IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 13, 2017, accepted April 14, 2017, date of publication April 24, 2017, date of current version June 7, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2696032

ZF-SIC Based Individual Secrecy in SIMO Multiple Access Wiretap Channel

KAIWEI JIANG[1,2], TAO JING[1], FAN ZHANG[1], YAN HUO[1], (Member, IEEE), AND ZHEN LI[1]

[1]School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing 100044, China
[2]School of Electric and Information Engineering, Taizhou Vocational & Technical College, Zhejiang 318000, China

Corresponding author: Kaiwei Jiang (kwjiang@bjtu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61572070 and Grant 61371069 and in part by the Specialized Research Fund for the Doctoral Program of Higher Education under Grant 20130009110015.

ABSTRACT In this paper, a decoding method of joint zero-forcing and successive interference cancellation (ZF-SIC) is put forward to assist the study of the individual secrecy in the quasi-static Rayleigh fading single-input multiple-output multiple access wiretap channel. We first evaluate the individual secrecy performance by deriving the closed-form expressions in terms of positive secrecy capacity probability, secrecy outage probability, and effective secrecy throughput (EST). Besides the expected impact of the SIC order, we find, in high signal-to-noise ratio (SNR) regime, the secrecy performance is only determined by the transmitter's relative distance to eavesdropper over legitimate receiver rather than the SNR. Such a result prompts us to propose an SIC order scheduling scheme (alternative scheme) on basis of the transmitters' relative distances from the shortest to the longest. It is proved optimal in achieving total maximum EST in high SNR regime. Finally, we also investigate the problem of optimal power allocation to each transmitter under the constraint of the limited total power. An interesting solution to this problem is disclosed with the aid of numerical analysis.

INDEX TERMS Multiple access wiretap channel (MAC-WT), zero-forcing (ZF), successive interference cancellation (SIC), secrecy performance.

I. INTRODUCTION

With the increasing demands for mobility and ubiquitous connectivity, wireless communications have been playing an increasingly important role in our daily lives. Meanwhile, the broadcast nature of wireless communications makes the security and privacy issues full of challenges. Many techniques have been studied to overcome these issues. One of them is the physical layer security, which was first introduced by Wyner in his seminal work [1]. In that pioneering work, Wyner characterized the rate-equivocation region for the degraded wiretap channel, which was extended to more general non-degraded and Gaussian wiretap channel in [2] and [3], respectively. The secrecy capacity usually is the main metric of secrecy performance in the Gaussian scenario, where a non-zero secrecy rate can be achieved as long as the main channel is more favorable than the eavesdropper channel [3]. However, in the fading scenarios, more favorable main channel is not always guaranteed, which brings in another two secrecy performance metrics, *secrecy outage probability* and *ergodic secrecy capacity* [4], [5]. They show a positive secrecy rate is available even when the eavesdropper channel is more favorable on the average.

The secrecy transmissions for the multi-user scenario were also intensively studied. In a massive amount of work, the multi-user wiretap channel is usually modeled from the downlink. [6]–[9] characterize the problems without considering the existence of user interference to both the eavesdropper and the desired user. In [10], the downlink multi-user secrecy transmissions were implemented by a multi-beam directional modulation, where beamforming vector of the confidential message is designed to preserve its power as possible in the desired directions while the projection matrix of artificial noise is to minimize the effect on the desired directions. [11] introduced an original symbol phase rotated (OSPR) secure transmission scheme to defend against eavesdroppers employed with massive antennas for the downlink multi-user secrecy transmissions. The same scheme was applied for the uplink case in [12]. Another important work about multi-user wiretap channel from the perspective of uplink was introduced in [13]. However, the authors just

characterized how to schedule the users to achieve optimal multi-user diversity gain. The user interference is avoided deliberately in the designed model. Similar study was done in [14], by expanding to the multi-cell scenario. In contrast, [15] took the user interference into account, yet the study mainly focused on the achievable ergodic secrecy sum-rates rather than the secrecy performance of a single user.

Recently, a new paradigm of the multi-user wiretap channel is known as multiple access wiretap channel (MAC-WT), where multiple access (MAC) along with one eavesdropper is modeled to achieve secrecy transmissions. Here, the user interference to both the transmitters and the eavesdropper is taken into account. The Gaussian MAC-WT was first introduced by Ender Tekin *et al.* [16]. the authors identified the achievable secrecy rate regions by using codebooks generated randomly according to a Gaussian distribution, namely Gaussian signaling, for the degraded Gaussian MAC-WT. Later, the general case of Gaussian MAC-WT was extended in [17], and the Gaussian signaling is still used to achieve the secrecy rate regions. However, the secure degree of freedom (DoF) of these Gaussian signaling based achievable schemes mentioned above is zero, which motivates researchers for further work on the secure DoF of the MAC-WT [18], [19]. In [20], the secrecy rate is achievable with polar coding scheme via rate-splitting and different cooperative jamming strategies.

The fading MAC-WT was first addressed by Tekin and Yener [21], where they still utilize the Gaussian signaling together with cooperative jamming based schemes to provide the achievable ergodic secrecy rate regions just as in [17]. As expected, no secure DoF is available. [22] proposed a new achievable scheme to achieve secure DoF for the two users. [23] investigated the problem of maximizing the average secrecy sum rate with linear precoders in the fading cognitive multiple access wiretap channel, where the interference threshold is constrained at the multiple primary user receivers.

It is worth mentioning there are still many other literatures about the MAC-WT. Nevertheless, in all these works, the studies mainly focused on the signaling schemes to achieve the secrecy rate regions. That is, they only characterized the secrecy performance of the MAC-WT as a whole from information theoretic perspective without considering the specific decoding methods at the legitimate receiver.

In this work, we intend to address the MAC-WT from the perspective of the secrecy performance of an individual transmitter. The MAC-WT we consider is composed of one N-antenna desired receiver, one M-antenna eavesdropper and K single-antenna transmitters. We call it K-transmitter single-input multiple-output (SIMO) MAC-WT. Jiang *et al.* [24] have already investigated the individual performance of the K-user SIMO MAC-WT, where eavesdropper is assumed to be armed with single antenna. In this paper, we extend the single antenna to the multiple antennas for the eavesdropper, and re-derive the closed-form expressions of the secrecy performance. Moreover, we propose two schemes about how to schedule the SIC order for the legitimate receiver, and also study the problem of optimal power allocation to the transmitters, subject to the limited total power. The system model and channel conditions are similar to the assumption in [24]. The secrecy performance is also measured in terms of the positive secrecy capacity probability, secrecy outage probability and effective secrecy throughput. Differently, we only specialize the decoding method to the joint zero-forcing and SIC (ZF-SIC) at the legitimate receiver in this work.

The main contributions of the paper are summarized as follows

- Formulate the secrecy capacity of a single transmitter on basis of ZF-SIC decoding, and derive the cumulative distribution function (CDF) and probability density function (pdf) of signal-to-interference-plus-noise ratios (SINRs).
- Characterize the individual secrecy performance in terms of positive secrecy capacity probability, secrecy outage probability and effective secrecy throughput (EST); Evaluate the impacts of the SIC order, signal-to-noise ratio (SNR) and the number of antennas.
- Investigate the asymptotic behaviors of the individual secrecy performance, revealing the secrecy performance is only location-dependent in high SNR regime.
- Propose two SIC order scheduling scheme, round-robin scheme and alternative scheme, and prove the alternative scheme is optimal in achieving sum of maximum ESTs in high SNR regime.
- Study the problem of optimal power allocation under the constraint of the limited total power, and present an interesting solution to the problem.

