27), the CDF of γ_{B_1} is presented in the following lemma.

Lemma 3: The CDF of γ_{B_1} is derived as

$$F_{\gamma_{B_1}}(x) = \frac{N_A}{\Gamma(N_B)} \sum_{q=0}^{N_A-1} \binom{N_A-1}{q} \frac{(-1)^q}{(1+q)^{N_B}} \Xi(N_B,q) \times \frac{\Gamma(n_{sum}+N_B)}{\overline{\gamma}_B^{n_{sum}}} \left(\frac{\left(1-\rho_d^2\right)\overline{\gamma}_B}{1+q\left(1-\rho_d^2\right)}\right)^{n_{sum}} \times \sum_{k=0}^{n_{sum}} \binom{n_{sum}}{k} \frac{1}{\Gamma(k+N_B)} \left(\frac{\rho_d^2/\left(1-\rho_d^2\right)}{1+q}\right)^k \times \gamma\left(k+N_B, \frac{(1+q)\,x}{\left[1+q\left(1-\rho_d^2\right)\right]\overline{\gamma}_B}\right), \quad (28)$$

where $n_{sum} = 0$, $n_{prod} = 1$, $\Xi(N,q) = 1$ if $q = 0$, and $n_{sum} = \sum_{p=1}^{q}(n_p - 1)$, $n_{prod} = \prod_{p=1}^{q}\Gamma(n_p)$, $\Xi(N,q) = \sum_{n_1}^{N}\sum_{n_2}^{N}\cdots\sum_{n_q}^{N}\frac{1}{n_{prod}}$ if $q \geq 1$.

Proof: The proof is given in Appendix D. ∎

Substituting (18) and (28) into (20), the exact secrecy outage probability is derived as

$$P_{out}^{(1)}(R_s) = 1 - \frac{2^{R_s}N_A}{\Gamma(N_B)\overline{\gamma}_B{}^{N_B}} \sum_{q=0}^{N_A-1} \exp\left(\frac{(1+q)\left(1-2^{R_s}\right)}{\left[1+q\left(1-\rho_d^2\right)\right]\overline{\gamma}_B}\right) \times \binom{N_A-1}{q} \frac{\Xi(N_B,q)}{\overline{\gamma}_B{}^{n_{sum}}} \left(\frac{\left(1-\rho_d^2\right)\overline{\gamma}_B}{1+q\left(1-\rho_d^2\right)}\right)^{n_{sum}} \times \frac{\Gamma(n_{sum}+N_B)}{\left[1+q\left(1-\rho_d^2\right)\right]^{N_B}} \sum_{k=0}^{n_{sum}} \binom{n_{sum}}{k} \frac{(-1)^q}{\Gamma(k+N_B)} \times \left(\frac{\rho_d^2/\left[\left(1-\rho_d^2\right)\overline{\gamma}_B\right]}{1+q\left(1-\rho_d^2\right)}\right)^k \sum_{t=0}^{k+N_B-1} \binom{k+N_B-1}{t} \times \left(2^{R_s}-1\right)^{k+N_B-1-t} 2^{tR_s} \left\{\left[\frac{1+q\left(1-\rho_d^2\right)}{2^{R_s}(1+q)}\right]^{t+1} \times \Gamma(t+1)\,\overline{\gamma}_B^{t+1} - \sum_{s=0}^{N_E-1} \frac{\Gamma(s+t+1)}{\Gamma(s+1)\overline{\gamma}_E^{s}} \times \left[\frac{2^{R_s}(1+q)}{1+q\left(1-\rho_d^2\right)}\frac{1}{\overline{\gamma}_B} + \frac{1}{\overline{\gamma}_E}\right]^{-(s+t+1)}\right\}. \quad (29)$$

To derive the asymptotic secrecy outage probability $P_{out}^{(1)\infty}(R_s)$, the first non-zero order expansion of $F_{\gamma_{B_1}}(\gamma)$, $F_{\gamma_{B_1}}^{\infty}(\gamma)$, is given by

$$F_{\gamma_{B_1}}^{\infty}(x) = \frac{N_A}{\Gamma(N_B+1)\Gamma(N_B)} \sum_{q=0}^{N_A-1} \binom{N_A-1}{q} \Xi(N_B,q) \times \frac{\Gamma(n_{sum}+N_B)}{\overline{\gamma}_B^{n_{sum}}} \left(\frac{\left(1-\rho_d^2\right)\overline{\gamma}_B}{1+q\left(1-\rho_d^2\right)}\right)^{n_{sum}} \times \left(\frac{1+q}{1+q\left(1-\rho_d^2\right)}\right)^{N_B} \left(\frac{\gamma}{\overline{\gamma}_B}\right)^{N_B} + o\left(\overline{\gamma}_B^{-N_B}\right). \quad (30)$$

