EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Individual secrecy of fading homogeneous multiple access wiretap channel with successive interference cancellation

Kaiwei Jiang[1,2*], Tao Jing[1], Zhen Li[1], Yan Huo[1] and Fan Zhang[1]

Abstract

We investigate individual secrecy performance in a *K*-user quasi-static Rayleigh fading homogeneous multiple access wiretap channel (MAC-WT), where a legitimate receiver employs successive interference cancellation (SIC) decoding. We first evaluate individual secrecy performance under an arbitrary SIC order by deriving closed-form expressions with respect to secrecy outage probability and effective secrecy throughput (EST) as main metrics. The resulting closed-form expressions disclose a significant impact on the secrecy performance from the order of SIC decoding. Therefore, we propose three SIC decoding order scheduling schemes: (1) round-robin scheme, absolutely fair and served as a benchmark; (2) suboptimal scheme, based on each user's main channel condition; and (3) optimal scheme, based on each user's achievable secrecy rate. Comparison results show that the last two schemes outperform the first one with regard to both the EST and the multi-user diversity gain, whereas the performance of the suboptimal scheme is highly close to that of the optimal scheme which is usually impractical due to a requirement for the eavesdropper's channel state information (CSI).

Keywords: Multiple access wiretap channel, Successive interference cancellation, Secrecy performance, Scheduling scheme

1 Introduction

Since Wyner introduced the notion of the *wiretap channel* in his seminal work [1], the studies of keyless physical-layer secrecy transmission have made tremendous progress. He initially characterized a rate-equivocation region for a degraded wiretap channel, which was extended to a more general non-degraded version in [2]. The Gaussian wiretap channel was investigated in [3], which confirmed that the secrecy capacity is the difference between the capacities of main and eavesdropper channels. Thus, a more favorable main channel means the existence of a positive secrecy capacity. However, during wireless transmission, fading channels rather than stationary channels with Gaussian noise are a natural situation, where a more favorable main channel is not always guaranteed. Consequently, researchers characterized another two secrecy metrics, *secrecy outage probability* and *ergodic secrecy capacity* [4, 5]. Besides, one interesting measure, *effective secrecy throughput* (EST), was introduced in [6] by Nan Yang et al. evaluating an average secrecy rate at which messages are transmitted to a legitimate receiver confidentially.

A great deal of research work addressed how to improve secrecy performance, some from the perspective of precoding and beamforming [7–10], some via the utilization of artificial noise or jamming [11–14], and some jointly applying these approaches [15–18]. Overall, the purpose of exploiting these techniques is to enlarge the capacity difference between main and eavesdropper channels. One can further refer to a recent survey of physical-layer security which has been investigated from information theory to security engineering in [19].

Inspired by a capacity improvement on an individual user in a multi-user system with a successive interference cancellation (SIC) receiver [20], in this work, we consider a secrecy scenario as depicted in Fig. 1, where *K* transmitters send confidential messages to a legitimate receiver

*Correspondence: kwjiang@bjtu.edu.cn
[1] School of Electronics and Information Engineering, Beijing Jiaotong University, 100044 Beijing, China
[2] School of Electric and Information Engineering, Taizhou Vocational and Technical College, 318000 Taizhou, China

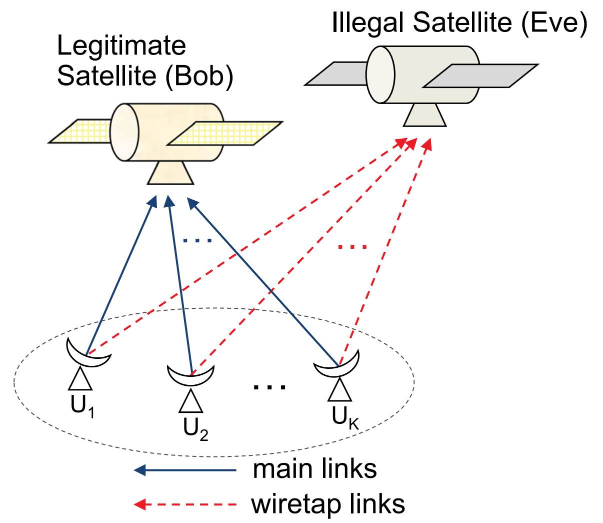

Fig. 1 Model of quasi-static Rayleigh fading homogeneous multiple access wiretap channel with *K* earth stations, one legitimate satellite, and one illegal satellite, each with a single antenna

who employs SIC decoding with the existence of an eavesdropper. We investigate the impacts of the SIC order and multi-user diversity on individual secrecy performance and propose three SIC order scheduling schemes.

The system model in this work is a typical multiple access wiretap channel (MAC-WT)[1], which has been intensively studied recently. However, all of these references [21–34] considered problems from an information-theoretical perspective and characterized the setting as a whole. Ender Tekin et al. characterized secrecy rate regions and an upper bound for the secrecy sum-rate for a Gaussian MAC-WT via the Gaussian encoding in [21]. They also addressed a fading MAC-WT in [22], providing achievable ergodic secrecy rate regions as well as its outer bounds and giving optimal power allocations to maximize the sum-rate. Hassan Zivari-Fard et al. [23] investigated a 2-user MAC-WT with a common message which can be decoded by both the legitimate receiver and the eavesdropper, and derived general inner and outer bounds on a secrecy capacity region for both discrete memoryless and Gaussian cases. The authors further addressed this type of MAC-WT (with a common message) in [24], where only one transmitter's private messages should be kept secret from the adversary. They derived general inner and outer bounds for both imperfect and perfect secrecy conditions for the adversary under discrete memoryless, less noisy, and Gaussian versions of the MAC-WT. Yet, the secure degrees of freedom (DoF) of such Gaussian signaling-based schemes are zero, which means the schemes are suboptimal and leads to further work for new encoding techniques. One commonly used encoding technique is the real interference alignment [25–27]. Other techniques, e.g., uniform distributed source coding and polar coding, are also developed and applied for the MAC-WT [28–30]. Moreover, two alignment techniques, *scaling-based alignment* (SBA), and *ergodic secret alignment* (ESA), were proposed in [31] to achieve an ergodic secrecy rate region for a 2-user fading MAC-WT. The SBA performs repetition coding at two consecutive time instances while the ESA performs repetition coding at two carefully chosen time instances. Another research direction of interest on the MAC-WT is secure DoF, which was also fully studied in recent years [25, 32–34]. Xie and Ulukus [25] derived the sum secure DoF of a *K*-user Gaussian MAC-WT. The entire secure DoF region of the *K*-user Gaussian MAC-WT was determined in [32]. Mukherjee and Ulukus [33] considered the secure DoF of the case with no eavesdropper's channel state information (CSI). The results showed the sum secure DoF is less than that of the case with a subset or all of the transmitters knowing the eavesdropper's CSI. The secure DoF of a MIMO MAC-WT was studied in [34], showing that the optimal sum secure DoF is affected by the number of eavesdropper antennas.

The problems in this work are also different from the existing literature regarding multi-user uplink wiretap channels [35–37]. Jin et al. [35] and Zou et al. [36] ignored cochannel interference deliberately in the system models. Although cochannel interference was considered in [37], where uplink secure communications in a cellular network are studied, such cochannel interference is not from the users in a cell but from neighboring base stations.

Secrecy problems related to SIC were studied in [38], where the authors only considered the case of two transmitter-receiver pairs and tried to find the coordinated beamforming vectors at the transmitters to reach an ergodic secrecy rate balancing point. In [39], we investigated individual secrecy performance for a *K*-user MAC-WT, where the legitimate receiver possesses multiple antennas and employs two specific decoding methods, zero-forcing (ZF), and minimum mean-square error (MMSE), jointly with SIC. For simplicity, we ignored the cochannel interference to the eavesdropper during modeling. We later complicated the eavesdropper setting from a single-antenna to multi-antenna scenario in [40], where, besides the derivations of individual secrecy performance, we further proposed one SIC order scheduling scheme based on each user's relative distance to the eavesdropper over the legitimate receiver, and gave a solution to the problem of uplink optimal power allocation.

In this paper, we continue to study individual secrecy performance for the *K*-user MAC-WT with SIC. We take into account the cochannel inference to the eavesdropper for evaluating the secrecy performance. Moreover, we propose three new SIC decoding order scheduling schemes. Both the main and eavesdropper channels are assumed to experience quasi-static Rayleigh fading, just as in [39, 40]. We further assume the users are homogeneous, i.e., all the users experience the same received power on average at each of the receivers (the legitimate receiver and the eavesdropper). We call such a network as the homogeneous MAC-WT, which is assumed throughout this paper. Similar to [39, 40], secrecy outage probability and effective secrecy throughput are utilized as our key measures in evaluating the secrecy performance.

It is worthwhile to mention that an assumption of homogeneous (also call "symmetric" in some literature) networks is widely used to address wireless communication issues. In [41], homogeneous users were assumed in the system model to address a secrecy issue of multi-user downlinks. Reid et al. [42], Nitinawarat [43], Chou et al. [44] studied related wireless communication problems based on symmetric multiple access channels. A 2-user symmetric MAC-WT was investigated in [45], while reference [46] modeled a *K*-user symmetric MIMO MAC-WT for analyzing secure DoF.

To demonstrate how the SIC order impacts the individual secrecy performance, we derive the closed-form expressions of the secrecy outage probability and the effective secrecy throughput with a specified SIC order. Observing these closed-from expressions, we can assess the impact of the SIC order.

To compare these three SIC order scheduling schemes, we first make succinct comparisons of the EST of the *best* case (i.e., no cochannel interference) for each scheme, since the performance of the best case predominates the other cases, which will be seen clearly later in this paper. Then, with the aid of simulations, we make full performance comparisons of these schemes regarding the maximum sum-EST and the multi-user diversity gain.

The main contributions of the paper are summarized as follows:

1) Model the fading homogeneous MAC-WT and derive closed-form expressions of the cumulative distribution function (CDF) of signal-to-interference-plus-noise ratios (SINRs) for any individual transmitter at the legitimate receiver and the eavesdropper, respectively.
2) Evaluate the impacts of the SIC order and multi-user diversity on the secrecy performance in terms of secrecy outage probability, effective secrecy throughput, and other secrecy performance metrics by deriving the corresponding closed-form expressions.
3) Propose and evaluate three SIC decoding order scheduling schemes, namely, round-robin scheme, suboptimal scheme, and optimal scheme.

The rest of the paper is organized as follows: in Section 2, we model the quasi-static Rayleigh fading homogeneous MAC-WT. Section 3 investigates the individual secrecy performance. Three SIC order scheduling schemes are proposed in Section 4. Numerical results and further discussions are presented in Section 5. Finally, Section 6 concludes the work.