The remainder of this paper is organized as follows. In Section II, we model the network and form the problem. The secrecy performance as well as the asymptotic behavior is investigated in Section III. Section IV comes up with two SIC order scheduling schemes. The problem of optimal power allocation is studied in Section V. Section VI aims to further examine the problem numerically. Finally, we draw the conclusion in Section VII.

Notation: Vectors and matrix are symbolized by a bold font and $\mathbf{I}_m$ denotes the $m \times m$ identity matrix. $||\cdot||$ is Euclidean norm of a vector, and $(\cdot)^H$ is Hermitian transpose operator. Sets are denoted by a script font. $\mathcal{A}\backslash\mathcal{B}$ denotes set $\mathcal{A}$ minus set $\mathcal{B}$, $\emptyset$ indicates empty set, and $|\cdot|$ indicates the cardinality of set. $\mathcal{CN}$ and χ^2_m specify circularly symmetric complex Gaussian distribution and the chi-squared distribution with m degrees of freedom, respectively. The logarithm function log is base 2, and $[\cdot]^+ = max(\cdot, 0)$.

II. SYSTEM MODEL

We consider one type of MAC-WT, as depicted in Fig. 1, where K single-antenna users $(U_1, \ldots, U_K)$ are intended to transmit their confidential messages to the N-antenna base station (BS) through a quasi-static Rayleigh fading MAC link, while the M-antenna eavesdropper (Eve) attempts to intercept

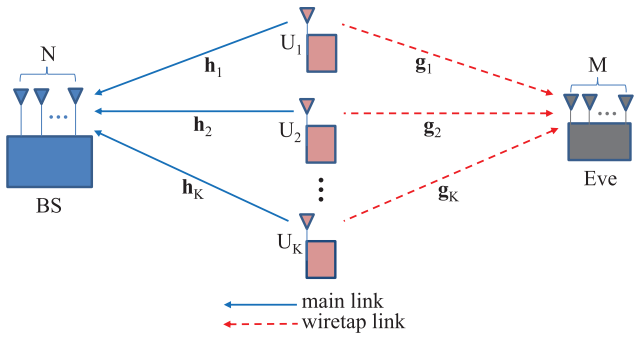


FIGURE 1. A model of quasi-static Rayleigh fading multiple access wiretap channel with one *N*-antenna BS, one *M*-antenna eavesdropper and *K* single-antenna users.

the data from one of the user (U_k) through another quasi-static Rayleigh fading link. Here, $N \geq K$ and $M \geq 1$ are assumed.

For all $k \in \mathcal{K} \triangleq \{1, \ldots, K\}$, we have the following notation descriptions:

- x_k is the desired signal sent from U_k, the transmit power of which is denoted by P_k.
- $\mathbf{h}_k$ and $\mathbf{g}_k$ are the main and eavesdropper's channel gain vectors for U_k, and suppose $\mathbf{h}_k \sim \mathcal{CN}(0, \delta_k^2 \mathbf{I}_N)$ and $\mathbf{g}_k \sim \mathcal{CN}(0, \sigma_k^2 \mathbf{I}_M)$.
- $\mathbf{n}$ and $\mathbf{w}$ are the additive zero-mean complex Gaussian noise vectors at BS and Eve, respectively. The corresponding covariance matrices are denoted as $N_b\mathbf{I}_N$ and $N_e\mathbf{I}_M$, i.e., $\mathbf{n} \sim \mathcal{CN}(0, N_b\mathbf{I}_N)$ and $\mathbf{w} \sim \mathcal{CN}(0, N_e\mathbf{I}_M)$.
- λ_k and μ_k are defined as $\lambda_k = \frac{N_b}{P_k\delta_k^2}$ and $\mu_k = \frac{N_e}{P_k\sigma_k^2}$.

Therefore, the instantaneous composite signals received at BS and Eve can be formulated as

$$\mathbf{y} = \sum_{i=1}^{K} \mathbf{h}_i x_i + \mathbf{n}, \tag{1}$$

$$\mathbf{z} = \sum_{i=1}^{K} \mathbf{g}_i x_i + \mathbf{w}. \tag{2}$$

A. INDIVIDUAL SECRECY CAPACITY

According to [4], in the quasi-static fading channels, the achievable instantaneous secrecy capacity is the difference between the instantaneous capacity of main and eavesdropper's channel. As such, we formulate the instantaneous secrecy capacity of an individual user, e.g., U_k, as

$$C_{s,k}^{(\Im)} = \left[C_{b,k}^{(\Im)} - C_{e,k}\right]^+, \tag{3}$$

where $C_{b,k}^{(\Im)} = \log(1 + \gamma_k^{(\Im)})$ and $C_{e,k} = \log(1 + \eta_k)$ are the corresponding instantaneous capacities of the main and eavesdropper's channel for U_k. The superscript $\Im$ indicates the dependence of the order of SIC decoding.

1) MAIN CAPACITY

We first re-write the expression in (1) by additionally considering the employment of the SIC decoding at the BS. In general, the aggregate signal left before decoding U_k at the BS can be expressed as,

$$\mathbf{y}_k^{(\Im)} = \mathbf{h}_k x_k + \sum_{i \in \Im} \mathbf{h}_i x_i + \mathbf{n}, \tag{4}$$

where $\Im \subseteq \mathcal{K} \backslash \{k\}$, indicating U_k is decoded just before user(s) in the set $\Im$ (index) during the SIC process. When $\Im = \mathcal{K} \backslash \{k\}$, (4) is equivalent to (1), specifying U_k is decoded at first. $\Im = \emptyset$ means no interference term in (4), showing U_k is decoded at final.

Obviously, the SINR of U_k at the BS (i.e., $\gamma_k^{(\Im)}$) not only depends on the SIC order, but also depends on the decoding method, which are specialized to ZF in this work.

The main idea of ZF-SIC decoding is to remove the interference term $\sum_{i \in \Im} \mathbf{h}_i x_i$ in (4) by projecting the aggregated signal $\mathbf{y}_k^{(\Im)}$ onto the subspace (denoted by $\mathbf{V}_k^{(\Im)}$, whose dimension is supposed to be $d_k^{(\Im)}$) orthogonal to the one spanned by the vectors $\mathbf{h}_i$ ($\forall i \in \Im$) [25]. The projection can be represented by $\mathbf{Q}_k^{(\Im)}\mathbf{y}_k^{(\Im)}$, where $\mathbf{Q}_k^{(\Im)}$ is a $d_k^{(\Im)}$ by N matrix and its rows form the orthonormal basis of $\mathbf{V}_k^{(\Im)}$. Due to the independence of vectors $\mathbf{h}_j$ ($\forall j \in \mathcal{K}$), the space spanned by the vectors $\mathbf{h}_i$ ($\forall i \in \Im$) is supposed to be full rank, hence, the dimension $d_k^{(\Im)}$ is exactly equal to $N - |\Im|$.

After interference nulling, (4) is transformed into $\mathbf{Q}_k^{(\Im)}\mathbf{y}_k^{(\Im)} = \mathbf{Q}_k^{(\Im)}\mathbf{h}_k x_k + \mathbf{Q}_k^{(\Im)}\mathbf{n}$. Applying maximal ratio combining (MRC), we get $\gamma_k^{(\Im)} = \frac{P_k ||\mathbf{Q}_k^{(\Im)}\mathbf{h}_k||^2}{N_b}$. Consequently, the main capacity can be formulated as

$$C_{b,k}^{(\Im)} = \log\left(1 + \frac{P_k ||\mathbf{Q}_k^{(\Im)}\mathbf{h}_k||^2}{N_b}\right). \tag{5}$$

2) WIRETAP CAPACITY

As for wiretap capacity of U_k, we directly characterize it with its upper bound expression for simplicity such that all users' interference is eliminated. Consequently, we obtain,

$$C_{e,k} = \log\left(1 + \frac{P_k ||\mathbf{g}_k||^2}{N_e}\right), \tag{6}$$

where the received SINR $\eta_k = \frac{P_k ||\mathbf{g}_k||^2}{N_e}$ is obtained with MRC at Eve.