Based on these results, the secrecy diversity order and the secrecy array gain are derived as $d_1 = N_B$ and

$$G_1 = \frac{N_A}{\Gamma(N_B+1)\Gamma(N_B)} \sum_{q=0}^{N_A-1} \binom{N_A-1}{q} \frac{(-1)^q}{(1+q)^{N_B}} \times \Xi(N_B,q) \frac{\Gamma(n_{sum}+N_B)}{\overline{\gamma}_B^{n_{sum}}} \left(\frac{\left(1-\rho_d^2\right)\overline{\gamma}_B}{1+q\left(1-\rho_d^2\right)}\right)^{n_{sum}} \times \left(\frac{1+q}{1+q\left(1-\rho_d^2\right)}\right)^{N_B} \frac{1}{\Gamma(N_E)} \sum_{q=1}^{N_B} \binom{N_B}{q} \times \left(2^{R_s}-1\right)^{N_B-q} 2^{qR_s}\Gamma(q+N_E)\,\overline{\gamma}_E^{q}. \quad (31)$$

respectively. Comparing d_1 with the result in conventional TAS system [17], we find that the outdated antenna selection in the main channel reduces the secrecy diversity order from N_AN_B to N_B. In addition, comparing G_1 with G in (25), we find that the antenna correlation at Bob increases the secrecy array gain at high SNRs and thus reduces the secrecy outage performance.

D. Special Case 2: Exponential Antenna Correlation Only

In this section, TAS is conducted based on perfect CSI, while exponential antenna correlation exists among the N_B antennas. We denote the instantaneous SNR of the main channel in this special case by γ_{B_2}. We then derive the CDF of γ_{B_2} as

$$F_{\gamma_{B_2}}(x) = \left(1 - \sum_{u=1}^{N_B} \alpha_u \exp(-\beta_u x)\right)^{N_A}. \quad (32)$$

Substituting (18) and (32) into (20), the exact secrecy outage probability is derived as

$$P_{out}^{(2)}(R_s) = \sum_{n=0}^{N_A} \binom{N_A}{n} (-1)^n\, n! \sum_{\sum_{i=1}^{N_B} k_i = n} \left(\prod_{i=1}^{N_B} \frac{\alpha_i^{k_i}}{k_i!}\right) \times \frac{\exp\left(-\left(\sum_{i=1}^{N_B} k_i\beta_i\right)\left(2^{R_s}-1\right)\right)}{\left[1+2^{R_s}\overline{\gamma}_E\left(\sum_{i=1}^{N_B} k_i\beta_i\right)\right]^{N_E}}. \quad (33)$$

To derive the asymptotic secrecy outage probability $P_{out}^{(2)\infty}(R_s)$, the first non-zero order expansion of $F_{\gamma_{B_2}}(\gamma)$,

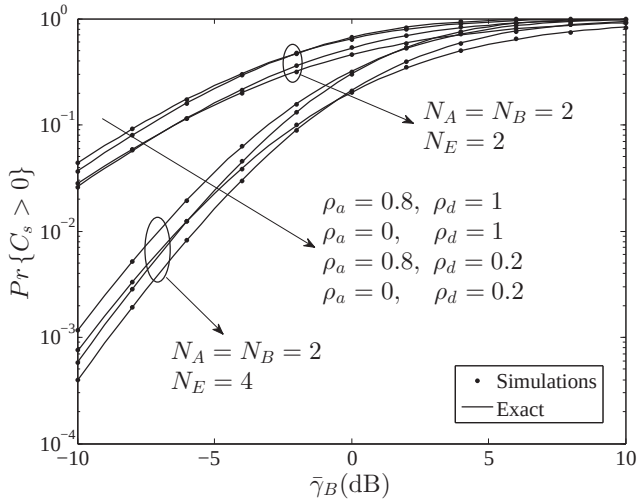

Fig. 3. The probability of non-zero secrecy capacity for $\overline{\gamma}_E = 0$ dB.

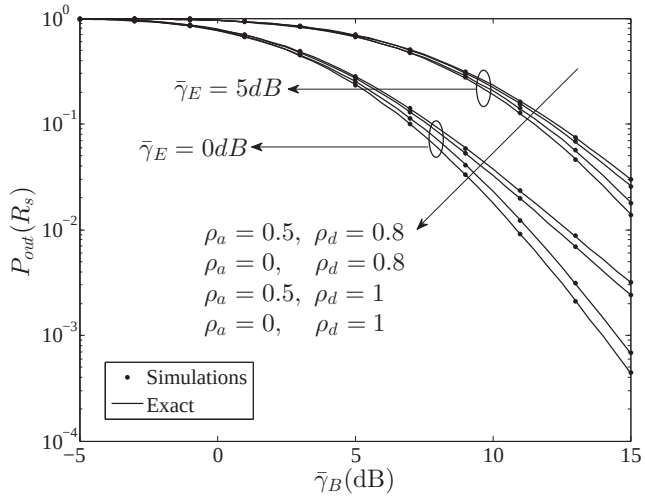

Fig. 4. The secrecy outage probability for $N_A = 2$, $N_B = 2$, $N_E = 2$, and $R_s = 1$.