Notation: $\mathcal{A}\backslash\mathcal{B}$ denotes set $\mathcal{A}$ minus set $\mathcal{B}$. $\mathcal{CN}$, Exp, and χ_m^2 specify the circular symmetric complex Gaussian distribution, the exponential distribution and the chi-squared distribution with m degrees of freedom, respectively. log denotes the base 2 logarithm. $[\cdot]^+ = \max(0, \cdot)$. $\mathbf{E}(\cdot)$ specifies the expectation operator.

2 Fading homogeneous MAC-WT modeling

As illustrated in Fig. 1, K earth stations $(U_1, \ldots, U_K)$ are intended to transmit their confidential messages to a legitimate satellite (Bob) through main multiple access links, while an illegal satellite (Eve) attempts to intercept data from a specific user U_k, $k \in \mathcal{K} \triangleq \{1, \ldots, K\}$, through a corresponding wiretap link with the existence of cochannel interference. Assuming that all of the nodes (K users, i.e., earth stations, Bob, and Eve) are equipped with a single antenna, the main channel coefficient between U_k and Bob is denoted as h_k, while g_k denotes the eavesdropper channel coefficient between U_k and Eve. We suppose Bob has instantaneous knowledge of the realization of h_k, but only has the statistic of g_k. The signal transmitted from U_k is denoted as x_k, which has an identical average power constraint of P for all $k \in \mathcal{K}$.

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

$$y_b = \sum_{i=1}^{K} h_i x_i + w_b, \tag{1}$$

$$y_e = \sum_{i=1}^{K} g_i x_i + w_e, \tag{2}$$

where w_b and w_e are circular symmetric complex Gaussian random variables with the variances of N_b and N_e, respectively, i.e., $w_b \sim \mathcal{CN}(0, N_b)$ and $w_e \sim \mathcal{CN}(0, N_e)$.

We assume both the main and wiretap links experience quasi-static Rayleigh fading.[2] As such, $|h_k|^2$ and $|g_k|^2$ are exponentially distributed, the means of which are denoted as δ_k^2 and σ_k^2, respectively.

We further assume all the K users are situated in a small region (e.g., a diameter of several kilometers) relative to the distances between the users and both satellites (maybe several hundred or thousand kilometers). Such a scenario may exist in a military base or a television station where multiple earth stations need to transmit their signals to a relay satellite. The assumption implies all the users are approximately equidistant from each of the satellites. Thus, all these users can be considered to be homogeneous, i.e., the average power received at Bob/Eve from each user is the same, as long as they have identical average transmit power.

Interestingly, in this case, the K single-antenna users can also correspond to one K-antenna transmitter, where each antenna transmits one independent data stream. Therefore, the system can also be regarded as a multiple-input-single-output (MISO) wiretap channel, where the eavesdropper attempts to intercept messages from one specific data stream. Different from issues of the MISO wiretap channel in [6, 47–49], we focus on the impact of the SIC order on the individual secrecy performance (i.e., secrecy performance of each data stream in this equivalent MISO wiretap channel model).

2.1 Achievable individual secrecy rate with SIC

In traditional multi-user decoding, a receiver decodes each user's data by treating all other users' data as noise. Such a method is not capacity-achieving. In this network model, Bob employs SIC decoding by subtracting already-decoded data from the composite signal, reducing the amount of cochannel interference for the next user's decoding. Therefore, the main capacity of an individual user is determined not only by its signal-to-noise ratio (SNR) but also by its own order in SIC decoding. When a user is decoded at first, it is just the same as the traditional way of decoding for that user, achieving the *worst* case. In contrast, it achieves the *best* case, i.e., no cochannel interference, if it is decoded at last. In general, we can express the main capacity of an individual user (i.e., U_k) with SIC as

$$C_{b,k}^{(\Im)} = \log\left(1 + \frac{\xi_k}{1 + \sum_{j\in\Im} \xi_j}\right) = \log\left(1 + \gamma_k^{(\Im)}\right), \quad (3)$$

where $\xi_k = \frac{|h_k|^2 P}{N_b}$ ($\forall k \in \mathcal{K}$) is the instantaneous SNR of U_k at Bob with the mean of $\overline{\xi_k} = \frac{\delta_k^2 P}{N_b} = 1/\lambda_k$; $\Im \subseteq \mathcal{K}\backslash\{k\}$, implying U_k is decoded just before the users in the set $\Im$ (index) during SIC decoding; and $\gamma_k^{(\Im)}$ denotes the SINR of U_k at Bob, the superscript of which indicates where the cochannel interference comes from.

It is reasonable to assume that Eve cannot do any SIC decoding before it is able to intercept a message successfully from any user. Consequently, the wiretap capacity for U_k can be expressed as

$$C_{e,k} = \log\left(1 + \frac{\eta_k}{1 + \sum_{j\neq k} \eta_j}\right) = \log\left(1 + \rho_k\right), \quad (4)$$

where $\eta_k = \frac{|g_k|^2 P}{N_e}$ ($\forall k \in \mathcal{K}$) is the instantaneous SNR of U_k at Eve with the mean of $\overline{\eta_k} = \frac{\sigma_k^2 P}{N_e} = 1/\mu_k$, and ρ_k denotes the SINR of U_k at Eve.

Thereby, in this MAC-WT channel, the instantaneous achievable individual secrecy rate with SIC can be formulated as [21, 50]

$$C_{s,k}^{(\Im)} = \left[C_{b,k}^{(\Im)} - C_{e,k}\right]^{+}. \quad (5)$$

2.2 Statistics of SINRs

Since the derivation of the secrecy outage probability requires the statistics of $\gamma_k^{(\Im)}$ and ρ_k, we decide to derive them in advance in this subsection.

Before deriving the statistic of $\gamma_k^{(\Im)}$, we first investigate the random variables $\xi_1, \xi_2, \ldots, \xi_K$. As $\xi_k \propto |h_k|^2$ ($\forall k \in \mathcal{K}$), the random variables $(\xi_1, \xi_2, \ldots, \xi_K)$ are mutually independent and exponentially distributed, i.e., $\xi_k \sim \mathrm{Exp}(\lambda_k)$ ($\forall k \in \mathcal{K}$). The CDF of $\gamma_k^{(\Im)}$ can be obtained,

$$F_{\gamma_k^{(\Im)}}(\gamma_k) = \begin{cases} 1 - \frac{\prod_{i\in\Im} \lambda_i}{\prod_{i\in\Im}(\lambda_i + \lambda_k \gamma_k)} e^{-\lambda_k \gamma_k}, & \gamma_k \geq 0 \\ 0, & \gamma_k < 0. \end{cases} \quad (6)$$

Similarly, the random variables $\eta_1, \eta_2, \ldots, \eta_K$ are exponentially and independently distributed, i.e., $\eta_k \sim \mathrm{Exp}(\mu_k)$ ($\forall k \in \mathcal{K}$). The CDF of ρ_k can be formulated in the same fashion,

$$F_{\rho_k}(\rho_k) = \begin{cases} 1 - \frac{\prod_{i\neq k} \mu_i}{\prod_{i\neq k}(\mu_i + \mu_k \rho_k)} e^{-\mu_k \rho_k}, & \rho_k \geq 0 \\ 0, & \rho_k < 0. \end{cases} \quad (7)$$

The detailed derivations of (6) and (7) can be found in Appendix A.

Due to the homogeneousness, $\lambda_1 = \lambda_2 = \ldots = \lambda_K$ and $\mu_1 = \mu_2 = \ldots = \mu_K$. Thus, (6) and (7) can be further simplified to

$$F_{\gamma^{(n)}}(\gamma) = 1 - \frac{e^{-\lambda\gamma}}{(1+\gamma)^n}, \quad \gamma \geq 0 \quad (8)$$

$$F_{\rho}(\rho) = 1 - \frac{e^{-\mu\rho}}{(1+\rho)^{K-1}}, \quad \rho \geq 0. \quad (9)$$

Here, the subscript k is omitted, as each user has the same attributes, and the superscript $\Im$ is changed into its cardinality n, i.e., the number of cochannel interferers.

Their probability density functions (PDFs) can be yielded by differentiating the related CDFs in (8) and (9), respectively.

$$f_{\gamma^{(n)}}(\gamma) = \frac{(1+\gamma)\lambda + n}{(1+\gamma)^{n+1}} e^{-\lambda\gamma}, \quad \gamma > 0 \quad (10)$$

$$f_{\rho}(\rho) = \frac{(1+\rho)\mu + K - 1}{(1+\rho)^{K}} e^{-\mu\rho}, \quad \rho > 0. \quad (11)$$

Notably, the subscript k of notations will be automatically omitted in the rest of the paper if necessary.

3 Individual secrecy performance with SIC

This section investigates the individual secrecy performance, termed secrecy performance for short hereinafter, under an arbitrary SIC order in terms of *secrecy outage probability*, *effective secrecy throughput*, and some other secrecy performance metrics. The closed-form expressions are derived and related performance analysis is explored.

3.1 Secrecy outage probability

The secrecy outage probability is the probability of the achievable secrecy rate that is less than a predefined secrecy rate R_s,

$$P_{\mathrm{so}}^{(n)}\left(R_s\right) = \Pr\left(C_s^{(n)} < R_s\right). \tag{12}$$

Here, $C_s^{(n)}$ denotes the instantaneous achievable individual secrecy rate with n cochannel interferers, and its prototype definition can be found in (5).

