Achievable Secrecy Rate Region for Buffer-Aided Multiuser MISO Systems

Xiaolong Lan, *Member, IEEE*, Juanjuan Ren, *Student Member, IEEE*, Qingchun Chen, *Senior Member, IEEE,* and Lin Cai

***Abstract*— In this paper, we consider a buffer-aided multiuser multiple-input single-output (MISO) network consisting of one multi-antenna access point (AP) and multiple single-antenna users, in which the AP is provisioned with data buffers for temporarily storing the data for each user either from the upper layer applications or the message by the AP. The data for one specific user must be kept confidential from all other unintended users. For such a system, we aim at maximizing the long-term average achievable secrecy rate region by carefully designing the flow control, the information signal and artificial noise beamforming, as well as the user selection. To address this issue, we first transform the time average optimization problem into a real-time one by using the Lyapunov optimization framework. Then it is proposed to decompose the optimization problem into several sub-problems by using the optimization decomposition technique. Although the information signal and artificial noise beamforming sub-problem is non-convex, we show that it can be decomposed into a two-stage optimization problem to effectively solve it by using the exact line search and DC (difference of two convex functions) algorithms. Moreover, we extend the average secrecy rate region maximization problem to the worst-case scenario, in which all unintended users are colluding in eavesdropping. Our analysis discloses that, there exists an inherent tradeoff between the average achievable secrecy rate region and the average queueing length. It is shown that a better average secrecy rate region can be realized by fully taking advantage of the buffer-aided transmission potentials in the MISO network, if a certain queueing delay is tolerable.**

***Index Terms*— Buffer-aided MISO network, artificial noise beamforming, secrecy rate region, eavesdroppers.**

Manuscript received June 13, 2019; revised November 15, 2019 and March 5, 2020; accepted April 10, 2020. Date of publication April 20, 2020; date of current version May 5, 2020. This work was supported in part by the National Natural Science Foundation of China (NSFC) under Grant 61771406, in part by the Chinese Scholarship Council (CSC), and in part by the Natural Sciences and Engineering Research Council of Canada (NSERC) and Compute Canada. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Matthieu R. Bloch. *(Corresponding author: Qingchun Chen.)*

Xiaolong Lan is with the College of Cybersecurity, Sichuan University, Chengdu 610065, China (e-mail: xiaolonglan1112@gmail.com).

Juanjuan Ren is with the School of Information Science and Technology, Southwest Jiaotong University, Chengdu 611756, China (e-mail: juanjuanren@foxmail.com).

Qingchun Chen is with the Department of Electronics and Communication Engineering, Guangzhou University, Guangzhou 510006, China (e-mail: qcchen@gzhu.edu.cn).

Lin Cai is with the Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC V8W 3P6, Canada (e-mail: cai@ece.uvic.edu).

Digital Object Identifier 10.1109/TIFS.2020.2988567

I. Introduction

OWING to the broadcast nature of the wireless medium, information transmission by legitimate users over wireless channels is vulnerable to eavesdropping attacks by unintended receivers. On the other hand, the secure transmission of private data in wireless communications becomes increasingly important and highly desirable. To this end, physical layer security techniques have attracted considerable research attention [1]–[9]. Unlike the crypto-based security system that relies on a trustable key distribution system via a separate secure channel, physical layer security ensures secure transmission of private data by utilizing the physical characteristics of wireless channels. Wyner has shown in [10] that perfect secure communication is theoretically achievable as long as the wireless channel of the eavesdropper is weaker than that of the legitimate user. However, the secrecy transmission rate might be very low or even zero when the wireless channel of the authorized user is poor. Subsequently, the artificial noise based secure transmission protocol was proposed to enhance the secrecy rate, in which artificially generated noise will be intentionally introduced to confuse the eavesdroppers [11]–[16]. In addition, the multi-antenna transmission technique provides us an alternative solution to improve the secrecy rate by exploiting the spatial degree of freedom [17]–[24]. For instance, with multi-antenna, effective information signal beamforming technique can be utilized to weaken the received signal at eavesdroppers, resulting in a higher secrecy rate. In [11], it is proposed to weaken the channel of eavesdropper by using a portion of the available power to generate artificial noise, which gives rise to the improved secrecy rate. The secrecy rate maximization problem was studied in [17], in which the transmitter is equipped with multi-antennas so that it can design an effective beamforming scheme to enhance the intended user's received signal. The secrecy outage probability in downlink wireless networks with randomly located eavesdroppers was analyzed in [24], in which the transmit antenna selection and the artificial noise signal were jointly considered to strengthen secrecy.