B. STATISTICS OF SINRs

Since $\mathbf{h}_k \sim \mathcal{CN}(0, \delta_k^2 \mathbf{I}_N)$ and $\mathbf{Q}_k^{(\Im)}(\mathbf{Q}_k^{(\Im)})^H = \mathbf{I}_{N-|\Im|}$, $\mathbf{Q}_k^{(\Im)}\mathbf{h}_k \sim \mathcal{CN}(0, \delta_k^2 \mathbf{I}_{N-|\Im|})$, hence, $\frac{||\mathbf{Q}_k^{(\Im)}\mathbf{h}_k||^2}{\delta_k^2} \sim \chi^2_{2(N-|\Im|)}$, i.e., $\lambda_k \gamma_k^{(\Im)} \sim \chi^2_{2(N-|\Im|)}$. We note the statistic of $\gamma_k^{(\Im)}$ is dependent on the cardinality of $\Im$ rather than the specific user(s) in the set. For the notation convenience, we rewrite $\gamma_k^{(\Im)}$ to $\gamma_k^{(n)}$. Here, the superscript n denotes the cardinality of $\Im$, indicating the number of interferers.

The closed-form expression of CDF of $\gamma_k^{(n)}$ can be obtained according to [26],

$$F_{\gamma_k^{(n)}}(\gamma_k) = 1 - e^{-\lambda_k \gamma_k} \sum_{m=0}^{N-n-1} \frac{1}{m!} (\lambda_k \gamma_k)^m, \quad \gamma_k \geq 0. \tag{7}$$

Similarly, as the fact that $\mathbf{g}_k \sim \mathcal{CN}(0, \sigma_k^2 \mathbf{I}_M)$, it comes with $\frac{||\mathbf{g}_k||^2}{\sigma_k^2} \sim \chi^2_{2M}$, i.e., $\mu_k \eta_k \sim \chi^2_{2M}$. The closed-form expression of pdf for η_k is given by,

$$f_{\eta_k}(\eta_k) = \frac{\mu_k^M}{(M-1)!} \eta_k^{M-1} e^{-\mu_k \eta_k}, \quad \eta_k > 0. \tag{8}$$

III. SECRECY PERFORMANCE

In this section, we investigate the individual secrecy performance, called *secrecy performance* for short hereinafter, in terms of *positive secrecy capacity probability*, *secrecy outage probability*, ϵ*-outage secrecy capacity* and *effective secrecy throughput*. The closed-form expressions are derived and related performance analysis is conducted as well.

A. POSITIVE SECRECY CAPACITY PROBABILITY

Let us start with the positive secrecy capacity probability. From the definition of the secrecy capacity in (3), the positive secrecy capacity probability is equivalent to the probability that the SINR at the BS is greater than that at Eve. It can be formulated as

$$P_{ps,k}(n) = Pr\left(\gamma_k^{(n)} > \eta_k\right). \tag{9}$$

We present the closed-form expression of the positive secrecy capacity probability in the following theorem.

Theorem 1: The positive secrecy capacity probability of an individual user U_k is given by

$$P_{ps,k}(n) = \sum_{m=0}^{N-n-1} \binom{M+m-1}{M-1} \frac{\mu_k^M \lambda_k^m}{(\mu_k+\lambda_k)^{M+m}}. \tag{10}$$

Proof: See Appendix A. ∎

Observing (10), one can find that $P_{ps,k}(n)$ is a decreasing function of n which ranges from 0 to $K-1$. The cardinality $n = K-1$ indicates U_k is decoded at first, i.e., no user interference is eliminated, while $n = 0$ corresponds the best case of this user which is decoded at final. It also reveals U_k only needs to concern its own order "position" in the SIC process without caring other users'. An increase in the number of antennas N also makes $P_{ps,k}(n)$ increase as well, showing that the spatial diversity gain is available for this secrecy performance metric.

Interestingly, we can further evaluate this secrecy performance metric from the perspective of locations. In the path-loss model, we notice that $\lambda_k \propto d_{b,k}^{\alpha}$ and $\mu_k \propto d_{e,k}^{\alpha}$ (here, suppose $N_b = N_e$), where $d_{b,k}$ is the distance between U_k and BS, $d_{e,k}$ is the distance between U_k and Eve, and α is the path-loss exponent. (10) then can be transformed into

$$P_{ps,k}(n) = \sum_{m=0}^{N-n-1} \binom{M+m-1}{M-1} \frac{\left(\frac{d_{e,k}}{d_{b,k}}\right)^{\alpha M}}{\left\{1+\left(\frac{d_{e,k}}{d_{b,k}}\right)^{\alpha}\right\}^{M+m}}. \tag{11}$$

We note the positive secrecy capacity probability of U_k is only dependent on its relative distance to Eve over BS, besides its cardinality (i.e., n) and the number of antennas (i.e., N and M). It has nothing to do with its power as well as other users', which makes it possible for BS to calculate the positive secrecy capacity probability for all legitimate users in its cell against the potential eavesdropper (who might be switched from the legitimate user such that the BS also knows its location) according to their locations.

B. SECRECY OUTAGE PROBABILITY AND ϵ-OUTAGE SECRECY CAPACITY

The secrecy outage probability is defined as the probability of secrecy capacity that is less than a predefined secrecy rate R_s,

$$P_{so,k}(n, R_s) = Pr\left(C_{s,k}^{(n)} < R_s\right), \tag{12}$$

where the superscript $\Im$ of the secrecy capacity is automatically changed into n, as it is only dependent on the cardinality of the set $\Im$ rather than the specific users in the set according to our previous analysis.

Similarly, we state the closed-form expression of the secrecy outage probability in the form of theorem.

Theorem 2: The secrecy outage probability of an individual user U_k is given by

$$P_{so,k}(n, R_s) = 1 - \frac{\mu_k^M e^{-\lambda_k(2^{R_s}-1)}}{(M-1)!} \sum_{m=0}^{N-n-1} \frac{2^{R_s m} \lambda_k^m}{m!} \cdot \sum_{r=0}^{m} \binom{m}{r} \left(1-2^{-R_s}\right)^{m-r} \frac{(M-1+r)!}{(\mu_k+\lambda_k 2^{R_s})^{M+r}}. \tag{13}$$

Proof: See Appendix B. ∎

Apparently, $P_{so,k}(n, R_s)$ is an increasing function of n and/or R_s. Also, the spatial diversity gain of the legitimate receiver exists, as the increment of N reduces $P_{so,k}(n, R_s)$. Oppositely, the secrecy performance worsens when the number of antennas at Eve (i.e., M) increases.

The *secrecy transmission probability* is defined as the probability of secrecy capacity that is equal to or greater than a predefined secrecy rate, which is just the complement of secrecy outage probability. The expression is given by

$$P_{st,k}(n, R_s) = 1 - P_{so,k}(n, R_s). \tag{14}$$

It is, obviously, a decreasing function of n and/or R_s. Here, a special case of the secrecy transmission probability can be concluded, $P_{st,k}(n, 0) = P_{ps,k}(n)$.

Another performance metric which is always accompanied with the secrecy outage probability is ϵ*-outage secrecy capacity*. It is defined as the highest secrecy rate when the secrecy outage probability is not greater than ϵ, which can be defined as

$$P_{so,k}\left(n, C_{s,k}^{(n)}(\epsilon)\right) = \epsilon. \tag{15}$$

Here, $C_{s,k}^{(n)}(\epsilon)$ specifies ϵ-outage secrecy capacity of U_k.