Due to the independence between the main and wiretap links, the random variables $\gamma^{(n)}$ and ρ are also independent. Along with (8), (9), (10) and (11), the secrecy outage probability can be derived as follows:

$$\begin{aligned}
P_{\mathrm{so}}^{(n)}\left(R_s\right) &= \Pr\left(\frac{1+\gamma^{(n)}}{1+\rho} < 2^{R_s}\right)\\
&= \int_0^{\infty}\int_0^{2^{R_s}\rho+2^{R_s}-1} f_{\rho}\left(\rho\right) f_{\gamma^{(n)}}\left(\gamma\right) d\gamma\, d\rho\\
&= \int_0^{\infty} f_{\rho}\left(\rho\right) F_{\gamma^{(n)}}\left(2^{R_s}\rho + 2^{R_s}-1\right) d\rho\\
&= \int_0^{\infty} f_{\rho}\left(\rho\right) d\rho - \int_0^{\infty} f_{\rho}\left(\rho\right) \frac{e^{-\lambda\left(2^{R_s}\rho+2^{R_s}-1\right)}}{\left(2^{R_s}+2^{R_s}\rho\right)^n} d\rho\\
&= 1 - \int_0^{\infty} \frac{\left(1+\rho\right)\mu + K - 1}{\left(1+\rho\right)^K} e^{-\mu\rho} \frac{e^{-\lambda\left(2^{R_s}\rho+2^{R_s}-1\right)}}{\left(2^{R_s}+2^{R_s}\rho\right)^n} d\rho\\
&= 1 - \underbrace{\frac{e^{-\lambda\left(2^{R_s}-1\right)}}{2^{nR_s}}}_{I_1} \underbrace{\left\{\Theta_1(n)+\Theta_2(n)\right\}}_{I_2},
\end{aligned} \tag{13}$$

where

$$\Theta_1(n) = \mu \mathbf{U}\left(K+n-1, \mu + 2^{R_s}\lambda\right), \tag{14}$$

$$\Theta_2(n) = (K-1)\, \mathbf{U}\left(K+n, \mu + 2^{R_s}\lambda\right). \tag{15}$$

The function $\mathbf{U}(k,\theta)$ has the following definition,

$$\mathbf{U}(k,\theta) = \int_0^{\infty} \frac{e^{-\theta x}}{(1+x)^k} dx. \tag{16}$$

The integral result of this function can be looked up from ([51], Eq. (3.353.2)),

$$\mathbf{U}(k,\theta) = \frac{\sum_{j=1}^{k-1}(j-1)\,!(-\theta)^{k-j-1} - (-\theta)^{k-1}e^{\theta}\mathrm{Ei}(-\theta)}{(k-1)\,!}. \tag{17}$$

Here, Ei (x) is the exponential integral function with the definition

$$\mathrm{Ei}\left(x\right) = \int_{-\infty}^{x} \frac{e^t}{t} dt. \tag{18}$$

By observing (16), it is easy to find that $\mathbf{U}(k,\theta)$ is a decreasing function of θ and/or k. Particularly, $\mathbf{U}(k,\theta) \to 0$ as k or $\theta \to \infty$. Since the term I_2 in (13) is a non-negative linear combination of the decreasing function $\mathbf{U}(k,\theta)$, it decreases with n or R_s increasing by fixing the other arguments. So does the term I_1. Moreover, the item I_1 has an exponential decay with either n or R_s increasing.

Thereby, we can attain that $P_{\mathrm{so}}^{(n)}\left(R_s\right)$ is an increasing function of n and/or R_s.

In the path-loss model, we realize $\lambda \propto d_b^{\alpha}$ and $\mu \propto d_e^{\alpha}$ (here, suppose $N_b = N_e$), where d_b denotes the straight-line distance between an individual user and Bob, d_e is each user's distance to Eve, and α is the path-loss exponent. μ can then be transformed into the form of $(d_e/d_b)^{\alpha}\lambda$. Substituting it into the corresponding expressions in (14) and (15), we can obtain the result in (13) from the perspective of locations. On the other hand, such a form of expression makes it possible for Bob to reversely derive the insecure range of any individual user for a certain secrecy quality-of-service (QoS) (secrecy outage probability under a predefined secrecy rate). Concretely, for a specified SIC order as well as a certain secrecy QoS, the distance d_e is available via numerical root-finding, and it is exactly the radius of an insecure range centered on that user.

Accordingly, the *secrecy transmission probability* can be deduced,

$$\begin{aligned}
P_{\mathrm{st}}^{(n)}\left(R_s\right) &= 1 - P_{\mathrm{so}}^{(n)}\left(R_s\right)\\
&= \frac{e^{-\lambda\left(2^{R_s}-1\right)}}{2^{nR_s}} \left\{\Theta_1(n)+\Theta_2(n)\right\},
\end{aligned} \tag{19}$$

which is, obviously, a decreasing function of n and/or R_s.

3.2 Effective secrecy throughput

In accordance with [6], the EST is the product of a secrecy rate R_s and the corresponding secrecy transmission probability $P_{\mathrm{st}}^{(n)}\left(R_s\right)$,

$$\begin{aligned}
T^{(n)}\left(R_s\right) &= P_{\mathrm{st}}^{(n)}\left(R_s\right) R_s\\
&= \frac{e^{-\lambda\left(2^{R_s}-1\right)}}{2^{nR_s}} \left\{\Theta_1(n)+\Theta_2(n)\right\} R_s.
\end{aligned} \tag{20}$$

Since $P_{\mathrm{st}}^{(n)}\left(R_s\right)$ is a decreasing function of n, $T^{(n)}\left(R_s\right)$ declines with an increase in n. Moreover, $P_{\mathrm{st}}^{(n)}\left(R_s\right)$ decreases exponentially with R_s increasing. Thus, multiplying it with R_s makes the product increase at first and then decrease quickly, which denotes the existence of the maximum EST over R_s.

The maximum EST is expressed as

$$T_{\max}^{(n)}\left(R_s^{*(n)}\right) = P_{\rm st}^{(n)}\left(R_s^{*(n)}\right) R_s^{*(n)}. \tag{21}$$

Apparently, the *optimal secrecy rate* $R_s^{*(n)}$ to achieve the maximum EST is not identical for different numbers of cochannel interferers n. Interestingly, $R_s^{*(n)}$ with a small value of n is higher than that with a big one, because $P_{\rm st}^{(n)}(R_s)$ under a small value of n decays more slowly over R_s. We can view such a phenomenon more clearly in Fig. 2.

For the path-loss model, it is possible for each of the users to calculate its optimal secrecy rate with the locations of Bob and Eve. Yet, it is usually difficult for each user to obtain Eve's location. In practice, the estimation of the optimal secrecy rate for each user can be done by Bob instead, and each user tunes to its optimal secrecy rate to gain the maximum EST with an instruction from Bob.

More numerical details for the EST and the estimations of optimal secrecy rates will be examined later in Section 5.

3.3 Other secrecy performance metrics

One of the most important metrics is the *positive secrecy rate probability* (denoted as $P_{\rm ps}^{(n)}$) which is equivalent to the probability of $\gamma^{(n)} > \rho$. It can be easily obtained, $P_{\rm ps}^{(n)} = P_{\rm st}^{(n)}(0)$.

Another interesting performance measure is the ϵ-outage secrecy rate which is defined as the highest secrecy rate when the secrecy outage probability is not greater than ϵ. It can be formulated by

$$P_{\rm so}^{(n)}\left(C_s^{(n)}(\epsilon)\right) = \epsilon. \tag{22}$$

Although we cannot achieve the closed-form expression of the ϵ-outage secrecy rate due to the complexity of (13), it is possible to obtain the result by numerical root-finding.

3.4 Asymptotic behaviors

We proceed with the asymptotic behaviors of the secrecy performance for an extreme value of K or μ while limiting the other parameters.

Observing (17), an interesting equation can be obtained,

$$\lambda \mathbf{U}(k-1,\lambda) + (k-1)\,\mathbf{U}(k,\lambda) = 1. \tag{23}$$

By applying (23), we rewrite (13) as

$$P_{\rm so}^{(n)}(R_s) = 1 - \frac{e^{-\lambda\left(2^{R_s}-1\right)}}{2^{nR_s}}(1-\Phi), \tag{24}$$

where,

$$\Phi = 2^{R_s}\lambda \mathbf{U}\left(K+n-1, \mu+2^{R_s}\lambda\right) + n\mathbf{U}\left(K+n, \mu+2^{R_s}\lambda\right). \tag{25}$$

Obviously, (24) is a decreasing function of K and/or μ.

Note that $\Phi \to 0$, as K or $\mu \to \infty$. Thus, we can obtain the following asymptotic expression of the secrecy outage probability,

$$\lim_{K or \mu\to\infty} P_{\rm so}^{(n)}(R_s) = 1 - \frac{e^{-\lambda\left(2^{R_s}-1\right)}}{2^{nR_s}}, \tag{26}$$

which is completely reduced to the *transmission outage probability*.

Accordingly, the asymptotic expression of the EST can be formulated as

$$\lim_{K or \mu\to\infty} T^{(n)}(R_s) = \frac{e^{-\lambda\left(2^{R_s}-1\right)}}{2^{nR_s}} R_s. \tag{27}$$

Further, we get the asymptotic expression of the maximum EST,

$$\lim_{K or \mu\to\infty} T_{\max}^{(n)}\left(R_s^{*(n)}\right) = \frac{e^{-\lambda\left(2^{R_s^{*(n)}}-1\right)}}{2^{nR_s^{*(n)}}} R_s^{*(n)}, \tag{28}$$

where $R_s^{*(n)}$ is the optimal secrecy rate to achieve the maximum value of this asymptotic EST, and it should not be greater than the related main capacity.

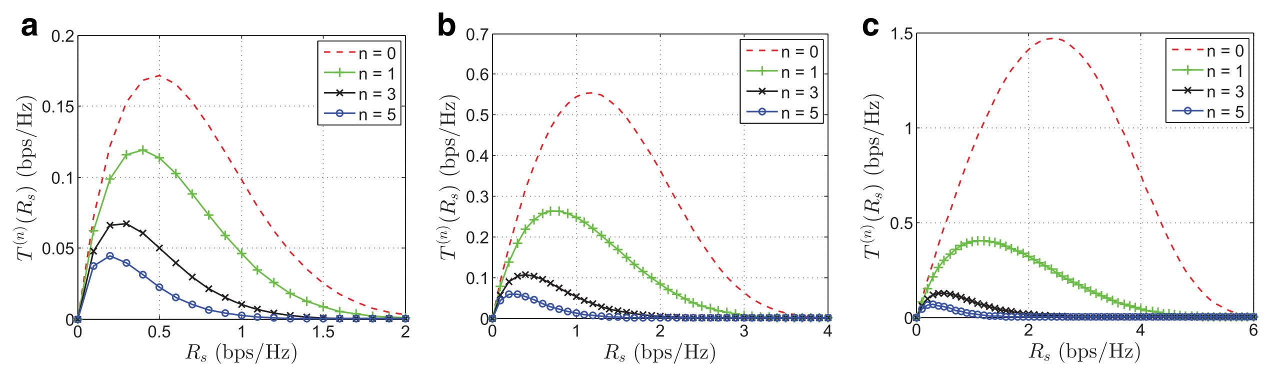

Fig. 2 Relationship between effective secrecy throughput $T^{(n)}(R_s)$ and R_s with different n on basis of $\beta = 1$. **a** SNR = − 3 dB. **b** SNR = 3 dB. **c** SNR = 10 dB

By observing (27), we note the EST declines dramatically with the weight of 2^{-nR_s}. For $n = 3$ and $R_s = 1$ bps/Hz, $\lim_{K or \mu \to \infty} T^{(3)}(1)$ is only about 1/8 of that for the best case ($n = 0$). In other words, the EST with $n = 0$ overwhelms the other cases.