Physical layer security techniques for multiple-user MISO systems have attracted many research efforts in [4], [12], [13], [15]–[23]. These works aim at either maximizing the secrecy rate [21]–[23] or minimizing the power consumption [16], [19], [20]. In these works, legitimate users might be potential eavesdroppers. When the channel

state information (CSI) of eavesdroppers are known, the optimal information signal beamforming and artificial noise beamforming can be jointly designed to maximize the secrecy rate [15], [17], [20]. Recently, the secrecy rate maximization with imperfect CSIs was investigated to show how to devise robust secure beamforming schemes in [12], [18], [19]. The maximum ratio transmission (MRT) based information signal beamforming and zero-forcing (ZF) based artificial noise beamforming schemes were proposed to cope with uncertainties in CSIs of eavesdroppers in [11], [13], [16]. Although there are well-established algorithms to design the signal beamforming and artificial noise beamforming scheme, most of the research results focused on how to maximize the secrecy sum rate or the secrecy rate of a specific legitimate user. The heterogeneous data arrival process was not considered yet, which may make the beamforming design unsuitable for the actual application requirements. This is exactly the first motivation of our work in this paper.

Meanwhile, the buffer-aided transmission strategy can enable better scheduling transmission according to the underlying CSI, the buffer state information and the energy consumption status in either the physical layer or the link layer [25]–[31]. In the buffer-aided communication system, the data traffic from other nodes or upper layer applications can be stored in the data buffer at first, and then will be adaptively transmitted, hence giving rise to a higher transmission efficiency in terms of either a better throughput or less energy consumption at the expense of some increase in the queueing delay. In the multiple relay cooperative non-orthogonal multiple access networks, a novel prioritization-based buffer-aided relay selection scheme was proposed in [31], and it was shown that applying buffers at relays can further improve the achievable throughput. Recently, some works began to study the impact of data buffer on the secure communication, and their efforts were mainly focused on secure relay networks [32]–[36]. In [33], the transmit power and link selection were jointly optimized to maximize the average secrecy rate for the buffer-aided energy harvesting relay network. A link adaptive selection scheme was proposed in [34], and it is shown that the buffer-aided relaying can significantly improve the achieved security. Considering the advantages of buffer-assisted transmission, a new max-ratio relay selection scheme was proposed for the multi-relay network to optimize the secrecy transmission in [36], in which all the possible source-to-relay and relay-to-destination links are compared to select the relay with the maximum signal-to-eavesdropper channel gain ratio. Although the buffer-aided transmission has shown its great potential in improving communication performance, to the best of authors' knowledge, the effect of data buffer on the secure transmission in the multiuser MISO system has not been studied before. In addition, for such a MISO network, when the AP is equipped with data buffers to temporarily store the users' data, three basic questions should be addressed: (i) how to design an appropriate flow control scheme to ensure the stability of the data queues? (ii) how to develop an efficient information signal beamforming and artificial noise beamforming? (iii) how to select the user at each time slot based on current data queue backlog and CSI to improve the secrecy rate? These questions motivate our research reported in this paper.

We focus on a buffer-aided multiuser MISO system, in which one AP is provisioned with the data buffers for temporarily storing the data for each user either from the upper layer applications or the message by the AP itself. To improve the achievable secrecy rate of all users, we consider both the information signal beamforming and artificial noise beamforming design. In addition, different users may have quite different confidential traffic arrival rates, for instance, in practical email/text message transfer and video conferencing transmission. To effectively adapt to heterogeneous data traffics, different confidential data arrival processes by different users are also considered in this paper. Based on the aforementioned problem formulation, the opportunistic scheduling problem is formulated to maximize the average secrecy rate region, *i.e.*, the maximum heterogeneous data traffic arrival rate region that the system can support, subject to the short-term (peak) and long-term (average) power consumption, as well as data queue causality constraints. To address the issue, we transform the aforementioned time-average optimization problem into a queue stability problem and then decompose it into several sub-problems to obtain the adaptive transmission scheme. The main contributions of the paper are summarized as follows,

- An adaptive transmission scheme is proposed in this paper to effectively improve the long-term average secrecy rate by carefully designing the information signal and artificial noise beamforming, flow control, and user selection. Moreover, we extend the average secrecy rate region maximization problem to the worst-case scenario, in which all unintended users are colluding in eavesdropping. Furthermore, it is shown that the proposed beamforming scheme is superior to the superposition of the MRT and ZF beamforming scheme.
- It is proposed to transform the information signal and artificial noise beamforming design problem into an equivalent problem by using semidefinite relaxation, which will be further decomposed into a two-stage optimization problem. We show that the external problem can be solved by employing a one-dimensional search, while the internal problem can be handled by using a DC (difference of two convex functions) programming algorithm.
- An inherent tradeoff between the average secrecy rate region and the average queueing size is disclosed to show that, the proposed adaptive transmission scheme can achieve the near-optimal average secrecy rate, if a certain queueing delay is tolerable.