Although the complexity of (13) leads to no closed-form expression of the ϵ-outage secrecy capacity, it is possible to obtain the result via numerical root-finding.

C. EFFECTIVE SECRECY THROUGHPUT

To further evaluate the average secrecy rate at which messages are transmitted to the legitimate receiver confidentially, we adopted another secrecy measure, called EST, which has been introduced in [27]. It is defined as the product of the secrecy rate R_s and the corresponding secrecy transmission probability $P_{st,k}(n, R_s)$,

$$T_k(n, R_s) = P_{st,k}(n, R_s) \times R_s. \tag{16}$$

Obviously, $T_k(n, R_s)$ is a decreasing function of n, as $P_{st,k}(n, R_s)$ is. Differently, since $P_{st,k}(n, R_s)$ is an exponentially decaying function of R_s, multiplying it with R_s makes the product rise at first and then decline quickly with R_s increasing, which indicates that there exists a maximum value for EST regarding R_s.

We call the secrecy rate to achieve the maximum EST as the *optimal secrecy rate*, denoted by $R_s^{*(n)}$. Intuitively, the optimal secrecy rate varies with different values of n. $R_s^{*(n)}$ with small value of n is greater than that with a big one, as $P_{st,k}(n, R_s)$ decays more slowly with small value of n.

The maximum EST is denoted as

$$T_{max,k}\left(n, R_s^{*(n)}\right) = P_{st,k}\left(n, R_s^{*(n)}\right) \times R_s^{*(n)}. \tag{17}$$

Notably, the maximum EST is not limited to the function of n and $R_s^{*(n)}$. It will be transformed into other form of representation if necessary later.

More numerical detail for the EST will be examined later in Section VI.

D. ASYMPTOTIC ANALYSIS

We continue to analyze the asymptotic behaviors of the secrecy performance for extreme values of N and SNR.

Without loss of generality, we omit the subscript k for the expressions and notations in this subsection, and it will be omitted automatically if necessary later in this work.

We start from the asymptotic behaviors with the extreme value of N first. When $N \to \infty$ for (7), $F_{\gamma^{(n)}}(\gamma)$ approaches to 0. Substituting it into the derivations in the Appendix A and B, we obtain,

$$P_{ps}(n) \xrightarrow[N]{a.s.} 1,$$
$$P_{so}(n, R_s) \xrightarrow[N]{a.s.} 0.$$

Thus, the asymptotic expression of EST for infinite value of N is

$$T(n, R_s) \xrightarrow[N]{a.s.} R_s,$$

where the optimal secrecy rate is limited to the related main capacity.

We move on to the asymptotic behaviors with the extreme value of SNR.

By setting the received average SNR at BS (on one diversity branch, denoted by $\overline{SNR_b}$) as the benchmark, the received average SNR at Eve (one diversity branch) is specified as $\overline{SNR_e} = \beta\overline{SNR_b}$, i.e., $\lambda/\mu = \beta$. Hereinafter, the "SNR" refers in particular to $\overline{SNR_b}$.

Assuming the ratio β is a non-zero value, with SNR approaching to ∞, λ and μ approach to 0. Consequently, we achieve the following asymptotic result for the infinite SNR from (13),

$$\begin{aligned} P_{so}(n, R_s) &\xrightarrow[SNR]{a.s.} 1 - \sum_{m=0}^{N-n-1} \binom{M+m-1}{M-1} \frac{2^{mR_s}(\frac{\mu}{\lambda})^M}{\left(\frac{\mu}{\lambda} + 2^{R_s}\right)^{M+m}} \\ &= 1 - \sum_{m=0}^{N-n-1} \binom{M+m-1}{M-1} \frac{2^{mR_s}(\frac{1}{\beta})^M}{\left(\frac{1}{\beta} + 2^{R_s}\right)^{M+m}}. \end{aligned} \tag{18}$$

The asymptotic expression for the EST can be obtained accordingly,

$$\begin{aligned} T(n, R_s) &\xrightarrow[SNR]{a.s.} \sum_{m=0}^{N-n-1} \binom{M+m-1}{M-1} \frac{2^{mR_s}(\frac{1}{\beta})^M}{\left(\frac{1}{\beta} + 2^{R_s}\right)^{M+m}} R_s \\ &= \sum_{m=0}^{N-n-1} \binom{M+m-1}{M-1} \frac{2^{mR_s}(\frac{d_e}{d_b})^{\alpha M} R_s}{\left((\frac{d_e}{d_b})^{\alpha} + 2^{R_s}\right)^{M+m}}, \end{aligned} \tag{19}$$

where we also further make the expression from the perspective of locations by replacing $1/\beta$ with $(d_e/d_b)^{\alpha}$.

We note the secrecy performance is only determined by the relative distance to Eve over BS rather than SNR in a high SNR regime.

IV. SIC ORDER SCHEDULING

Since the significant impact of the SIC order on the secrecy performance, we intend to explore the SIC order scheduling strategies from the viewpoint of the BS. We first come up with the round-robin scheduling, and then propose an alternative scheduling scheme.

A. ROUND-ROBIN SCHEME

The round-robin SIC order scheduling scheme is an absolutely fair strategy for each user to share all these possible SIC orders. Any individual user takes turns to hold one certain SIC order "position" from the first to the last (correspondingly from $n = K-1$ to $n = 0$) for an equal time. Thus, the average maximum EST for an individual user U_k can be given by

$$T_{max,k}^{av}\left(R_s^{*(0)}, \ldots, R_s^{*(K-1)}\right) = \frac{1}{K} \sum_{n=0}^{K-1} T_{max,k}\left(n, R_s^{*(n)}\right). \tag{20}$$

The total max-EST for this scheme is the sum of average maximum ESTs over all users.

To implement the round-robin scheduling, BS needs to access each corner point in the K-user capacity region with

SIC for an equal time. Here, one corner point corresponds one possible SIC order among these K users. To achieve total max-EST, BS has to calculate all optimal secrecy rates for these K users at each corner point. There are exactly $K!$ possible corner points in this capacity region. Hence, the computational complexity is enormous, especially when the value of K is big enough.

B. ALTERNATIVE SCHEME

The alternative scheme is based on the users' the relative distance to Eve over BS (d_e/d_b) in a certain time slot. To be concrete, the SIC order is sorted by Bob according to each user's the relative distance to Eve over BS from the shortest to the longest. That is, the user with shortest relative distance is decoded at first ($n = K-1$), while the user with longest relative distance is decoded at last ($n = 0$).

Such a scheduling scheme significantly simplifies the computational complexity. Moreover, it is more practical to know the location of Eve than knowing its' CSI. Most importantly, in a high SNR regime, the alternative scheme can achieve the most total max-EST (sum of maximum ESTs of all users). We state it in the following theorem.

Theorem 3: In high SNR regime, the alternative scheme is the optimal SIC order scheduling scheme in achieving the sum of the maximum ESTs over all users.

Proof: First, let us divert to state the notation of the maximum EST in high SNR regime. We note, from (19), the asymptotic expression for the EST is the function of n, R_s and d_e/d_b (ignore N and M temporarily). Thus, the maximum asymptotic EST over R_s is reduced to be the function of n and d_e/d_b. As such, we refer to it as $T_{max}^{(a.s.)}(n, \frac{d_e}{d_b})$.