Remark 1 *As the SIC order in this section is assumed to be random, the individual secrecy performance obtained above is an average result.*

Remark 2 *Although it is predictable that a decrease in n and/or an increase in K improve the individual secrecy performance in this SIC-based homogeneous MAC-WT network, the closed-form expressions clearly show how the SIC order and the multi-user diversity impact the secrecy performance. Moreover, it provides a foundation for understanding the SIC order scheduling schemes proposed in the upcoming section.*

4 SIC order scheduling schemes

As the order of SIC affects the secrecy performance significantly, we further explore SIC order scheduling policies from the perspective of Bob. Three SIC order scheduling schemes are studied in this section. First, we consider a conventional round-robin scheduling scheme, which is also used as a benchmark. Next, a suboptimal scheduling scheme is proposed, which schedules on the basis of users' main channel conditions. Finally, we study an optimal scheduling scheme, which is based on achievable individual secrecy rates. We refer to all these three schemes as *round-robin scheme*, *suboptimal scheme*, and *optimal scheme* for short, respectively. It is essential to clarify that the scheme name optimal scheme does not mean the best scheme of all (including not mentioned in this work) but only signifies superiority over the other two schemes.

4.1 Round-robin scheme

In this scheme, all the K users take the same chance for all possible SIC orders, which brings extreme fairness for each user. Specifically, there are exactly $K!$ corner points in the K-user capacity region with SIC decoding, each one corresponding to an SIC order among the users ([20], Chapter 6.1.4). Bob takes turns to access each of the $K!$ corner points for an equal period of time (i.e., $\frac{1}{K!}$ of scheduling duration), which makes every user experience each of the total $K!$ SIC orders for equal time. It seems impossible for Bob to take all the turns around within one time slot, especially with a large K. Such a problem can be solved by changing the scheduling duration from one time slot to an appropriate number of time slots, e.g., $K!$ time slots, one time slot for each corner point.

As is known to all, a secrecy outage event occurs, when an achievable secrecy rate falls below a predefined secrecy rate R_s. Nevertheless, the secrecy outage probability on each corner point is not necessarily the same. In fact, the secrecy outage probabilities on most of the corner points are different. Thus, an average secrecy outage probability is usually used as a performance metric in this case.

A straightforward way to get the average secrecy outage probability of an individual user for a predefined secrecy rate R_s is to calculate the secrecy outage probability on each corner point separately, add up all the results, and average over the total number of corner points $K!$. As the system in this work is homogeneous, there exactly exist $(K-1)!$ corner points for an individual user with n cochannel interferers (i.e., the total number of SIC orders in which the specified user is decoded at $(n+1)^{th}$ from the end). Therefore, the average secrecy outage probability of an individual user can be formulated as

$$\begin{aligned} P_{\mathrm{so}}^{\mathrm{av}}(R_s) &= \frac{1}{K!}\sum_{n=0}^{K-1}(K-1)!\,P_{\mathrm{so}}^{(n)}(R_s) \\ &= 1-\frac{1}{K}\sum_{n=0}^{K-1}\frac{e^{-\lambda(2^{R_s}-1)}}{2^{nR_s}}\{\Theta_1(n)+\Theta_2(n)\}. \end{aligned} \quad (29)$$

Subsequently, the average individual EST can be easily obtained, the maximum expression of which is denoted as

$$T_{\max}^{\mathrm{av}}(R_s) = \max_{R_s}\left(\left(1 - P_{\mathrm{so}}^{\mathrm{av}}(R_s)\right)R_s\right). \quad (30)$$

However, the maximum value acquired by (30) is suboptimal, as the optimal secrecy rate R_s^* for the above maximum value is fixed for all possible n. The optimal maximum value can be obtained by taking n into account for each optimal secrecy rate, just as in Subsection 3.2,

$$T_{\max}^{\mathrm{av(opt)}}\left(R_s^{*(0)},\ldots,R_s^{*(K-1)}\right) = \frac{1}{K}\sum_{n=0}^{K-1}T_{\max}^{(n)}\left(R_s^{*(n)}\right), \quad (31)$$

where $R_s^{*(n)}$ and $T_{\max}^{(n)}\left(R_s^{*(n)}\right)$ is given in (21).

Accordingly, the maximum sum-EST in this scheme can be achieved by multiplying the maximum average EST with K,

$$\begin{aligned} T_{\max}^{\mathrm{sum}}\left(R_s^{*(0)},\ldots,R_s^{*(K-1)}\right) &= KT_{\max}^{\mathrm{av(opt)}}\left(R_s^{*(0)},\ldots,R_s^{*(K-1)}\right) \\ &= \sum_{n=0}^{K-1}T_{\max}^{(n)}\left(R_s^{*(n)}\right), \end{aligned} \quad (32)$$

which is equivalent to the sum of the maximum EST of an individual user over all possible n.

Although the round-robin scheme is a good way for fairness, it is not an optimal option for achieving the maximum sum-EST from Bob's point of view. We next introduce the other two schemes, i.e., the suboptimal scheme and the optimal scheme, which achieve more maximum sum-EST. The former needs no CSI of Eve for Bob, while the latter requires Eve's CSI. Although the optimal scheme is usually impractical, we still study it for the purpose of comparisons.

4.2 Suboptimal scheme

The suboptimal scheme is based on instantaneous main channel gains in a certain time slot. To be concrete, the SIC order is sorted by Bob according to each user's instantaneous channel gain from the lowest to the highest. That is, the user with the lowest instantaneous channel gain is decoded at first (no interference cancellation), while the user with the highest gain is decoded at last (no cochannel interference).

The reason why Bob sorts the SIC order that way (from the lowest gain to the highest) is that the EST of an individual user with the best case (decoded at last, i.e., $n = 0$, we call such EST as best-case-EST later) overwhelms the other cases for the same SNR. Meanwhile, the EST increases with an increase in SNR. Therefore, Bob allocates the best case to the user with the best main channel condition (i.e., achieving the highest SNR for the same transmit power), expecting to achieve more maximum sum-EST.

Although it is difficult to derive the closed-form expressions of the EST for all possible cases (from the best to the worst case) in this scheme, the closed-form expression of one special case, i.e., the best case for the user with the best channel condition, can be derived,[3]

$$\begin{aligned} T^{\dagger(0)}(R_s) &= \left(1 - P_{\text{so}}^{\dagger(0)}(R_s)\right) R_s \\ &= -\sum_{i=1}^{K} \binom{K}{i} (-1)^i e^{-\lambda(2^{R_s}-1)i} \left\{ \Theta_1^{'}(i) + \Theta_2^{'}(i) \right\} R_s, \end{aligned} \tag{33}$$

where

$$\Theta_1^{'}(i) = \mu \mathbf{U}\left(K-1, \mu + i2^{R_s}\lambda\right), \tag{34}$$

$$\Theta_2^{'}(i) = (K-1)\, \mathbf{U}\left(K, \mu + i2^{R_s}\lambda\right). \tag{35}$$

The process of the derivation can be found in Appendix B.

Note that $\Theta_1^{'}(1) = \Theta_1(0)$ and $\Theta_2^{'}(1) = \Theta_2(0)$. We transform (33) into

$$\begin{aligned} T^{\dagger(0)}(R_s) &= \mathrm{K}e^{-\lambda(2^{R_s}-1)} \{\Theta_1(0) + \Theta_2(0)\} R_s - \Delta \\ &= \mathrm{KT}^{(0)}(R_s) - \Delta, \end{aligned} \tag{36}$$

where

$$\Delta = \sum_{i=2}^{K} \binom{K}{i} (-1)^i e^{-\lambda(2^{R_s}-1)i} \left\{ \Theta_1^{'}(i) + \Theta_2^{'}(i) \right\} R_s. \tag{37}$$

We can acquire that the first term in (36) has a K-fold gain over $T^{(0)}(R_s)$, which means the multi-user diversity gain is achieved significantly in this scheme.

Since the maximum best-case-EST predominates the maximum sum-EST for both the round-robin and suboptimal schemes, it is illustrative to contrast the performance of these two schemes with respect to the maximum best-case-EST instead of the maximum sum-EST. According to (36), $T_{\max}^{\dagger(0)}\left(R_s^{*(0)}\right)$ is significantly greater than $T_{\max}^{(0)}\left(R_s^{*(0)}\right)$. As such, we can infer that the performance of the suboptimal scheme outperforms that of the round-robin scheme significantly with regard to the maximum sum-EST. More numerical analysis will be continued in Section 5.

Let us further explore the asymptotic expression of $T^{\dagger(0)}(R_s)$, as $K \to \infty$.

By applying (23) to (34) and (35), we obtain,

$$\Theta_1^{'}(i) + \Theta_2^{'}(i) = 1 - i2^{R_s}\lambda \mathbf{U}\left(K-1, \mu + i2^{R_s}\lambda\right), \tag{38}$$

which approaches to 1, as $K \to \infty$.

Then, the asymptotic expression of (33) can be derived as,

$$\begin{aligned} \lim_{K\to\infty} T^{\dagger(0)}(R_s) &= \lim_{K\to\infty} -\sum_{i=1}^{K} \binom{K}{i} (-1)^i e^{-\lambda(2^{R_s}-1)i} R_s \\ &= \lim_{K\to\infty} \left\{ 1 - \left(1 - e^{-\lambda(2^{R_s}-1)}\right)^K \right\} R_s \\ &= R_s. \end{aligned} \tag{39}$$

Subject to the constraint of the main capacities, the maximum value of $\lim_{K\to\infty} T^{\dagger(0)}(R_s)$ is given by,

$$\lim_{K\to\infty} T_{\max}^{\dagger(0)}\left(R_s^{*}\right) = \log\left(1 + \max_{i\in\mathcal{K}} \xi_i\right). \tag{40}$$

4.3 Optimal scheme

The optimal scheme schedules the SIC order based on achievable individual secrecy rates, which implies a need for Eve's CSI. Concretely, Bob sorts the SIC order according to each user's instantaneous achievable secrecy rate ($n = 0$) from the lowest to the highest, i.e., the user with the highest achievable secrecy rate is decoded at last. For the same reason that the best-case-EST predominates the sum-EST for this scheme, we compare the performance of this scheme with the above two schemes in terms of best-case-EST for simplicity. Before achieving the closed-form expression of the best-case-EST of the user with the highest achievable secrecy rate, we first derive the corresponding secrecy outage probability, which is formulated as[4]

$$\begin{aligned} P_{\text{so}}^{\ddagger(0)}(R_s) &= Pr\left(\max_{i\in\mathcal{K}} C_{s,i}^{(0)} < R_s\right) \\ &= \prod_{i\in\mathcal{K}} \Pr\left(C_{s,i}^{(0)} < R_s\right) \\ &= \left[P_{\text{so}}^{(0)}(R_s)\right]^K, \end{aligned} \tag{41}$$

where $C_{s,i}^{(0)}$ denotes the i^{th} user's achievable secrecy rate with no cochannel interference.