$F^{\infty}_{\gamma_{B_2}}(\gamma)$, is obtained as

$$F^{\infty}_{\gamma_{B_2}}(\gamma) = \left(\frac{(-1)^{N_B+1}}{\Gamma(N_B+1)}\sum_{u=1}^{N_B}\frac{\alpha_u}{\varphi_u^{N_B}}\right)^{N_A}\left(\frac{\gamma}{\overline{\gamma}_B}\right)^{N_A N_B} + o\left(\overline{\gamma}_B^{-N_A N_B}\right). \quad (34)$$

Using (34), the secrecy diversity order and the secrecy array gain are derived as $d_2 = N_A N_B$ and

$$G_2 = \left(\frac{(-1)^{N_B+1}}{\Gamma(N_B+1)}\sum_{u=1}^{N_B}\frac{\alpha_u}{\varphi_u^{N_B}}\right)^{N_A}\sum_{q=1}^{N_A N_B}\binom{N_A N_B}{q} \times \frac{\Gamma(q+N_E)}{\Gamma(N_E)} 2^{R_s q}\left(2^{R_s}-1\right)^{N_A N_B - q}\overline{\gamma}_E^{q}, \quad (35)$$

respectively. Comparing d_2 with d in (24), we find that outdated antenna selection leads to a loss of the secrecy diversity order. That is, outdated antenna correlation reduces the transmit diversity from N_A to 1. We further confirm that the antenna correlation among the N_B antennas does not affect the diversity order.

IV. Numerical Results

We present numerical results in this section to examine the secrecy performance of the proposed TAS scheme in the presence of outdated antenna selection and antenna correlation. It is evident from Figs. 3 and 4 that the Monte Carlo simulation points, marked by '•', match precisely with the analytical curves, which demonstrates the accuracy of our analysis.

Fig. 3 plots the probability of non-zero secrecy capacity versus $\overline{\gamma}_B$ for different values of ρ_a and ρ_d. In this figure, we observe that the exponential correlation at N_B antennas is beneficial to the secrecy performance at low SNR, but detrimental to the secrecy performance at medium and high SNRs. For example, when $\overline{\gamma}_B < 0$ dB, $\Pr\{C_s > 0\}$ improves when ρ_a increases for $\rho_d = 0.2$ and $N_E = 4$. This observation is not surprising since the spatial correlation reduces the effective dimensionality at Bob at low $\overline{\gamma}_B$, which enables power focusing. Alternatively, when $\overline{\gamma}_B > 0$ dB, $\Pr\{C_s > 0\}$ decreases when ρ_a increases for $\rho_d = 0.2$ and $N_E = 4$. This is due to the fact that at medium and high $\overline{\gamma}_B$, higher ρ_a indicates the degraded quality of the main channel, which leads to a poorer secrecy performance. Moreover, we observe that the outdated antenna selection is detrimental to the secrecy performance for the whole range of $\overline{\gamma}_B$. For example, $\Pr\{C_s > 0\}$ decreases when ρ_d decreases for a fixed ρ_a. This performance loss is caused by the time delay during the TAS process. Furthermore, we observe that $\Pr(C_s > 0)$ significantly decreases as N_E increases. This is due to the fact that the use of multiple antennas at Eve brings a better quality of the eavesdropper's channel.

Fig. 4 plots the secrecy outage probability versus $\overline{\gamma}_B$ for different values of ρ_a, ρ_d and $\overline{\gamma}_E$. This figure demonstrates that when $\overline{\gamma}_B$ is high, antenna correlation and outdated antenna selection are detrimental to the secrecy performance. Specifically, $P_{out}(R_s)$ increases when ρ_a increases for a fixed ρ_d, but decreases when ρ_d increases for a fixed ρ_a. This can be explained by the fact that at high SNR, a higher ρ_a degrades the benefits of MRC at Bob and a lower ρ_d degrades the benefits of TAS at Alice. In addition, we observe that the secrecy outage probability increases when Eve moves closer to Alice (i.e., higher $\overline{\gamma}_E$). This is due to the fact that the shorter distance between Alice and Eve strengthens the eavesdropper's channel quality and thus weakens the secrecy performance.

Fig. 5 plots the exact and asymptotic secrecy outage probability versus $\overline{\gamma}_B$ for different values of ρ_a and ρ_d. Since our analytical results have been verified using Monte Carlo simulations in Figs. 3 and 4, we omit Monte Carlo simulation points in this figure to avoid unnecessarily cluttering. Note that G_0 and d_0 in this figure correspond to the conventional TAS scheme with perfect CSI but without antenna correlation [17]. We first observe that our asymptotic curves accurately predict the secrecy diversity order and the secrecy array gain. Moreover, we observe that the secrecy diversity order is not affected by ρ_a, but reduced by ρ_d, as indicated by $d_2 = d_0 =$