Without loss of generality, we assume $\frac{d_{e,1}}{d_{b,1}} < \frac{d_{e,2}}{d_{b,2}} < \ldots < \frac{d_{e,K}}{d_{b,K}}$. With the alternative scheme, the SIC order is $U_1 \rightarrow U_2 \rightarrow \ldots \rightarrow U_K$ (U_1 is decoded first, the corresponding cardinality (n) for U_i is $K-i$, $i \in \mathcal{K}$). We say this SIC order permutation ($U_1 U_2 \ldots U_K$) is naturally ordered. As we know, any other permutations can be achieved via several steps of inversion from the naturally-ordered permutation. Taking a 5-permutation for instance, to achieve the permutation of $U_3U_2U_5U_1U_4$, three steps of inversion is enough: $U_1U_2U_3U_4U_5 \rightarrow U_1U_2U_3U_5U_4 \rightarrow U_1U_2U_5U_3U_4 \rightarrow U_3U_2U_5U_1U_4$. In the first step, the position exchange between U_4 and U_5 is an inversion. In the second step, the inversion takes place between U_3 and U_5, while the exchange of U_1 and U_3 is an inversion in the last step. Thus, as long as we can prove that any step of order position inversion will reduce the total maximum EST, the proof is done.

Assume $\frac{d_{e,i}}{d_{b,i}} < \frac{d_{e,j}}{d_{b,j}}$, $1 \le i < j \le K$, and U_i ($n = q$) is decoded before U_j ($n = p$) in the current SIC order. As such, the cardinality for U_i is greater than that for U_j, i.e., $q > p$. Let us exchange the positions of these two users but keep the other users' positions. Obviously, an inversion happens. In the new SIC order permutation, the cardinality for U_i is changed from q to p while the cardinality for U_j is changed to q. Thus, the difference of total maximum EST between old and new SIC orders is $T_{max}^{(a.s.)}(q, \frac{d_{e,i}}{d_{b,i}}) + T_{max}^{(a.s.)}(p, \frac{d_{e,j}}{d_{b,j}}) - T_{max}^{(a.s.)}(p, \frac{d_{e,i}}{d_{b,i}}) - T_{max}^{(a.s.)}(q, \frac{d_{e,j}}{d_{b,j}})$. Then, the problem is transformed into proving $T_{max}^{(a.s.)}(q, \frac{d_{e,i}}{d_{b,i}}) + T_{max}^{(a.s.)}(p, \frac{d_{e,j}}{d_{b,j}}) > T_{max}^{(a.s.)}(p, \frac{d_{e,i}}{d_{b,i}}) + T_{max}^{(a.s.)}(q, \frac{d_{e,j}}{d_{b,j}})$.

Although the closed-form expression of the function $T_{max}^{(a.s.)}(n, \frac{d_e}{d_b})$ is not available, we can prove the problem via the property of this function. We note the slope of this function with respect to d_e/d_b increases with n decreasing, which means the gap of two curves with different n will enlarge with d_e/d_b increasing. One can view it more clearly from Fig. 4, which is obtained via numerical root-finding. Therefore, we get $T_{max}^{(a.s.)}(p, \frac{d_{e,j}}{d_{b,j}}) - T_{max}^{(a.s.)}(q, \frac{d_{e,j}}{d_{b,j}}) > T_{max}^{(a.s.)}(p, \frac{d_{e,i}}{d_{b,i}}) - T_{max}^{(a.s.)}(q, \frac{d_{e,i}}{d_{b,i}})$. The proof is done. ■

Since the SIC order scheduled from the longest to the shortest relative distance has the most steps of inversion, it apparently achieves the least total max-EST. We present it with the following corollary.

Corollary 1: In high SNR regime, the worst SIC order scheduling scheme in achieving the sum of the maximum ESTs is reverting the alternative scheme, i.e., the user with the longest relative distance is decoded at first, while the user with the shortest relative distance is decoded at last.

V. OPTIMAL POWER ALLOCATION

In this section, we investigate the problem of optimal power allocation to the users in achieving the most total max-EST, subject to the limited total power P_{total}. Before going on, we need to revise the representation of the notation.

Observing (13), we note the maximum EST in (20) can be expressed as the function of n, β_k and P_k. Thus, we change the expression in (20) with $T_{max,k}(n, \beta_k, P_k)$, where $\beta_k = \lambda_k/\mu_k = (d_{b,k}/d_{e,k})^\alpha$.

We adopt the alternative scheme for scheduling the SIC order for these users. Without loss of generality, we assume $\beta_1 < \beta_2 < \ldots < \beta_K$, thus, the SIC order is $U_K \rightarrow \ldots \rightarrow U_2 \rightarrow U_1$. Accordingly, the cardinality (n) for U_i is $i-1$, $i \in \mathcal{K}$.

Consequently, the problem can be formulated as follows,

$$\max_{P_1,\ldots,P_K} \sum_{i=1}^{K} T_{max,i}(i-1, \beta_i, P_i)$$
$$\sum_{i=1}^{K} P_i = P_{total}$$
$$P_i \ge 0, i = 1, \ldots, K.$$

It can be solved explicitly by Lagrangian methods. The Lagrange function is given by

$$\mathcal{L}(P_1, \ldots, P_K, L) = \sum_{i=1}^{K} T_{max,i}(i-1, \beta_i, P_i) + L\left(P_{total} - \sum_{i=1}^{K} P_i\right), \quad (21)$$

where L is a Lagrange multiplier.

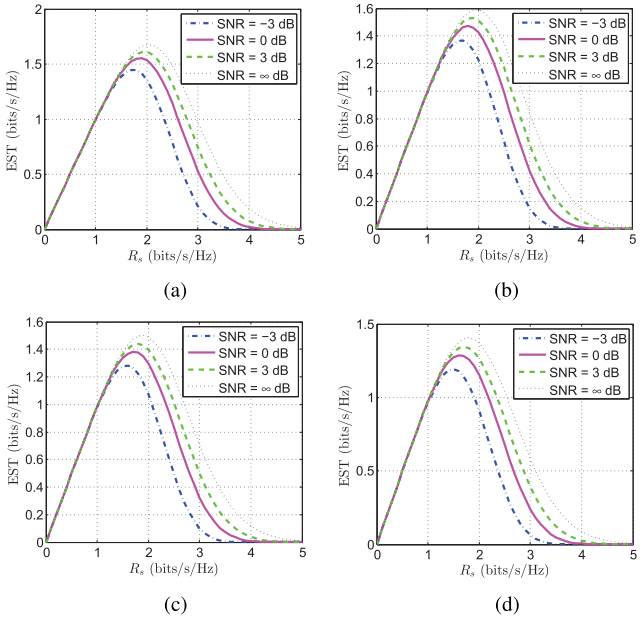


FIGURE 2. EST with regard to secrecy rate R_s for different SNRs at the assumption of $\beta = 1$. (a) $n = 0$. (b) $n = 2$. (c) $n = 4$. (d) $n = 6$.

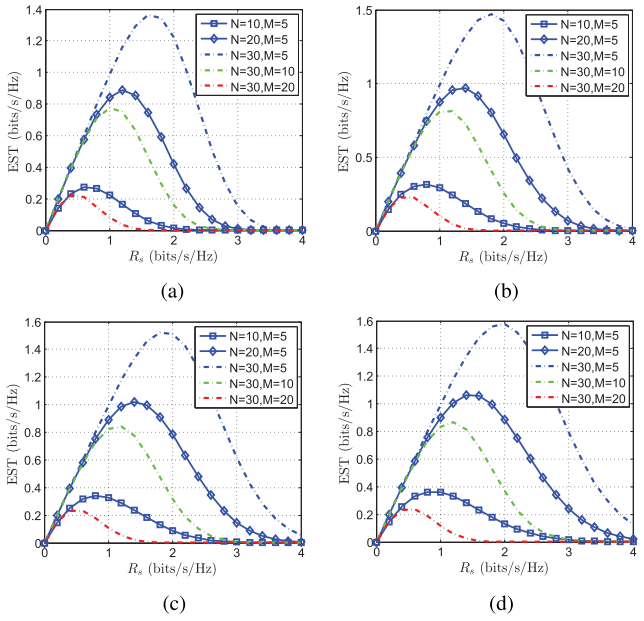


FIGURE 3. EST with regard to secrecy rate R_s for different number of antennas at BS and Eve ($n = 2$ and $\beta = 1$). (a) for SNR = -3 dB. (b) for SNR = 0 dB. (c) for SNR = 3 dB. (d) for SNR = 10 dB.