Subsequently, the best-case-EST for this scheme can be expressed as

$$T^{\ddagger(0)}(R_s) = \left(1 - \left[P_{\text{so}}^{(0)}(R_s)\right]^K\right) R_s, \tag{42}$$

which is obviously bigger than $T^{(0)}(R_s)$ by observing (20). Next, we try to prove that $T^{\ddagger(0)}(R_s)$ is also not less than $T^{\dagger(0)}(R_s)$.

Proof We first rewrite the expression of $P_{\text{so}}^{\ddagger(0)}(R_s)$ as

$$\begin{aligned} P_{\text{so}}^{\ddagger(0)}(R_s) &= \left[P_{\text{so}}^{(0)}(R_s)\right]^K \\ &= \left[\int_0^\infty \left(1 - e^{-\lambda\left(2^{R_s}\rho + 2^{R_s} - 1\right)}\right) f_\rho(\rho) d\rho\right]^K \\ &= \left[\mathbf{E}\left(1 - e^{-\lambda\left(2^{R_s}\rho + 2^{R_s} - 1\right)}\right)\right]^K. \end{aligned} \tag{43}$$

Due to the Jensen's inequality and the convexity of $(\cdot)^K$, $\left[\mathbf{E}\left(1-e^{-\lambda\left(2^{R_s}\rho+2^{R_s}-1\right)}\right)\right]^K \le \mathbf{E}\left(\left(1-e^{-\lambda\left(2^{R_s}\rho+2^{R_s}-1\right)}\right)^K\right) \overset{(a)}{=} P_{\text{so}}^{\dagger(0)}(R_s)$, where (*a*) can be obtained from (53) in Appendix A. We then get $T^{\ddagger(0)}(R_s) \ge T^{\dagger(0)}(R_s)$, which completes the proof. □

Nevertheless, $T^{\dagger(0)}(R_s)$ is very close to $T^{\ddagger(0)}(R_s)$ even with moderate values of SNR and K. In other words, the suboptimal scheme is close to the optimal scheme with respect to the EST. It is worth explaining why the performance (in terms of EST) gap between the practical suboptimal scheme and the ideal optimal scheme is not so much significant.

As mentioned previously, the suboptimal scheme sorts the SIC order by users' channel gains (equivalently, main capacities) from the lowest to the highest, while the optimal scheme schedules via users' achievable secrecy rates. In light of (5), the user with the highest achievable secrecy rate also has an appreciably high probability of being with the highest main capacity. Similarly, the user with the lowest achievable secrecy rate has an appreciably high probability of owning the lowest main capacity. It is applicable for the other cases between the highest achievable secrecy rate and the lowest. Therefore, we can achieve very similar performance statistically just by using users' channel gains instead of achievable secrecy rates for scheduling. In other words, we can obtain the conclusion that the suboptimal scheme is highly close to the optimal scheme with respect to the EST. Such a conclusion will be confirmed once more in Section 5.

5 Numerical results and discussions

In this section, numerical results are presented to further examine and verify the analytical results mentioned above. On account of the consistency of the secrecy outage probability and the effective secrecy throughput as well as the limited space, we only demonstrate the numerical results in terms of effective secrecy throughput. Additionally, the performance comparison of these three SIC order scheduling schemes regarding the maximum sum-EST is examined as well. We make an additional discussion to end this section.

By setting the average received SNR of an individual user at Bob, i.e., $\overline{\xi}$, as the benchmark, the average received SNR at Eve is specified as $\overline{\eta} = \beta\overline{\xi}$, i.e., $\lambda/\mu = \beta$. Hereinafter, the "SNR" refers in particular to $\overline{\xi}$. We assume the default value of K is 10.

5.1 Secrecy performance

5.1.1 Effective secrecy throughput

Figure 2 depicts EST curves versus R_s for different values of n and SNR. Here, $\beta = 1$ is supposed. Note that the curve increases first and then decreases for each value of n and SNR, which confirms the inference in Subsection 3.2 that there exists a maximum value for each EST curve, namely, $T_{\max}^{(n)}\left(R_s^{*(n)}\right)$. Another verification is also done that the optimal secrecy rate $R_s^{*(n)}$ to achieve the maximum EST for different numbers of co-channel interferers is different. The lesser the n is, the higher the $R_s^{*(n)}$ becomes. Observing the comparisons from Fig. 2a to c, it is easy to find $T^{(n)}(R_s)$ for each specific n increases when the SNR increases. Interestingly, the gap between $T_{\max}^{(0)}\left(R_s^{*(0)}\right)$ and any other $T_{\max}^{(n)}\left(R_s^{*(n)}\right)$ (where n is not equal to 0) becomes bigger and bigger with an increase in SNR. Also, it confirms that $T_{\max}^{(0)}\left(R_s^{*(0)}\right)$ overwhelms the maximum EST for other cases. This is why we make the performance comparisons of the scheduling schemes by mainly evaluating $T^{(0)}(R_s)$, $T^{\dagger(0)}(R_s)$, and $T^{\ddagger(0)}(R_s)$.

5.1.2 Optimal secrecy rate estimation

We here demonstrate how Bob estimates the optimal secrecy rate for each user from a viewpoint of locations. Since each user's location is available to Bob, the distance between any individual user to Bob can be acquired by Bob itself. Likewise, each user's distance to Eve can also be calculated by Bob, as long as Bob has the information of Eve's location. Obviously, it is much more feasible for Bob to detect Eve's location than knowing its CSI.

To be more specific, we take a simple example. Suppose Bob is 200 km right above the users and Eve is 132 km away from Bob in the horizontal direction. Hence, $d_b = 200$ km, $d_e \approx 240$ km and $d_e/d_b \approx 1.2$. We further assume the path-loss exponent $\alpha = 2.5$, and the SNR perceived at Bob is 3 dB. Then, the maximum EST

Table 1 Maximum EST and corresponding optimal secrecy rate for each n

(bps/Hz)	$n = 0$	$n = 1$	$n = 2$	$n = 3$	$n = 4$
$T_{\max}^{(n)}$	0.5566	0.2655	0.1588	0.1078	0.0790
$R_s^{*(n)}$	1.16	0.76	0.52	0.38	0.30

and the corresponding optimal secrecy rate for each n can be estimated via numerical root-finding. The results are listed in Table 1. We can also obtain the results for other values of distance ratio. The complete relationships between distance ratios and EST curves are demonstrated in Fig. 3.

We note that the distance ratio does not affect the EST significantly. When Eve is extremely far away, with the limitation of the main capacities, the EST is still limited. Otherwise, when Eve is very close to the users, the EST is also not reduced too much. That is because the cochannel interference at Eve is increased as well when the SNR at Eve rises up.

5.2 Comparison of scheduling schemes

Figure 4 illustrates the best-case-EST curves for these three SIC order scheduling schemes, i.e., round-robin scheme, suboptimal scheme and optimal scheme, for three different cases of SNR, with an assumption of $\beta = 1$. The best-case-EST for the round-robin scheme ($T^{(0)}(R_s)$, green curves) is much lesser than that for the suboptimal (red curves) or optimal (blue curves) scheme. The gaps of the maximum best-case-EST between the round-robin scheme and the other two schemes enlarge when the SNR increases. In contrast, the best-case-EST for the suboptimal scheme ($T^{\dagger(0)}(R_s)$) is very close to that for the optimal scheme ($T^{\ddagger(0)}(R_s)$), which shows the more practical suboptimal scheme is a good option to replace the ideal but impractical optimal scheme.

In Fig. 5, it shows that $T^{\dagger(0)}(R_s)$ (blue line-marker curves) and $T^{\ddagger(0)}(R_s)$ (red line-marker curves) increases significantly with K increasing while $T^{(0)}(R_s)$ (black curves) does not increase much. Such a phenomenon shows that the multi-user diversity impacts the round-robin scheme very little, while the other two schemes achieve significant multi-user diversity gains. Similarly, the multi-user diversity gain for $T^{\dagger(0)}(R_s)$ is very close to that for $T^{\ddagger(0)}(R_s)$. Moreover, the gaps between $T^{\dagger(0)}(R_s)$ or $T^{\ddagger(0)}(R_s)$ and $T^{(0)}(R_s)$ expand drastically with K increasing.

In order to compare the performance of the scheduling schemes in terms of the maximum sum-EST numerically, we first calculate $T_{\max}^{(n)}(R_s^{*(n)})$ for all n with four different cases of SNR by numerical root-finding. The results are listed in Table 2. Here, $\beta = 1$. Observing the data, it confirms once more that the maximum sum-EST is dominated by the maximum best-case-EST. Similarly, the maximum values of best-case-EST for the other two schemes, $T_{\max}^{\dagger(0)}$ and $T_{\max}^{\ddagger(0)}$, are also calculated by numerical root-finding and listed in the right-hand columns of Table 3. From the table, we find $T_{\max}^{\dagger(0)}$ or $T_{\max}^{\ddagger(0)}$ is even larger than the maximum sum-EST for the round-robin scheme (listed in the second column of Table 3) except the case of SNR = − 3 dB for $T_{\max}^{\dagger(0)}$, where $T_{\max}^{\dagger(0)}$ is only a little less. Since the expressions of the maximum sum-EST for the suboptimal and optimal schemes are $\sum_{n=0}^{K-1} T_{\max}^{\dagger(n)}$ and $\sum_{n=0}^{K-1} T_{\max}^{\ddagger(n)}$, respectively, it obviously verify the maximum sum-EST for the suboptimal or optimal scheme is much larger than that for the round-robin scheme. In other words, the suboptimal or optimal scheme is much better than the round-robin scheme from the perspective of the maximum sum-EST in this model of MAC-WT.