The remainder of this paper is organized as follows. Section II presents the system model. In Section III, we present the adaptive transmission scheme design to maximize the average achievable secrecy rate region. In Section IV, we discuss the worst-case scenario, in which all unintended users collude in eavesdropping. Numerical results are presented in Section V to verify the effectiveness of the proposed scheme. Finally, Section VI concludes our work in this paper.

All the boldface letters represent vectors (lower case) or matrices (upper case). $|x|$ denotes the magnitude of a complex variable x, $||\boldsymbol{x}||$ denotes the l_2-norm of a complex vector $\boldsymbol{x}$. $\mathrm{Tr}(\boldsymbol{A})$ denotes the trace of a matrix $\boldsymbol{A}$. $\boldsymbol{A} \succeq 0$ denotes that

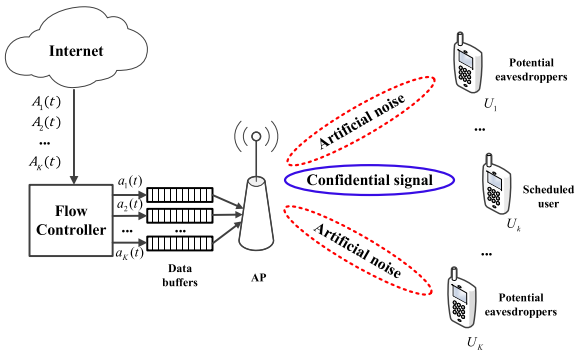


Fig. 1. Multiuser MISO system model.

the matrix $\boldsymbol{A}$ is positive semidefinite. The superscript $(\cdot)^H$ and $(\cdot)^T$ denotes the conjugate transpose and the transpose, respectively. $\det(\boldsymbol{A})$ and $\text{rank}(\boldsymbol{A})$ denotes the determinant and rank of a matrix $\boldsymbol{A}$, respectively.

II. System Model and Problem Formulation

A. Network Model

As shown in Fig. 1, let us consider a downlink network consisting of a multi-antenna AP and K single-antenna users, in which the AP is assumed to be equipped with N antennas. Let U_k and $\mathcal{K} = \{1, 2, \ldots, K\}$ denote the k-th user and the set of users in the MISO system, respectively. All users are supposed to receive the corresponding confidential information from the AP in a time division multiple access (TDMA) manner. We assume that the AP is provisioned with K data buffers, which are used to temporarily store the data for each user either from the upper layer applications or the message by the AP. As depicted in Fig. 1, there is a flow controller to control the amount of data actually placed in K data buffers. In the time-slotted system, let $A_k(t)$ denote the amount of data bits for U_k from upper layer applications or the message by the AP at time t. The amount of data bits for U_k that are actually placed in the corresponding data buffer at time t is denoted by $a_k(t)$. Note that if $a_k(t) < A_k(t)$, the AP will send an acknowledgment to the upper layer to inform that some data has been dropped because the current arrival rate of U_k is slightly higher, thus the arrival rate in the next time slot should be reduced accordingly. Let $Q_k(t)$ denote the data queue state of U_k in time slot t. In this paper, we assume that the data queue size is large enough such that the overflow probability of buffer is negligible. In Lemma 3 and Theorem 1, we will show that, there exists an upper bound on the data queue length, namely, there is no overflow if the data buffer size is large enough. All the involved links are assumed to be block fading such that the channel coefficients remain unchanged in each time slot, but may change independently from one time slot to next. Let $\boldsymbol{h}_k^H(t) \in \mathbb{C}^{N\times 1}$ denote the channel coefficient vector between the AP and U_k. Meanwhile, we assume that the AP can acquire perfect CSIs and all channels are reciprocal.

We assume that at most one user can be selected for transmission in each time slot. K binary variables of $\{d_k(t) \in \{0, 1\}, k \in \mathcal{K}\}$ are used to indicate whether the corresponding user is scheduled for transmission in the t-th time slot. $d_k(t) = 1$ if U_k is scheduled during time slot t, otherwise $d_k(t) = 0$. Due to the broadcast nature of the wireless channel, those $K-1$ unscheduled users can still receive the scheduled user's signal from the AP, resulting in the threat of eavesdropping. So in our proposed scheme, the AP regards all the unscheduled users as potential eavesdroppers to avoid the possible information disclosure. In addition, to enhance the security of the MISO system, we assume that the AP can use part of its transmit power to generate the artificial noise to interfere with unscheduled users. When U_k is scheduled to receive the confidential data from the AP in time slot t, the transmit signal by the AP can be given by

$$\boldsymbol{x}_k(t) = \boldsymbol{w}_k(t)s_k(t) + \boldsymbol{z}_k(t)q_k(t), \tag{1}$$