Making partial derivatives and setting $\frac{\partial \mathcal{L}}{\partial P_i} = 0$ ($\forall i \in \mathcal{K}$), we get $\frac{\partial T_{max,i}(i-1,\beta_i,P_i)}{\partial P_i} = L$. We refer to the optimal power as $[P_i^*(L)]^+$, which is subject to $\sum_{i=1}^{K}[P_i^*(L)]^+ = P_{total}$. We note the optimal power allocation point $(P_1^*, P_2^*, \ldots, P_K^*)$ makes all of the derivatives identical to each other. The problem can be solved numerically. It can be seen more clearly in Section VI.

VI. NUMERICAL RESULTS

We continue to examine the previous analytic results numerically in this section. Suppose the default values for both N and M are 30 and 5, respectively. Here, "SNR" and β have the same definitions as in Subsection III-D.

A. IMPACTS OF SNR AND SIC ORDER

Fig. 2 shows the relationship between EST and R_s for different values of SNR and n, where $\beta = 1$ is assumed. we can get the observations as follows:

- For a given SNR and n, the EST curves rise first and go down later regarding R_s.
- The EST is improved by high SNR.
- An decrease in n improves the EST, that is, the case of $n = 0$ achieves the most EST.

The first item of the observation verifies the inference in Subsection III-C that each EST curve has a maximum value, i.e., $T_{max}(n, R_s^{*(n)})$. Meanwhile, we note the optimal secrecy rate ($R_s^{*(n)}$) to achieve the maximum EST for each curve varies from SNR and n. The EST with low SNR will also obtain low optimal secrecy rate, while the less n achieves the higher $R_s^{*(n)}$. Although high SNR improves the EST, such an improvement has its limitation. Even SNR = 2 dB makes the EST very close to its asymptotic curve. Additionally, the EST difference for adjacent SIC order is not so significant, especially with high number of antennas in the legitimate receiver.

B. SPATIAL DIVERSITY

The Fig. 3 shows the impacts of the spatial diversity on the EST. We observe the EST increases dramatically with the increment of the number of the antennas at the BS, i.e., N, for all 4 different cases of SNR. Specifically, the maximum EST for $n = 2$ with $N = 10, M = 5$ in Fig. 3(c) is only 0.3416 bits/s/Hz, while it jumps to 1.0219 bits/s/Hz for $N = 20, M = 5$ with the same value of n, increasing almost 2 times. Moreover, it reaches 1.5283 bits/s/Hz for $N = 30, M = 5$. Although it continues to increase with N growing, the increment is getting weak, and the EST is finally limited to its channel capacity. Obviously, the spatial diversity gain improves the performance significantly, especially with high cardinality n (relative to N). Furthermore, such a spatial diversity gain can overcome the adverse impact incurred by low SNR. One can find that the maximum EST value for $N = 20$ and -3 dB is even significantly greater than that for 10 dB with $N = 5$. On the other hand, the increment of the number of the antennas at the Eve, i.e., M, worsens the performance significantly. The maximum EST declines from 1.5283 bits/s/Hz for $N = 30, M = 5$ to 0.8437 bits/s/Hz for $N = 30, M = 10$, and further down to 0.2413 bits/s/Hz for $N = 30, M = 20$. Therefore, from the perspective of the Eve, it also has the spatial diversity gain.

C. PERFORMANCE IN HIGH SNR REGIME

According to the analysis in Subsection III-D, in the high SNR regime, the secrecy performance is completely deter-

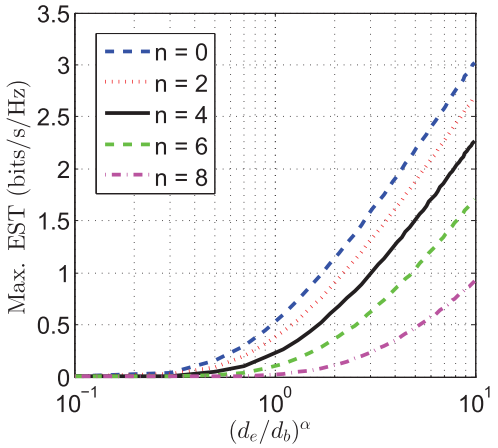


FIGURE 4. Maximum EST in high SNR regime with regard to relative distance to Eve over BS (d_e/d_b) for different cases of n.

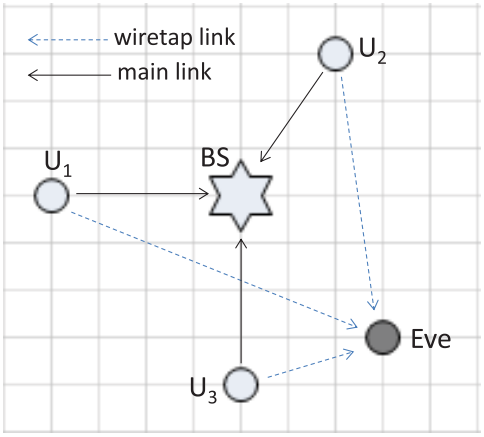


FIGURE 5. A scenario of one eavesdropper and 3 users in the cell, where BS knows all nodes' locations.

TABLE 1. Maximum EST and corresponding optimal secrecy rate (bits/s/Hz).

SIC order	U_1	U_2	U_3
$n=0$	4.1671 (4.46)	3.6807 (3.98)	0.9011 (1.31)
$n=1$	4.1179 (4.42)	3.6322 (3.94)	0.8668 (1.28)
$n=2$	4.0670 (4.37)	3.5820 (3.89)	0.8318 (1.25)

TABLE 2. Total max-EST for all possible SIC orders.

SIC orders	Total max-EST (bits/s/Hz)
$U_1 \to U_2 \to U_3$	8.6003
$U_1 \to U_3 \to U_2$	8.6145
$U_2 \to U_1 \to U_3$	8.6010
$U_2 \to U_3 \to U_1$	8.6159
$U_3 \to U_1 \to U_2$	8.6304
$U_3 \to U_2 \to U_1$	8.6311

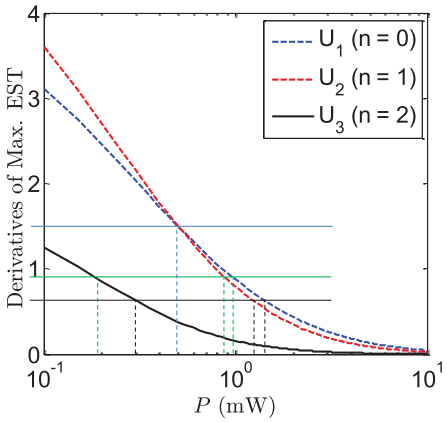


FIGURE 6. Derivatives of the maximum EST with respect to power. ($\alpha = 3$, $N_b = N_e = -10$ dBm).

mined by her relative distance to Eve over BS. Fig. 4 shows the maximum EST versus relative distance in the high SNR regime. We notice the slopes of the curves increase with n decreasing, which indicates the gap between any two curves with different n becomes bigger and bigger with relative distance increasing. Such a property is the key to prove Theorem 3.