To further evaluate the values of $T_{\max}^{\dagger(n)}$ and $T_{\max}^{\ddagger(n)}$ for the other cases (i.e., $n = 1, \ldots, K$), we perform simulations consisting of 2000 independent trials to obtain the average results of the EST curves for both schemes. Figure 6 demonstrates the simulation results (the cases for $n > 2$ are ignored, due to their low values for the curves) on basis of SNR = 3 dB. From Fig. 6, we observe the simulation curves for $T^{\dagger(0)}(R_s)$ (black dash-dot lines) and $T^{\ddagger(0)}(R_s)$ (red dashed lines) almost converge to those from the analytical results (blue circles for the suboptimal scheme and magenta diamonds for the optimal scheme), which shows

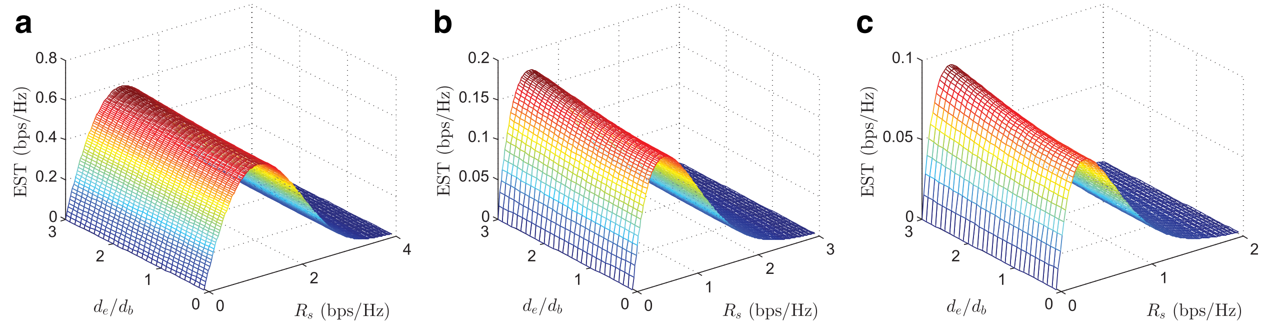

Fig. 3 Relationship between EST and distance ratio (d_e/d_b) on basis of SNR = 3 dB and $\alpha = 2.5$. **a** $n = 0$. **b** $n = 2$. **c** $n = 4$

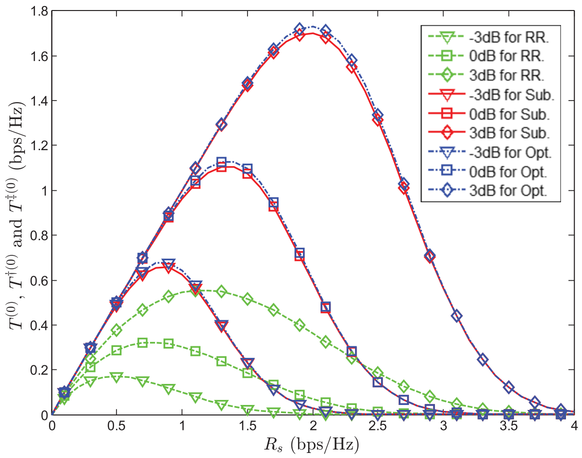

Fig. 4 Comparison of best-case-EST for round-robin scheme (RR.), suboptimal scheme (Sub.), and optimal scheme (Opt.) with different cases of SNR

the simulation results are reliable. Meanwhile, the simulation curves for both the suboptimal (black dash-dot lines) and optimal (red dashed lines) schemes are highly close to each other for $n > 0$, just like the case of $n = 0$. Although, for a big value of n, the maximum values of EST for these two schemes are poorer than the round-robin scheme, by observing the simulation results, $T_{\max}^{\dagger(1)}$ and $T_{\max}^{\ddagger(1)}$ are still superior to $T_{\max}^{(1)}$, and the maximum EST of either scheme for $n = 2$ is not too much less than that for the round-robin scheme.

To demonstrate the impacts of the multi-user diversity on $T^{\dagger(n)}$ and $T^{\ddagger(n)}$ for the other cases (i.e., $n = 1, \ldots, K$), we perform the simulation once more and achieve the results as plotted in Fig. 7 (partly, black curves for the suboptimal scheme and red curves for the optimal scheme), which shows the multi-user diversity gain for $T^{\dagger(n)}$ is also very close to that for $T^{\ddagger(n)}$ for $n = 1, \ldots, K$.

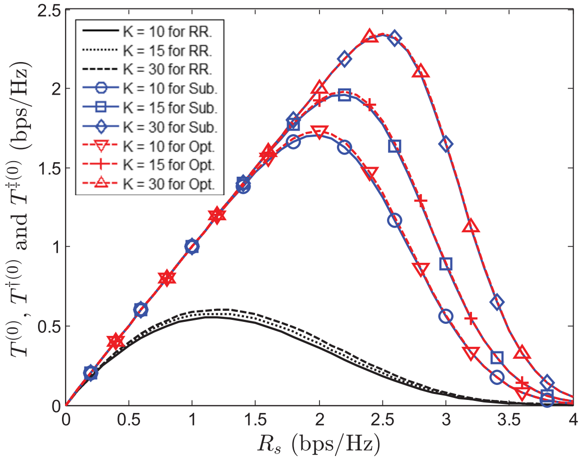

Fig. 5 Impacts of multi-user diversity on best-case-EST for round-robin scheme (RR.), suboptimal scheme (Sub.), and optimal scheme (Opt.)

Table 2 Maximum EST of round-robin scheme for different cases of n

SNR (dB)	$T_{\max}^{(0)}$	$T_{\max}^{(1)}$	$T_{\max}^{(2)}$	$T_{\max}^{(3)}$	$T_{\max}^{(4)}$
− 3	0.1716	0.1191	0.0881	0.0673	0.0540
0	0.3210	0.1873	0.1246	0.0893	0.0678
3	0.5540	0.2633	0.1575	0.1068	0.0781
10	1.4698	0.4033	0.2011	0.1260	0.0878
SNR (dB)	$T_{\max}^{(5)}$	$T_{\max}^{(6)}$	$T_{\max}^{(7)}$	$T_{\max}^{(8)}$	$T_{\max}^{(9)}$
− 3	0.0445	0.0368	0.0305	0.0259	0.0231
0	0.0533	0.0437	0.0360	0.0297	0.0248
3	0.0593	0.0477	0.0391	0.0322	0.0266
10	0.0663	0.0513	0.0419	0.0344	0.0283

5.3 Discussions

Although the performance of the suboptimal or optimal scheme precedes the round-robin scheme in achieving the maximum sum-EST for Bob, the values of EST for the users with bad channels are very low, which makes them be overheard easily. It seems unfair to these users. On the other hand, the absolutely fair round-robin is full of complexity in computing. Is there a scheduling scheme that can solve such a dilemma? It is easy to come up with a policy reversing the SIC order in the suboptimal scheme, i.e., sorting the SIC order from the highest channel gain to the lowest. We just call it *alternative scheme*. It is also difficult to derive the closed-form expressions of the EST for all cases of n for this scheme. Nevertheless, their simulation results can be obtained and demonstrated in Fig. 8, with the same simulation conditions as Fig. 6. We note, although the problem of fairness is improved, the performance is very bad such that not only the values of EST for the users with bad channel conditions are not improved too much but also the values of EST for the better-conditioned users are harmed significantly. The maximum EST for $n = 0$ is only about 0.06 bps/Hz, which indicates a good SIC order to a poor-conditioned user cannot improve its performance too much. On the other hand, the best channel condition in this scheme does not bring to the user high enough maximum EST (see curve with $n = 9$), which is less than that for $n = 4$, as its

Table 3 Comparison of $T_{\max}^{\text{sum}}$, $T_{\max}^{\dagger(0)}$, and $T_{\max}^{\ddagger(0)}$

SNR (dB)	$T_{\max}^{\text{sum}}$	$T_{\max}^{\dagger(0)}$	$T_{\max}^{\ddagger(0)}$
− 3	0.6609	0.6568	0.6771
0	0.9775	1.1046	1.1287
3	1.3646	1.7016	1.7305
10	2.5102	3.5042	3.5388

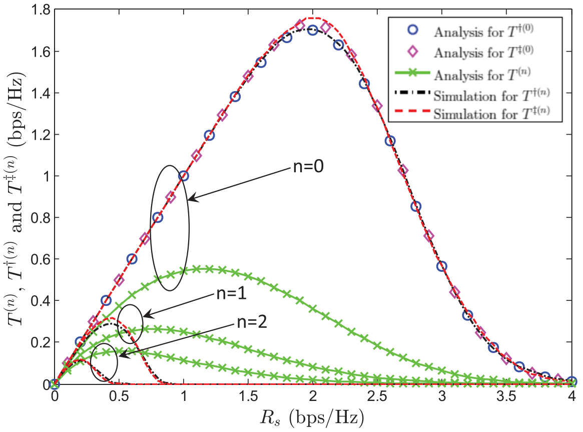

Fig. 6 Simulation results of EST for suboptimal scheme and optimal scheme on basis of SNR = 3 dB

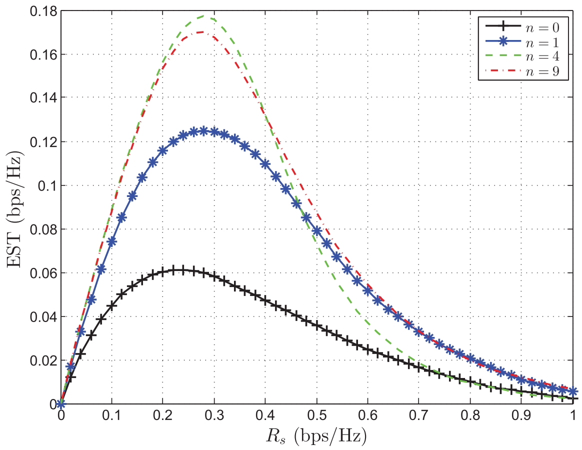

Fig. 8 Simulation results of EST for alternative scheme on basis of SNR = 3 dB

SIC order (decoded firstly) retards the performance. We also note the highest maximum EST occurs at $n = 4$ with a poor value less than 0.18 bps/Hz. All in all, the secrecy performance regarding the maximum sum-EST for this scheme is significantly worse than the other three schemes mentioned above.

Therefore, in this model of MAC-WT, to promote the security of the network, the users with bad conditions can play a role of jammers [21]. When their channel conditions improve, they can change their role of the jammers into the normal users, while other bad-conditioned users switch to the role of jammers.

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

6 Conclusions

In this work, we considered the quasi-static Rayleigh fading homogeneous MAC-WT with SIC decoding at the legitimate satellite and investigated the individual secrecy performance under an arbitrary SIC order by deriving the closed-form expressions of the secrecy outage probability and the effective secrecy throughput. We provided valuable insights into the impacts of the SIC order and the multi-user diversity on the secrecy performance. Three SIC order scheduling schemes were studied such that the suboptimal scheme and the optimal scheme have better performance in achieving the maximum sum-EST and the multi-user diversity gain while the round-robin scheme is a good option for fairness. In addition, the suboptimal scheme achieves the performance highly close to the ideal but usually impractical optimal scheme in terms of the EST and the multi-user diversity gain. We verified our analysis with the aid of numerical results.