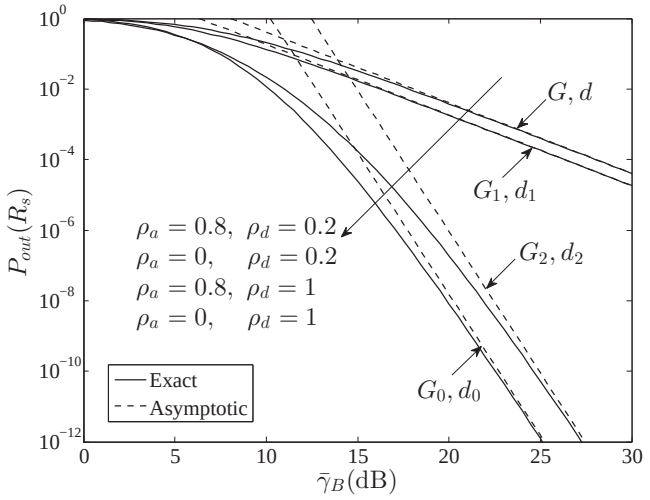

Fig. 5. The exact and asymptotic secrecy outage probability for $N_A = 4$, $N_B = 2$, $N_E = 4$, $\overline{\gamma}_E = 0$ dB, and $R_s = 1$.

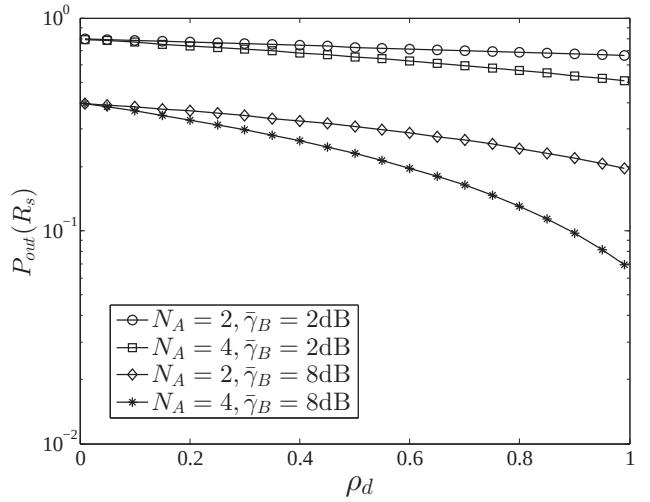

Fig. 6. The secrecy outage probability for $\rho_a = 0$, $N_B = 2$, $N_E = 4$, $\overline{\gamma}_E = 0$ dB, and $R_s = 1$.

$N_A N_B$ and $d = d_1 = N_B$. This observation demonstrates that outdated antenna selection, rather than antenna correlation at N_B antennas, leads to a loss of the secrecy diversity order. Furthermore, we observe that for a fixed ρ_d, a higher ρ_a brings about a poorer secrecy performance.

Fig. 6 plots the secrecy outage probability versus ρ_d for different values of N_A and $\overline{\gamma}_B$. In this figure, we do not consider the exponential antenna correlation such that $\rho_a = 0$. We first observe that the secrecy outage probability increases as ρ_d decreases. We also observe that for a fixed $\overline{\gamma}_B$, a higher N_A leads to an improvement in the secrecy performance for $\rho_d > 0$ but does not bring any improvement for $\rho_d = 0$. These observations indicate that a lower ρ_d reduces the benefits of TAS in security enhancement and $\rho_d = 0$ corresponds to the specific scenario where a completely random antenna is used for secure transmission and TAS does not offer any benefit. Based on this observation, we conclude that the

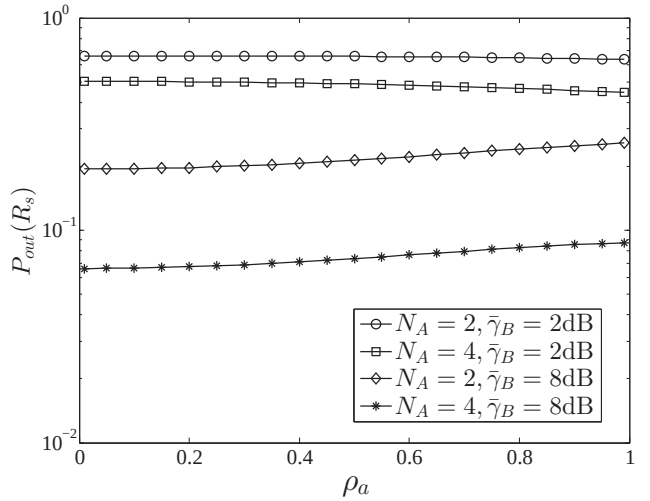

Fig. 7. The secrecy outage probability for $\rho_d = 1$, $N_B = 2$, $N_E = 4$, $\overline{\gamma}_E = 0$ dB, and $R_s = 1$.

improvement brought by a higher N_A to secrecy performance is sensitive to ρ_d. Furthermore, we observe that for a fixed N_A, a higher $\overline{\gamma}_B$ brings a significant improvement in the secrecy outage probability. Notably, this performance improvement diminishes when ρ_d decreases. Based on this observation, we conclude that the improvement brought by a higher $\overline{\gamma}_B$ to secrecy performance is also sensitive to ρ_d.