To better understand Theorem 3, we continue to demonstrate it specifically with the aids of Fig. 5.

According to the topology in Fig. 5, the relative distances to Eve over BS for U_1, U_2 and U_3 are $\sqrt{58}/4$, $\sqrt{37}/\sqrt{13}$ and $\sqrt{10}/4$, respectively. The maximum ESTs as well as corresponding optimal secrecy rates are listed in Table 1 for all possible SIC orders via numerical root-finding. Here, the path-loss exponent is assumed $\alpha = 3$. Once again, we confirm that the optimal secrecy rate with low n is high. Moreover, the sum of maximum ESTs for all possible SIC orders are listed in Table 2. As expected, the alternative scheme (SIC order is $U_3 \to U_2 \to U_1$, which is also the natural order in this case) achieves the most total max-EST, while the order opposite to alternative scheme (i.e., $U_1 \to U_2 \to U_3$) results in the worst performance. Any order inversion can lead to a reduction of total max-EST. For instance, $U_1 \to U_3 \to U_2$ can be obtained by one-step inversion from $U_3 \to U_1 \to U_2$, and the corresponding total max-EST is reduced to 8.6145 bits/s/Hz from 8.6304 bits/s/Hz. Otherwise, the sum of maximum ESTs for the round-robin scheme is just the average value of the total max-ESTs listed in Table 2. It is obviously less than the alternative scheme regarding the total max-EST.

D. POWER ALLOCATION

We continue the scenario in Fig. 5 to numerically examine the optimal power allocation with the constraint of limited total power. Fig. 6 plots the derivatives of the maximum ESTs for all these three users, where the SIC order of these users is scheduled with alternative scheme. The noise power (one diversity branch) at both BS and Eve is assumed to be -10 dBm, i.e., $N_b = N_e = -10$ dBm. The path-loss exponent is still $\alpha = 3$. According to the analysis in Section V, the condition of the optimal power allocation point

is that each user has the same derivative of the maximum EST at its allocated power, that is, $T'_{max,1}(P_1^*) = T'_{max,2}(P_2^*) = T'_{max,3}(P_3^*)$, where $[P_1^*]^+ + [P_2^*]^+ + [P_3^*]^+ = P_{total}$. Here, $T'_{max,i}(\cdot)$ $(i = 1, 2, 3)$ denotes the derivative of the maximum EST. Therefore, the optimal power allocation point can be found by adjusting the baseline in Fig. 6 to make the sum of each corresponding power meet the total power. For instance, to allocate the total power of 1 mW, i.e., $P_{total} = 1$ mW, the baseline moving to the position of the blue line can achieve the optimal power allocation point for these three users, correspondingly, $P_1^* = 0.5$ mW, $P_2^* = 0.5$ mW, $[P_3^*]^+ = 0$ mW. The power allocation point of $P_{total} = 2$ mW is in the position of green line, where $P_1^* = 0.96$ mW, $P_2^* = 0.86$ mW and $P_3^* = 0.18$ mW. The black line is the position for the allocation point of $P_{total} = 3$ mW, where $P_1^* = 1.45$ mW, $P_2^* = 1.25$ mW and $P_3^* = 0.3$ mW. One can get all the power allocation points for other values of total power.

Overall, the numeric results and observations in this section are consistent with the expectations.

VII. CONCLUSION

In this work, we considered the quasi-static Rayleigh fading K-user SIMO MAC-WT and evaluated the individual secrecy performance based on ZF-SIC. We derived the closed-form expressions of positive secrecy capacity probability, secrecy outage probability and effective secrecy throughput. With the aid of the closed-form expressions and numerical results, we provided valuable insights into the impacts of the SIC order (i.e., n), SNR as well as the spatial diversity (i.e., N and M). It also showed, in high SNR regime, the secrecy performance is only determined by the relative distance to Eve over BS, independent of its SNR and the CSI of other users. Two SIC order scheduling schemes are proposed, round-robin and alternative scheme. The latter one is optimal in achieving total max-EST in high SNR regime. Finally, we studied the problem of optimal power allocation among the users with the constraint of the limited total power, and disclosed the solution to this problem.

APPENDIX A
PROOF OF THEOREM 1

Given the independence of $\gamma_k^{(n)}$ and η_k, jointly with (7) and (8), the positive secrecy capacity probability of U_k is derived as follows,

$$\begin{aligned}
P_{ps,k}(n) &= Pr\left(\gamma_k^{(n)} > \eta_k\right) \\
&= 1 - \int_0^\infty d\eta_k \int_0^{\eta_k} f_{\eta_k}(\eta_k) f_{\gamma_k^{(n)}}(\gamma_k) d\gamma_k \\
&= 1 - \int_0^\infty f_{\eta_k}(\eta_k) F_{\gamma_k^{(n)}}(\eta_k)\, d\eta_k \\
&= 1 - \int_0^\infty f_{\eta_k}(\eta_k) \left(1 - e^{-\lambda_k \eta_k} \sum_{m=0}^{N-n-1} \frac{1}{m!} \lambda_k^m \eta_k^m\right) d\eta_k \\
&= \int_0^\infty \frac{\mu_k^M \eta_k^{M-1}}{(M-1)!} e^{-\mu_k \eta_k} e^{-\lambda_k \eta_k} \sum_{m=0}^{N-n-1} \frac{1}{m!} \lambda_k^m \eta_k^m d\eta_k \\
&= \sum_{m=0}^{N-n-1} \frac{\mu_k^M \lambda_k^m}{(M-1)! m!} \int_0^\infty \eta_k^{M+m-1} e^{-(\lambda_k+\mu_k)\eta_k} d\eta_k \\
&= \sum_{m=0}^{N-n-1} \binom{M+m-1}{M-1} \frac{\mu_k^M \lambda_k^m}{(\mu_k+\lambda_k)^{M+m}},
\end{aligned} \tag{22}$$

where $f_{\gamma_k^{(n)}}(\gamma_k)$ is the pdf of $\gamma_k^{(n)}$.

This completes the proof.

APPENDIX B
PROOF OF THEOREM 2

The process of the derivation for the secrecy outage probability of U_k is shown as follows,

$$\begin{aligned}
P_{so,k}(n, R_s) &= Pr\left(\frac{1+\gamma_k^{(n)}}{1+\eta_k} < 2^{R_s}\right) \\
&= \int_0^\infty d\eta_k \int_0^{2^{R_s}\eta_k + 2^{R_s} - 1} f_{\eta_k}(\eta_k) f_{\gamma_k^{(n)}}(\gamma_k)\, d\gamma_k \\
&= \int_0^\infty f_{\eta_k}(\eta_k)\, F_{\gamma_k^{(n)}}\left(2^{R_s}\eta_k + 2^{R_s} - 1\right) d\eta_k \\
&= 1 - \int_0^\infty \frac{\mu_k^M \eta_k^{M-1}}{(M-1)!} e^{-\mu_k \eta_k} \sum_{m=0}^{N-n-1} \frac{\lambda_k^m \left(2^{R_s}\eta_k + 2^{R_s} - 1\right)^m}{m! e^{\lambda_k\left(2^{R_s}\eta_k + 2^{R_s} - 1\right)}} d\eta_k \\
&= 1 - \frac{\mu_k^M e^{-\lambda_k(2^{R_s}-1)}}{(M-1)!} \sum_{m=0}^{N-n-1} \frac{2^{R_s m} \lambda_k^m}{m!} \\
&\quad \cdot \int_0^\infty \frac{\eta_k^{M-1} (\eta_k + 1 - 2^{-R_s})^m}{e^{(\mu_k + \lambda_k 2^{R_s})\eta_k}} d\eta_k \\
&\overset{(a)}{=} 1 - \frac{\mu_k^M e^{-\lambda_k(2^{R_s}-1)}}{(M-1)!} \sum_{m=0}^{N-n-1} \frac{2^{R_s m} \lambda_k^m}{m!} \\
&\quad \cdot \sum_{r=0}^{m} \binom{m}{r} \left(1 - 2^{-R_s}\right)^{m-r} \int_0^\infty \frac{\eta_k^{M-1+r}}{e^{(\mu_k + \lambda_k 2^{R_s})\eta_k}} d\eta_k \\
&= 1 - \frac{\mu_k^M e^{-\lambda_k(2^{R_s}-1)}}{(M-1)!} \sum_{m=0}^{N-n-1} \frac{2^{R_s m} \lambda_k^m}{m!} \\
&\quad \cdot \sum_{r=0}^{m} \binom{m}{r} \left(1 - 2^{-R_s}\right)^{m-r} \frac{(M-1+r)!}{(\mu_k + \lambda_k 2^{R_s})^{M+r}},
\end{aligned} \tag{23}$$