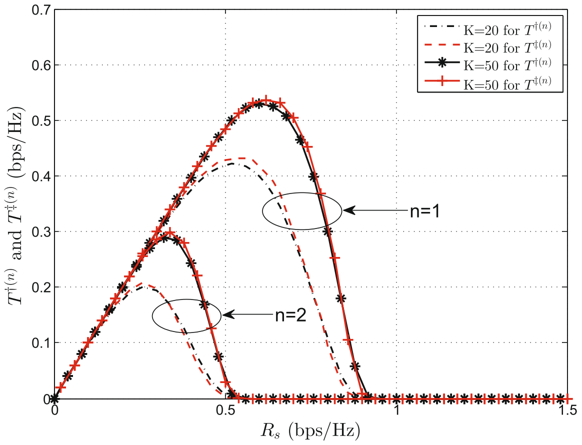

Fig. 7 Simulation results of multi-user diversity impacts on EST for suboptimal scheme and optimal scheme on basis of SNR = 3 dB

Endnotes

[1] The abbreviation of multiple access wiretap channel is a bit of confusion. It seems MAWC is more appropriate, yet, MAC-WT is more frequently used in the existing literature.

[2] The satellite channel model varies from different environments, which is beyond the scope of this paper. We just simplify it to be Rayleigh fading the same as some other literature, e.g., [52, 53] concerning low earth orbit (LEO) satellite communications.

[3] The superscript of † is used to specify corresponding notations for this scheme.

[4] The superscript of ‡ is used to differ corresponding notations from the other two schemes.

Appendix A

Assume a random variable $X \sim \text{Exp}(\lambda_0)$, and a random variable $Y_n = \sum_{i=1}^{n} \xi_i$, where $\xi_1, \xi_2, \ldots, \xi_n$ are independently and exponentially distributed, i.e., $\xi_i \sim \text{Exp}\left(\lambda_i\right)$ $(i = 1, \ldots, n)$ and $\lambda_i \neq \lambda_j, \forall i \neq j$. Further assume X and Y_n are independent.

Thus, the CDF of a random variable $Z_n = \frac{X}{1+Y_n}$ can be expressed as

$$\begin{aligned} F_{Z_n}(z) &= \int_0^{\infty} \int_0^{zy+z} f_{Y_n}(y) f_X(x)\, dx dy \\ &= \int_0^{\infty} f_{Y_n}(y)\, F_X(zy+z)\, dy \\ &= 1 - \underbrace{\int_0^{\infty} f_{Y_n}(y) \exp\left(-\lambda_0 (zy+z)\right) dy}_{L_1}, \end{aligned} \tag{44}$$

where,

$$F_X(x) = \begin{cases} 1 - \exp\left(-\lambda_0 x\right), & x \geq 0 \\ 0, & x < 0. \end{cases} \tag{45}$$

The PDF of Y_n is derived in [54],

$$f_{Y_n}(y) = \begin{cases} f_1(y) \prod_{i=1}^{n} \lambda_i, & y > 0 \\ 0, & y \leq 0. \end{cases} \tag{46}$$

where

$$\begin{aligned} f_1(y) =& \frac{\exp\left(-\lambda_1 y\right)}{\prod_{i=2}^{n} \left(\lambda_i - \lambda_1\right)} + \cdots \\ &+ \frac{(-1)^{k-1} \exp\left(-\lambda_k y\right)}{\prod_{i=k+1}^{n} \left(\lambda_i - \lambda_k\right) \prod_{j=1}^{k-1} \left(\lambda_k - \lambda_j\right)} + \cdots \\ &+ (-1)^{n-1} \frac{\exp\left(-\lambda_n y\right)}{\prod_{j=1}^{n-1} \left(\lambda_n - \lambda_j\right)}. \end{aligned} \tag{47}$$

Substitute (47) into L_1, and obtain,

$$\begin{aligned} L_1 &= \left(\prod_{i=1}^{n} \lambda_i\right) \int_0^{\infty} f_1(y) \exp\left(-\lambda_0 (zy+z)\right) dy \\ &= \exp\left(-\lambda_0 z\right) \frac{\prod_{i=1}^{n} \lambda_i}{\prod_{i=1}^{n} \pi_i} \underbrace{\int_0^{\infty} \overbrace{f_2(y) \prod_{i=1}^{n} \pi_i}^{L_2}\, dy}_{L_3}, \end{aligned} \tag{48}$$

where $\pi_i = \lambda_i + \lambda_0 z$, $i = 1, \ldots, n$, and,

$$\begin{aligned} f_2(y) =& \frac{\exp\left(-\pi_1 y\right)}{\prod_{i=2}^{n} \left(\pi_i - \pi_1\right)} + \cdots \\ &+ \frac{(-1)^{k-1} \exp\left(-\pi_k y\right)}{\prod_{i=k+1}^{n} \left(\pi_i - \pi_k\right) \prod_{j=1}^{k-1} \left(\pi_k - \pi_j\right)} + \cdots \\ &+ (-1)^{n-1} \frac{\exp\left(-\pi_n y\right)}{\prod_{j=1}^{n-1} \left(\pi_n - \pi_j\right)}. \end{aligned} \tag{49}$$

We note that the function $f_2(y)$ has the same structure as $f_1(y)$. Hence, L_2 is similar to (46), which is a PDF. In particular, when applying a zero-to-infinity integral of this PDF, we get $L_3 = 1$, simplifying (48) into

$$\begin{aligned} L_1 &= \exp\left(-\lambda_0 z\right) \frac{\prod_{i=1}^{n} \lambda_i}{\prod_{i=1}^{n} \pi_i} \\ &= \exp\left(-\lambda_0 z\right) \frac{\prod_{i=1}^{n} \lambda_i}{\prod_{i=1}^{n} \left(\lambda_i + \lambda_0 z\right)}, \end{aligned} \tag{50}$$

Furthermore, substitute (50) into (44), achieving,

$$F_{Z_n}(z) = \begin{cases} 1 - \exp\left(-\lambda_0 z\right) \frac{\prod_{i=1}^{n} \lambda_i}{\prod_{i=1}^{n} (\lambda_i + \lambda_0 z)}, & z \geq 0 \\ 0, & z < 0. \end{cases} \tag{51}$$

Finally, substituting specific parameters into (51) obtains both (6) and (7).

By the way, during the derivation of the PDF of Y_n, we assume that the mean of ξ_i $(i = 1, \ldots, n)$ in Y_n is not equal to each other, that is, $\lambda_i \neq \lambda_j, \forall i \neq j$. Actually, we can loose the assumption to the general case that there are m of them with the same mean. We set $Y_n = Y_{n-m}^{'} + Y_m^{''}$, where $Y_{n-m}^{'}$ denotes the sum of all $n-m$ random variables with different means, while $Y_m^{''}$ denotes the sum of all m random variables with the same mean. The PDF of $Y_{n-m}^{'}$ can be obtained from (46), whereas $Y_m^{''} \sim \chi_{2m}^2$. And the PDF of Y_n can be obtained by the convolution of the PDF of $Y_{n-m}^{'}$ and that of $Y_m^{''}$,

$$f_{Y_n}(y) = \int_{-\infty}^{+\infty} f_{Y_{n-m}^{'}}(x) f_{Y_m^{''}}(y-x)\, dx. \tag{52}$$

As a result, substituting (52) into (44) yields the same result as (51).

Appendix B

According to the statistics of the variables ξ_i $(i \in \mathcal{K})$ and ρ, we first derive the secrecy outage probability of the user who has the best channel condition and is decoded at last (no cochannel interference at all),

$$\begin{aligned} & P_{\text{so}}^{\dagger(0)}(R_s) \\ &= \Pr\left(\max_i \xi_i < 2^{R_s}\rho + 2^{R_s} - 1\right) \\ &= \int_0^{\infty} \left(1 - e^{-\lambda\left(2^{R_s}\rho + 2^{R_s} - 1\right)}\right)^K f_\rho(\rho)\, d\rho \\ &\overset{(a)}{=} \int_0^{\infty} \left(1 + \sum_{i=1}^{K} \binom{K}{i} \frac{(-1)^i}{e^{\lambda\left(2^{R_s}\rho + 2^{R_s} - 1\right)i}}\right) f_\rho(\rho)\, d\rho \\ &= 1 + \int_0^{\infty} \frac{(1+\rho)\mu + K - 1}{(1+\rho)^K e^{\mu\rho}} \sum_{i=1}^{K} \binom{K}{i} \frac{(-1)^i}{e^{\lambda\left(2^{R_s}\rho + 2^{R_s} - 1\right)i}}\, d\rho \\ &= 1 + \sum_{i=1}^{K} \binom{K}{i} (-1)^i e^{-\lambda\left(2^{R_s} - 1\right)i} \left\{\Theta_1^{'}(i) + \Theta_2^{'}(i)\right\}, \end{aligned} \tag{53}$$

$$\tag{54}$$

where $\Theta_1^{'}(i)$ and $\Theta_2^{'}(i)$ is given in (34) and (35), respectively. The step (a) is obtained by applying the Newton binomial theorem.

Therefore, the corresponding EST can be expressed as (33).

Acknowledgements
This work was supported by the National Natural Science Foundation of China (Grant Nos. 61572070 and 61371069) and the Specialized Research Fund for the Doctoral Program of Higher Education (Grant No. 20130009110015).

Authors' contributions
KJ conceived the idea of the system model and designed the proposed schemes. FZ performed simulations of the proposed schemes. YH and ZL provided substantial comments on the work. TJ supported and supervised the research. All of the authors participated in the project, and they read and approved the final manuscript.