Fig. 7 plots the secrecy outage probability versus ρ_a for different values of N_A and $\overline{\gamma}_B$. In this figure, we consider perfect TAS such that $\rho_d = 1$. We first observe that $P_{out}(R_s)$ slightly decreases as ρ_a increases when $\overline{\gamma}_B = 2$ dB. When $\overline{\gamma}_B = 8$ dB, we observe that $P_{out}(R_s)$ slightly increases as ρ_a increases. Such an observation is in accordance with the fact that the antenna correlation is beneficial to the secrecy performance at low $\overline{\gamma}_B$ but detrimental to the secrecy performance at medium and high $\overline{\gamma}_B$. We also observe that for a fixed $\overline{\gamma}_B$, higher N_A offers a decrease in $P_{out}(R_s)$. Notably, such a decrease almost does not change as ρ_a increases. Based on this observation, we conclude that the improvement brought by higher N_A to the secrecy performance is not sensitive to ρ_a.

We now show the additional overhead added by our proposed transmission scheme, which is one time slot, is worthwhile. We have clarified that if we adopt the conventional TAS scheme in the presence of outdated CSI, an outage event, defined as $E_{co} = \{\gamma_B > \tilde{\gamma}_B\}$, occurs in the main channel. We refer to this outage event as the *connection outage* in this paper. This outage event is caused by the fact that the main channel capacity known at Alice during the TAS process is higher than the main channel capacity during the transmission process. To offer more insights into connection outage, Fig. 8 plots the connection outage probability versus N_A for different values of ρ_d. It is evident from this figure that the connection outage probability is always higher than 0.5, which implies that more than half of the transmitted information bits cannot be decoded at Bob if the conventional TAS scheme is adopted. We also note that if the conventional TAS scheme is used in the presence of outdated CSI, a higher

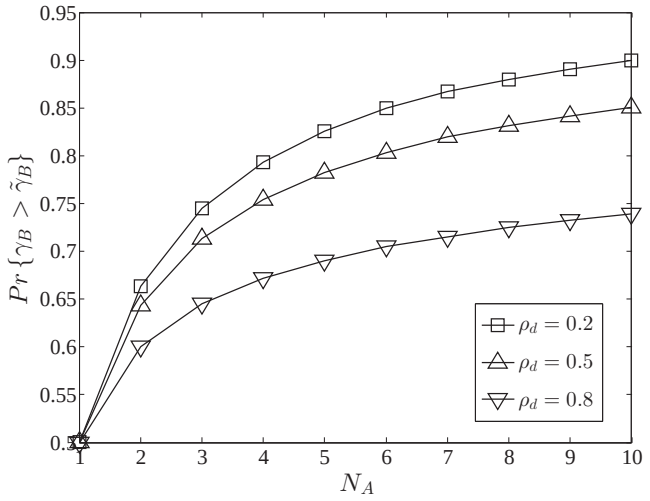

Fig. 8. The connection outage probability of the conventional TAS scheme in the presence of outdated CSI with $N_B = 2$ and $\overline{\gamma}_B = 10$ dB.

N_A brings a worse performance. This can be explained by the fact that a higher N_A leads to a higher probability that γ_B is greater than $\tilde{\gamma}_B$, due to the characteristics of Gauss-Markov process. In addition, the connection outage probability increases when ρ_d decreases for a fixed N_A. This is not surprising since a lower ρ_d reduces the benefits of TAS. All the aforementioned observations demonstrate the advantage of our proposed scheme relative to the conventional TAS scheme.

V. Conclusion

We presented a new secure transmission scheme that requires two feedback operations in different time slots to avoid the connection outage in the presence of outdated TAS. Based on our proposed scheme, we analyzed the secrecy performance with exponential antenna correlation at the legitimate receiver in MIMOME wiretap channels. New closed-form expressions were derived for the exact secrecy outage probability, the probability of non-zero secrecy capacity, and the asymptotic secrecy outage probability. Importantly, our asymptotic expressions demonstrated that the outdated TAS reduces the secrecy diversity order from $N_A N_B$ to N_B. Moreover, we demonstrated that at low $\overline{\gamma}_B$, higher antenna correlation brings a better secrecy performance, but at medium and high $\overline{\gamma}_B$, higher antenna correlation brings a worse secrecy performance. We further demonstrated that the secrecy performance improvement bought by increasing N_A is sensitive to ρ_d but not sensitive to ρ_a.

Appendix A
Proof of Lemma 1

Since $\tilde{\gamma}_k$ and γ_k are correlated generalized hyper-exponential distributed RVs, we use [36, Eq. (16)] to rewrite them as

$$\tilde{\gamma}_k = \sum_{i=1}^{N_B} \varphi_i \tilde{\gamma}_{i,k} \tag{36}$$

and

$$\gamma_k = \sum_{i=1}^{N_B} \varphi_i \gamma_{i,k}, \tag{37}$$

respectively, where $\tilde{\gamma}_{i,k}$ and $\gamma_{i,k}$ are exponentially distributed with $E[\tilde{\gamma}_{i,k}] = E[\gamma_{i,k}] = \bar{\gamma}_B$. The correlation coefficient between $\tilde{\gamma}_{i,k}$ and $\gamma_{i,k}$ is given by

$$\rho_d^2 = \frac{E[\tilde{\gamma}_{i,k} \cdot \gamma_{i,k}] - E[\tilde{\gamma}_{i,k}] E[\gamma_{i,k}]}{\sigma_{\tilde{\gamma}_{i,k}} \sigma_{\gamma_{i,k}}}, \tag{38}$$

where $\sigma_{\tilde{\gamma}_{i,k}}$ and $\sigma_{\gamma_{i,k}}$ are the variances of $\tilde{\gamma}_{i,k}$ and $\gamma_{i,k}$, respectively.