where the binomial theorem is applied in step (a).

The proof has been completed.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
[2] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
[3] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.
[4] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006, pp. 356–360.

[5] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[6] N. Li, X. Tao, and J. Xu, "Ergodic secrecy sum-rate for downlink multiuser MIMO systems with limited CSI feedback," *IEEE Commun. Lett.*, vol. 18, no. 6, pp. 969–972, Jun. 2014.

[7] H. Dong and S. Wang, "On ergodic secrecy rate of multiuser MISO downlink wiretap channel," in *Proc. ICSP*, Oct. 2014, pp. 1590–1594.

[8] N. Li, X. Tao, Q. Cui, and J. Xu, "Secure transmission with artificial noise in the multiuser downlink: Secrecy sum-rate and optimal power allocation," in *Proc. WCNC*, Mar. 2015, pp. 1416–1421.

[9] X. Ge, P. Wu, H. Jin, and V. C. M. Leung, "Secrecy analysis of multiuser downlink wiretap networks with opportunistic scheduling," in *Proc. ICC*, Jun. 2015, pp. 7370–7375.

[10] F. Shu, X. Wu, J. Li, R. Chen, and B. Vucetic, "Robust synthesis scheme for secure multi-beam directional modulation in broadcasting systems," *IEEE Access*, vol. 4, pp. 6614–6623, 2016.

[11] B. Chen, C. Zhu, W. Li, J. Wei, V. C. M. Leung, and L. T. Yang, "Original symbol phase rotated secure transmission against powerful massive MIMO eavesdropper," *IEEE Access*, vol. 4, pp. 3016–3025, 2016.

[12] B. Chen *et al.*, "Securing uplink transmission for lightweight single-antenna UEs in the presence of a massive MIMO eavesdropper," *IEEE Access*, vol. 4, pp. 5374–5384, 2016.

[13] H. Jin, W.-Y. Shin, and B. C. Jung, "On the multi-user diversity with secrecy in uplink wiretap networks," *IEEE Commun. Lett.*, vol. 17, no. 9, pp. 1778–1781, Sep. 2013.

[14] H. Jin, B. C. Jung, and W.-Y. Shin, "On the secrecy capacity of multi-cell uplink networks with opportunistic scheduling," in *Proc. ICC*, May 2016, pp. 1–5.

[15] H. Deng, H.-M. Wang, J. Yuan, W. Wang, and Q. Yin, "Secure communication in uplink transmissions: User selection and multiuser secrecy gain," *IEEE Trans. Commun.*, vol. 64, no. 8, pp. 3492–3506, Aug. 2016.

[16] E. Tekin, S. Şerbetli, and A. Yener, "On secure signaling for the Gaussian multiple access wire-tap channel," in *Proc. Asilomar Conf. Signals, Syst. Comput.*, Nov. 2005, pp. 1747–1751.

[17] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[18] J. Xie and S. Ulukus, "Secure degrees of freedom of the Gaussian multiple access wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2013, pp. 1337–1341.

[19] P. Mukherjee and S. Ulukus, "Secure degrees of freedom of the MIMO multiple access wiretap channel," in *Proc. Asilomar Conf. Signals, Syst. Comput.*, Nov. 2015, pp. 554–558.

[20] R. A. Chou and A. Yener, "Polar coding for the multiple access wiretap channel via rate-splitting and cooperative jamming," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2016, pp. 983–987.

[21] E. Tekin and A. Yener, "Secrecy sum-rates for the multiple-access wire-tap channel with ergodic block fading," in *Proc. Annu. Allerton Conf.*, Allerton, IL, USA, Sep. 2007, pp. 856–863.

[22] R. Bassily and S. Ulukus, "A new achievable ergodic secrecy rate region for the fading multiple access wiretap channel," in *Proc. Annu. Allerton Conf.*, Sep. 2009, pp. 819–826.

[23] J. Jin, C. Xiao, M. Tao, and W. Chen, "Linear precoding for fading cognitive multiple-access wiretap channel with finite-alphabet inputs," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3059–3070, Apr. 2016.

[24] K. Jiang, T. Jing, Z. Li, Y. Huo, and F. Zhang, "Analysis of secrecy performance in fading multiple access wiretap channel with sic receiver," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, May 2017, p. 9.

[25] D. Tse and P. Viswanath, *Fundamentals Wireless Communication*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[26] J. G. Proakis, *Digital Communications*, 4th ed. New York, NY, USA: McGraw-Hill, 2001.

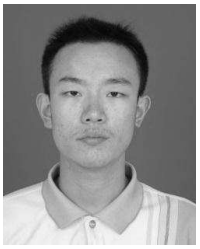
[27] N. Yang, S. Yan, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial noise: Transmission optimization in multi-input single-output wiretap channels," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1771–1783, May 2015.

KAIWEI JIANG received the B.S. degree from Northeast University, China, in 2004 and the M.S. degree from Beijing Jiaotong University, in 2007. He is currently pursuing the Ph.D. degree with Shu Hua Wireless Network and Information Perception Center, Beijing Jiaotong University. His research interests are cognitive radio networks and physical layer security.

TAO JING received the M.S. and Ph.D. degrees in the Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, in 1994 and 1999, respectively. He is currently a Professor with the School of Electronic and Information Engineering, Beijing Jiaotong University, China. His current research interests include capacity analysis, spectrum prediction and resource management in cognitive radio networks, RFID in intelligent transporting system, and smart phone application.

FAN ZHANG received the B.E. and M.S. degrees in communication and information system from Beijing Jiaotong University, Beijing, China, in 2011 and 2014, respectively. He is currently pursuing the Ph.D. degree with the Shu Hua Wireless Network and Information Perception Center, Beijing Jiaotong University. His research interests are cognitive radio networks, energy harvesting, and mobile social networks.

YAN HUO (M'12) received the B.E. and Ph.D. degrees in communication and information system from Beijing Jiaotong University, Beijing, China, in 2004 and 2009, respectively. He has been a Faculty Member with the School of Electronics and Information Engineering, Beijing Jiaotong University, since 2011, where he is currently an Associate Professor. He is a Visiting Scholar with the Department of Computer Science, George Washington University, from 2015 to 2016. His major research interests include wireless communication theory, cognitive radio, and signal processing.



ZHEN LI received the B.S. degree from Beijing Jiaotong University in 2012. He is currently pursuing the Ph.D. degree with Shu Hua Wireless Network and Information Perception Center, Beijing Jiaotong University. His research interests are cognitive radio networks, physical layer security, and mobile social networks.