Competing interests
The authors declare that they have no competing interests.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Received: 24 February 2017 Accepted: 19 September 2017
Published online: 05 October 2017

References

1. AD Wyner, The wire-tap channel. Bell Syst. Tech. J. **54**, 1355–1387 (1975)
2. I Csiszar, J Korner, Broadcast channels with confidential messages. IEEE Trans. Inf. Theory. **24**(3), 339–348 (1978)
3. SK Leung-Yan-Cheong, ME Hellman, The gaussian wire-tap channel. IEEE Trans. Inf. Theory. **IT-24**(4), 451–456 (1978)
4. J Barros, MRD Rodrigues, in *2006 IEEE International Symposium on Information Theory*. Secrecy capacity of wireless channels (IEEE, Seattle, 2006), pp. 356–360
5. PK Gopala, L Lai, HE Gamal, On the secrecy capacity of fading channels. IEEE Trans. Inf. Theory. **54**(10), 4687–4698 (2008)
6. N Yang, S Yan, J Yuan, R Malaney, I Land, Artificial noise: transmission optimization in multi-input single-output wiretap channels. IEEE Trans. Commun. **63**(5), 1771–1783 (2015)
7. M Jilani, T Ohtsuki, Joint svd-gsvd precoding technique and secrecy capacity lower bound for the mimo relay wire-tap channel. EURASIP Journal on Wireless Communications and Networking. **2012**(1), 361 (2012)
8. F Zhu, F Gao, M Yao, Zero-forcing beamforming for physical layer security of energy harvesting wireless communications. EURASIP J. Wireless Commun. Netw. **2015**(1), 58 (2015)
9. W Wu, B Wang, Robust secrecy beamforming for wireless information and power transfer in multiuser miso communication system. EURASIP J. Wireless Commun. Netw. **2015**(1), 161 (2015)
10. C Wang, HM Wang, DWK Ng, XG Xia, C Liu, Joint beamforming and power allocation for secrecy in peer-to-peer relay networks. IEEE Trans. Wirel. Commun. **14**(6), 3280–3293 (2015)
11. W Li, M Ghogho, B Chen, C Xiong, Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis. IEEE Commun. Lett. **16**(10), 1628–1631 (2012)
12. Z Lin, Y Cai, W Yang, X Xu, Opportunistic relaying and jamming with robust design in hybrid full/half-duplex relay system. EURASIP J. Wireless Commun. Netw. **2016**(1), 129 (2016)
13. M Wiese, J Notzel, H Boche, A channel under simultaneous jamming and eavesdropping attack — correlated random coding capacities under strong secrecy criteria. IEEE Trans. Inf. Theory. **62**(7), 3844–3862 (2016)
14. Y Wang, Z Miao, R Sun, L Jiao, Distributed coalitional game for friendly jammer selection in ultra-dense networks. EURASIP J. Wireless Commun. Netw. **2016**(1), 211 (2016)
15. Z Li, T Jing, X Cheng, Y Huo, W Zhou, D Chen, in *2015 IEEE International Conference on Communications (ICC)*. Cooperative jamming for secure communications in mimo cooperative cognitive radio networks (IEEE, London, 2015), pp. 7609–7614
16. B Li, Z Fei, Robust beamforming and cooperative jamming for secure transmission in df relay systems. EURASIP J. Wireless Commun. Netw. **2016**(1), 68 (2016)
17. L Li, Y Xu, Z Chen, J Fang, Robust transmit design for secure af relay networks with imperfect csi. EURASIP J. Wireless Commun. Netw. **2016**, 142 (2016)
18. N Yang, M Elkashlan, TQ Duong, J Yuan, R Malaney, Optimal transmission with artificial noise in misome wiretap channels. IEEE Trans. Veh. Technol. **65**(4), 2170–2181 (2016)
19. M Bloch, J Barros, *Physical-layer security: from information theory to security engineering*. (Cambridge University Press, Cambridge, 2011)
20. D Tse, P Viswanath, *Fundamentals of wireless communication*. (Cambridge University Press, Cambridge, 2005)
21. E Tekin, A Yener, The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. IEEE Trans. Inf. Theory. **54**(6), 2735–2751 (2008)
22. E Tekin, A Yener, in *Proc. Annual Allerton Conf*. Secrecy sum-rates for the multiple-access wire-tap channel with ergodic block fading (IEEE, Illinois, 2007), pp. 856–863
23. H Zivari-Fard, B Akhbari, M Ahmadian-Attari, MR Aref, Multiple access channel with common message and secrecy constraint. IET Commun. **10**(1), 98–110 (2016)
24. H Zivari-Fard, B Akhbari, M Ahmadian-Attari, MR Aref, Imperfect and perfect secrecy in compound multiple access channel with confidential message. IEEE Trans. Inf. Forensics Secur. **11**(6), 1239–1251 (2016)
25. J Xie, S Ulukus, in *2013 IEEE International Symposium on Information Theory*. Secure degrees of freedom of the gaussian multiple access wiretap channel (IEEE, Istanbul, 2013), pp. 1337-1341
26. Y Fan, X Liao, Z Gao, L Sun, in *2016 IEEE International Conference on Communications Workshops (ICC)*. Physical layer security based on real interference alignment in k-user mimo y wiretap channels (IEEE, Kuala Lumpur, 2016), pp. 207–212
27. P Mukherjee, S Ulukus, in *2016 IEEE International Conference on Communications (ICC)*. Real interference alignment for the mimo multiple access wiretap channel (IEEE, Kuala Lumpur, 2016), pp. 1–6
28. RA Chou, MR Bloch, in *2014 IEEE Conference on Communications and Network Security*. Uniform distributed source coding for the multiple access wiretap channel (IEEE, San Francisco, 2014), pp. 127–132
29. M Hajimomeni, H Aghaeinia, IM Kim, K Kim, Cooperative jamming polar codes for multiple-access wiretap channels. IET Commun. **10**(4), 407–415 (2016)
30. YP Wei, S Ulukus, Polar coding for the general wiretap channel with extensions to multiuser scenarios. IEEE J. Selected Areas Commun. **34**(2), 278–291 (2016)
31. R Bassily, S Ulukus, Ergodic secret alignment. IEEE Trans. Inf. Theory. **58**(3), 1594–1611 (2012)
32. J Xie, S Ulukus, in *2013 Asilomar Conference on Signals, Systems and Computers*. Secure degrees of freedom region of the gaussian multiple access wiretap channel (IEEE, Pacific Grove, 2013), pp. 293–297
33. P Mukherjee, S Ulukus, in *2015 IEEE International Symposium on Information Theory (ISIT)*. Secure degrees of freedom of the multiple access wiretap channel with no eavesdropper csi (IEEE, Hong Kong, 2015), pp. 2311–2315
34. P Mukherjee, S Ulukus, in *2015 49th Asilomar Conference on Signals, Systems and Computers*. Secure degrees of freedom of the mimo multiple access wiretap channel (IEEE, Pacific Grove, 2015), pp. 554–558
35. H Jin, WY Shin, BC Jung, On the multi-user diversity with secrecy in uplink wiretap networks. IEEE Commun. Lett. **17**(9), 1778–1781 (2013)
36. Y Zou, J Zhu, G Wang, H Shao, in *2014 IEEE/CIC International Conference on Communications in China (ICCC)*. Secrecy outage probability analysis of multi-user multi-eavesdropper wireless systems (IEEE, Shanghai, 2014), pp. 309–313
37. Y Jiang, J Zhu, Y Zou, in *2015 IEEE 14th International Conference on Cognitive Informatics & Cognitive Computing (ICCI*CC)*. Secrecy outage analysis of multi-user cellular networks in the face of cochannel interference (IEEE, Beijing, 2015), pp. 441–446
38. Z Ni, J Fei, C Xing, D Zhao, N Wang, J Kuang, Secrecy balancing over two-user miso interference channels with rician fading. Int. J. Antennas Propag. **2013**(2013), 1–7

39. K Jiang, T Jing, Z Li, Y Huo, F Zhang, in *INFOCOM*. Analysis of secrecy performance in fading multiple access wiretap channel with sic receiver (IEEE, Atlanta, 2017), pp. 1602–1610
40. K Jiang, T Jing, F Zhang, Y Huo, Z Li, Zf-sic based individual secrecy in simo multiple access wiretap channel. IEEE Access. **5**, 7244–7253 (2017)
41. N Li, X Tao, Q Cui, J Xu, in *2015 IEEE Wireless Communications and Networking Conference (WCNC)*. Secure transmission with artificial noise in the multiuser downlink: Secrecy sum-rate and optimal power allocation (IEEE, New Orleans, 2015), pp. 1416–1421
42. AB Reid, AJ Grant, PD Alexander, List detection for the k-symmetric multiple-access channel. IEEE Trans. Inf. Theory. **51**(8), 2930–2936 (2005)
43. S Nitinawarat, in *2011 IEEE International Symposium on Information Theory Proceedings*. On maximal error capacity regions of symmetric gaussian multiple-access channels (IEEE, St. Petersburg, 2011), pp. 2258–2262
44. RA Chou, MR Bloch, J Kliewer, in *2014 IEEE Information Theory Workshop (ITW 2014)*. Low-complexity channel resolvability codes for the symmetric multiple-access channel (IEEE, Hobart, 2014), pp. 466–470
45. S Salehkalaibar, MR Aref, Lossy transmission of correlated sources over multiple-access wiretap channels. IET Commun. **9**(6), 754–770 (2015)
46. AS Bendary, YZ Mohasseb, H Dahshan, in *2016 IEEE Conference on Communications and Network Security (CNS)*. On the secure degrees of freedom for the k-user symmetric mimo wiretap mac channel (IEEE, Philadelphia, 2016), pp. 591–595
47. M Chraiti, A Ghrayeb, C Assi, in *2016 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*. Achieving full secure degrees-of-freedom for the miso wiretap channel with an unknown eavesdropper, (2016), pp. 997–1001
48. A Chaaban, Z Rezki, B Alomair, MS Alouini, in *2016 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*. The miso wiretap channel with channel uncertainty: Asymptotic perspectives (IEEE, Washington, 2016), pp. 959–963
49. Z Rezki, A Chaaban, B Alomair, MS Alouini, in *2016 IEEE Global Communications Conference (GLOBECOM)*. The miso wiretap channel with noisy main channel estimation in the high power regime (IEEE, Washington, 2016), pp. 1–5
50. E Tekin, A Yener, The gaussian multiple access wire-tap channel. IEEE Trans. Inf. Theory. **54**(12), 5747–5755 (2008)
51. IS Gradshteyn, IM Ryzhik, *Table of integrals, series and products*, 7th. (Academic Press, New York, 2007)
52. N Lebedev, JF Diouris, in *Conference record of the thirty-fourth Asilomar conference on signals, systems and computers*. Capacity study of a leo satellite link with multiple antennas user terminals (IEEE, Pacific Grove, 2000), pp. 511–515
53. LH Abderrahmane, DEB Hamed, M Benyettou, in *2008 IEEE Aerospace Conference*. Design of an adaptive communication system for implementation on board a future algerian leo satellite (IEEE, Big Sky, 2008), pp. 1–5
54. S Shulong, On distribution of sums of n independent random variables subject to exponential distribution. J. Liaoning Normal Univ. **13**(4), 51–58 (1990)