We note that the two dimensional MGF of the bivariate generalized hyper-exponential distribution is defined as

$$\psi_{\tilde{\gamma}_k,\gamma_k}(s_1,s_2) = \int_0^\infty \int_0^\infty f_{\tilde{\gamma}_k,\gamma_k}(x,y) \exp(-s_1 x - s_2 y)\, dx dy. \tag{39}$$

Recall that the joint MGF of two correlated Gamma distributed RVs is given by [37]

$$\psi_{X,Y}(s_1,s_2) = \left(\frac{1-\rho_d^2}{\left[1+\frac{s_1\bar{\gamma}/m}{\left(1-\rho_d^2\right)^{-1}}\right]\left[1+\frac{s_2\bar{\gamma}/m}{\left(1-\rho_d^2\right)^{-1}}\right] - \rho_d^2} \right)^m, \tag{40}$$

where $X = \sum_{i=1}^m x_i$ and $Y = \sum_{i=1}^m y_i$, x_i and y_i are exponentially distributed with $E[x_i] = E[y_i] = \bar{\gamma}/m$, and ρ_d is the correlation coefficient between x_i and y_i. With the aid of (40), $\psi_{\tilde{\gamma}_k,\gamma_k}(s_1,s_2)$ is written as

$$\psi_{\tilde{\gamma}_k,\gamma_k}(s_1,s_2) = \prod_{u=1}^{N_B} \frac{1-\rho_d^2}{\left[1+\frac{s_1\varphi_u\bar{\gamma}_B}{\left(1-\rho_d^2\right)^{-1}}\right]\left[1+\frac{s_2\varphi_u\bar{\gamma}_B}{\left(1-\rho_d^2\right)^{-1}}\right] - \rho_d^2}. \tag{41}$$

Using partial fraction, $\psi_{\tilde{\gamma}_k,\gamma_k}(s_1,s_2)$ can be further expressed as

$$\psi_{\tilde{\gamma}_k,\gamma_k}(s_1,s_2) = \sum_{u=1}^{N_B} \alpha_u \frac{1-\rho_d^2}{\left[1+\frac{s_1\varphi_u\bar{\gamma}_B}{\left(1-\rho_d^2\right)^{-1}}\right]\left[1+\frac{s_2\varphi_u\bar{\gamma}_B}{\left(1-\rho_d^2\right)^{-1}}\right] - \rho_d^2}. \tag{42}$$

Inverting $\psi_{\tilde{\gamma}_k,\gamma_k}(s_1,s_2)$ with respect to s_1 and s_2 successively, we obtain the joint PDF of $\tilde{\gamma}_k$ and γ_k as

$$f_{\tilde{\gamma}_k,\gamma_k}(x,y) = \sum_{u=1}^{N_B} \frac{\alpha_u}{\left(1-\rho_d^2\right)\left(\varphi_u\bar{\gamma}_B\right)^2} \exp\left(-\frac{x+y}{\left(1-\rho_d^2\right)\varphi_u\bar{\gamma}_B}\right) \times I_0\left(\frac{2\rho_d\sqrt{xy}}{\left(1-\rho_d^2\right)\varphi_u\bar{\gamma}_B}\right). \tag{43}$$

Setting $\beta_u = \left(\varphi_u\bar{\gamma}_B\right)^{-1}$, we obtain the desired result in (12).

Appendix B
Proof of Lemma 2

Substituting (13) and (15) into (14), we express $f_{\tilde{\gamma}_B}(x)$ as

$$f_{\tilde{\gamma}_B}(x) = N_A \int_0^\infty f_{\tilde{\gamma}_k,\gamma_k}(x,y) \left[F_{\gamma_k}(y)\right]^{N_A-1} \mathrm{d}y. \tag{44}$$

Using the generalized multinomial theorem given by

$$\left(\sum x_i\right)^n = \sum_{\sum k_i = n} \frac{n!}{\prod k_i!} \prod x_i^{k_i}, \tag{45}$$

we express $[F_{\gamma_k}(y)]^{N_A-1}$ as

$$[F_{\gamma_k}(y)]^{N_A-1} = \sum_{n=0}^{N_A-1} \binom{N_A-1}{n} (-1)^n \sum_{\sum_{i=1}^{N_B} k_i = n} n! \times \left(\prod_{i=1}^{N_B} \frac{\alpha_i^{k_i}}{k_i!}\right) \exp\left(-y \sum\nolimits_{i=1}^{N_B} k_i \beta_i\right). \tag{46}$$

We then use [33, Eq. (6.614.3)] to obtain the desired result in (16).

APPENDIX C
PROOF OF THEOREM 1

The asymptotic outage probability can be derived by using the method in [18]. We first apply Taylor's series to derive first nonzero order expansion $F_{\tilde{\gamma}_B}^{\infty}(\gamma)$

$$\begin{aligned} F_{\tilde{\gamma}_B}^{\infty}(\gamma) =& \frac{N_A (-1)^{N_B+1}}{\Gamma(N_B+1)} \sum_{n=0}^{N_A-1} \binom{N_A-1}{n} (-1)^n n! \\ &\times \sum_{\sum_{i=1}^{N_B} k_i = n} \left(\prod_{i=1}^{N_B} \frac{\alpha_i^{k_i}}{k_i!}\right) \sum_{i=1}^{N_B} \frac{\alpha_i}{\varphi_i^{N_B+1}} \\ &\times \frac{\left(\varphi_i^{-1} + \sum_{l=1}^{N_B} k_l \varphi_l^{-1}\right)^{N_B-1}}{\left(\varphi_i^{-1} + (1-\rho_d^2) \sum_{l=1}^{N_B} k_l \varphi_l^{-1}\right)^{N_B}} \\ &\times \left(\frac{\gamma}{\overline{\gamma}_B}\right)^{N_B} + o\left(\overline{\gamma}_B^{-N_B}\right). \end{aligned} \tag{47}$$

Substituting (18) and (47) into (20) and using [33, Eq. (3.381.1)] to solve the resultant integrals, we obtain the expressions for d in (24) and G in (25).

APPENDIX D
PROOF OF LEMMA 3

Substituting (27) and (50) into (44), we obtain the PDF of γ_{B_1} as

$$\begin{aligned} f_{\gamma_{B_1}}(x) =& \frac{N_A}{(1-\rho_d^2)\Gamma(N_B)(\overline{\gamma}_B)^{N_B+1}} \exp\left(-\frac{x}{(1-\rho_d^2)\overline{\gamma}_B}\right) \\ &\times \left(\frac{x}{\rho_d^2}\right)^{\frac{N_B-1}{2}} \sum_{q=0}^{N_A-1} \binom{N_A-1}{q} \frac{(-1)^q \Xi(N_B,q)}{\overline{\gamma}_B^{n_{sum}}} \\ &\times \int_0^{+\infty} y^{n_{sum}+\frac{N_B-1}{2}} \exp\left(-\frac{y + yq(1-\rho_d^2)}{(1-\rho_d^2)\overline{\gamma}_B}\right) \\ &\times I_{N_B-1}\left(\frac{2\rho_d\sqrt{xy}}{(1-\rho_d^2)\overline{\gamma}_B}\right) \mathrm{d}y. \end{aligned} \tag{48}$$

Using [33, Eq. (6.643.2)], [33, Eq. (9.220.2)], and [38], we obtain the following useful formulae as

$$\begin{aligned} &\int_0^{+\infty} x^{\mu-1/2} \exp(-\alpha x) I_{2v}\left(2\beta\sqrt{x}\right) dx \\ =&\Gamma(\mu+v+1/2)\,\alpha^{-(\mu+1/2)} \exp\left(\beta^2/\alpha\right) \\ &\times \sum_{k=0}^{\mu-v-1/2} \binom{\mu-v-1/2}{k} \frac{\left(\beta^2/\alpha\right)^{v+k}}{\Gamma(k+2v+1)}. \end{aligned} \tag{49}$$

Using (49) to solve the integral in (48), the PDF of γ_{B_1} is derived as

$$\begin{aligned} f_{\gamma_{B_1}}(x) =& \frac{N_A x^{N_B-1}}{\Gamma(N_B)\overline{\gamma}_B^{N_B}} \exp\left(\frac{-x}{(1-\rho_d^2)\overline{\gamma}_B}\right) \sum_{q=0}^{N_A-1} (-1)^q \\ &\times \binom{N_A-1}{q} \exp\left(\frac{\rho_d^2 x/(1-\rho_d^2)}{[1+q(1-\rho_d^2)]\overline{\gamma}_B}\right) \\ &\times \frac{\Xi(N_B,q)}{[1+q(1-\rho_d^2)]^{N_B}} \left(\frac{(1-\rho_d^2)\overline{\gamma}_B}{1+q(1-\rho_d^2)}\right)^{n_{sum}} \\ &\times \sum_{k=0}^{n_{sum}} \binom{n_{sum}}{k} \left(\frac{\rho_d^2 x/(1-\rho_d^2)}{[1+q(1-\rho_d^2)]\overline{\gamma}_B}\right)^k \\ &\times \frac{\Gamma(n_{sum}+N_B)}{\overline{\gamma}_B^{n_{sum}}\Gamma(k+N_B)}. \end{aligned} \tag{50}$$

Applying [33, Eq. (3.381.8)] we obtain $F_{\gamma_{B_1}}(x)$ in (28).

REFERENCES

[1] B. Schneier, "Cryptographic design vulnerabilities," *Computer*, vol. 31, no. 9, pp. 29–33, Sep. 1998.

[2] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[3] A. D. Wyner, "The wire-tap channel," *Bell Syst. Techn. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[5] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[6] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. M. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[7] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[8] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[9] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*, CRC Press, 2013.

[10] N. Yang, S. Yan, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial noise: Transmission optimization in multi-input single-output wiretap channels," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1771-1783, May 2015.

[11] N. Yang, M. Elkashlan, T. Q. Duong, J. Yuan, and R. Malaney, "Optimal transmission with artificial noise in MISOME wiretap channels," *IEEE Trans. Veh. Technol.*, accepted to appear.

[12] A. Khisti and G. Wornell, "Secure transmission with multiple antennas–I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.

[13] A. Khisti and G. Wornell, "Secure transmission with multiple antennas–II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[14] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[15] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: an optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.
[16] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, June 2012.
[17] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.
[18] N. Yang, P. L. 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.*, vol. 17, no. 9, pp. 1754-1757, Sep. 2013.
[19] S. Yan, N. Yang, R. Malaney, and J. Yuan, "Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels," *IEEE Trans. Wireless Commun.,*, vol. 13, no. 3, pp. 1656–1667, Mar. 2014.
[20] S. Sanayei and A. Nosratinia, "Antenna selection in MIMO systems," *IEEE Commun. Mag.*, vol. 42, no. 10, pp. 68–73, Oct. 2004.
[21] B. S. Tan, K. H. li and K. C. Teh, "Transmit antenna selection systems," *IEEE Veh. Technol. Mag.*, vol. 8, no. 3, pp. 104–112, Sep. 2013.
[22] H. Zhang, A. Molisch, and J. Zhang, "Applying antenna selection in WLANs for achieving broadband multimedia communications," *IEEE Trans. Broadcasting*, vol. 52, no. 4, pp. 475–482, Dec. 2006.
[23] V. Kristem, N. B. Mehta, and A. F. Molisch, "Optimal weighted antenna selection for imperfect channel knowledge from training," in *Proc. IEEE ICC*, Germany, June 2009, pp. 1–6.
[24] R.M. Radaydeh, "Receive maximal-ratio combining with outdated arbitrary transmit antenna selection in *Nakagami*-m fading," *IET Commun.*, vol. 3, no. 10, pp. 1638–1648, Oct. 2009.
[25] T. R. Ramya and S. Bhashyam, "Using delayed feedback for antenna selection in MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 8, no. 12, pp. 6059–6067, Dec. 2009.
[26] R. M. Radaydeh, "Impact of delayed arbitrary transmit antenna selection on the performance of rectangular QAM with receive MRC in fading channels," *IEEE Commun. Lett.*, vol. 13, no. 6, pp. 390–392, June 2009.
[27] A. M. Salhab and S. A. Zummo, "Performance of *N*th-best antenna selection diversity systems with co-channel interference and outdated channel information," *IET Commun.*, vol. 8, no. 10, pp. 1674–1683, July 2014.
[28] 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. Foren. Sec.*, vol. 7, no. 1, pp. 388–396, Feb., 2012.
[29] D. S. Michalopoulos, H. A. Suraweera, G. K. Karagiannidis, and R. Schober, "Amplify-and-forward relay selection with outdated channel estimates", *IEEE Trans. Commun.*, vol. 60, no. 5, pp. 1278–1290, May 2012.
[30] V. A. Aalo, "Performance of maximal-ratio diversity systems in a correlated Nakagami-fading environment," *IEEE Trans. Commun.*, vol. 43, no. 8, pp. 2360–2369, Aug. 1995.
[31] J. Luo, J. R. Zeidler, and S. McLaughlin, "Performance analysis of compact antenna arrays with MRC in correlated Nakagami fading channels," *IEEE Trans. Veh. Technol.*, vol. 50, no. 1, pp. 267–277, Jan. 2001.
[32] N. S. Ferdinand and N. Rajatheva, "Unified performance analysis of two-hop amplify-and-forwad relay systems with antenna correlation," *IEEE Trans. Wireless Commun.*, vol. 10, no. 9, pp. 3002–3011, Sep. 2011.
[33] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 7th Edition. Academic Press, 2007.
[34] H. Cui, R. Zhang, L. Song, and B. Jiao, "Relay selection for bidirectional AF relay network with outdated CSI," *IEEE Trans. Veh. Technol.*, vol. 62, no. 9, pp. 4357–4365, Nov. 2013.
[35] N. S. Ferdinand, N. Rajatheva, and M. Latva-aho, "Effects of feedback delay in partial relay selection over Nakagami-m fading channels," *IEEE Trans. Veh. Technol.*, vol. 61, no. 4, pp. 1620–1634, May 2012.
[36] A. Firag, P. J. Smith, H. A. Suraweera, and A. Nallanathan, "Performance of beamforming in correlated MISO systems with estimation error and feedback delay," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2592–2602, Aug. 2011.
[37] M. Nakagami, "The m-distribution - A general formula of intensity distribution of rapid fading," *Statistical Methods in Radio Wave Propagation*, N.Y.: Pergamon Press, 1960.
[38] Available: http://functions.wolfram.com/07.20.03.002