where $s_k(t)$ and $q_k(t)$ denotes the transmit symbol and artificial noise symbol for U_k with $\mathbb{E}[|s_k(t)|^2] = \mathbb{E}[|q_k(t)|^2] = 1$, respectively. $\boldsymbol{w}_k(t) \in \mathbb{C}^{N\times 1}$ and $\boldsymbol{z}_k(t) \in \mathbb{C}^{N\times 1}$ stands for the information signal and artificial noise beamforming vector, respectively. The received signal at U_i can thus be given by

$$y_i(t) = \boldsymbol{h}_i(t)\boldsymbol{x}_k(t) + n_i(t), \quad i \in \mathcal{K}, \tag{2}$$

where $n_i(t) \sim \mathcal{CN}(0, 1)$ is independent identically distributed $(i.i.d.)$ additive white Gaussian noise.

Given $\boldsymbol{w}_k(t)$ and $\boldsymbol{z}_k(t)$, the achievable secrecy rate at U_k is given by [37]

$$R_s^k(t) = \big(C_k(t) - \max_{i\in\mathcal{K}\setminus\{k\}} C_{e,i}(t)\big)^+, \tag{3}$$

where $(\cdot)^+ = \max\{\cdot, 0\}$ and

$$C_k(t) = \log_2\Big(1 + \frac{|\boldsymbol{h}_k(t)\boldsymbol{w}_k(t)|^2}{1 + |\boldsymbol{h}_k(t)\boldsymbol{z}_k(t)|^2}\Big), \tag{4}$$

$$C_{e,i}(t) = \log_2\Big(1 + \frac{|\boldsymbol{h}_i(t)\boldsymbol{w}_k(t)|^2}{1 + |\boldsymbol{h}_i(t)\boldsymbol{z}_k(t)|^2}\Big), \quad i \in \mathcal{K}\setminus\{k\}. \tag{5}$$

$C_k(t)$ and $C_{e,i}(t)$ stands for the mutual information at the scheduled user U_k and at the non-intended user U_i, respectively. Once U_k is selected to receive the confidential data from the AP, the AP will extract data of U_k from the corresponding data buffer. For each secure transmission, we assume that the AP uses the codebook $\mathcal{C}(2^{nC_k(t)}, 2^{nR_s^k(t)}, n)$, where the codebook contains $2^{nC_k(t)}$ independently and identically generated codewords, $2^{nR_s^k(t)}$ is the number of confidential message to be transmitted, and n is the codeword length. All $2^{nC_k(t)}$ codewords are firstly equally partitioned into $2^{nR_s^k(t)}$ bins. To send confidential message $w \in \{1, \ldots, 2^{nR_s^k(t)}\}$, one codeword $s_k(t)$ will be randomly selected from bin w to transmit over the wireless channel [32]. Thus, the actual confidential message payload of U_k for the secure transmission is $R_s^k(t)$, and $\max_{i\in\mathcal{K}\setminus\{k\}} C_{e,i}(t)$ can be regarded as the security overhead. In addition, since the amount of actual departure data of U_k does not exceed the confidential data stored in its data buffer, $i.e.$, the actual departure secrecy rate equals to $\min\{Q_k(t)/\mathcal{T}, R_s^k(t)\}$, the evolution of data queue at U_K can be given by [34]

$$Q_k(t+1) = \Big(Q_k(t) + a_k(t) - d_k(t)R_s^k(t)\mathcal{T}\Big)^+, \tag{6}$$

where $\mathcal{T}$ is the duration of one time slot. For simplicity, we assume a normalized unit time slot, $i.e.$, $\mathcal{T} = 1$.

B. Problem Formulation

Our objective is to maximize the average secrecy rate region subject to the average and peak transmit power constraint of the AP and the practical constraint on data queue causality. Since the AP is equipped with data buffers to store the data for the corresponding user, an appropriate flow control scheme is required to ensure the stability of all data queues, *i.e.*, the size of data queues cannot increase to infinity over time. When the perfect CSI and buffer state information are assumed available at the AP, we focus on designing the optimal information signal beamforming vector, the artificial noise beamforming vector, flow control, and user selection scheme to maximize the average secrecy rate region. The achievable secrecy rate region can be obtained by maximizing the following average weighted secrecy sum-rate for all possible weighting coefficients $\theta_k \in [0, 1]$ and $\sum_{k=1}^{K} \theta_k = 1$ [29], [38],

$$\begin{aligned}
\mathbf{P0}: \quad & \max_{a_k(t), \boldsymbol{w_k}(t), \boldsymbol{z_k}(t), d_k(t)} : \lim_{T\to\infty} \frac{1}{T} \sum_{t=0}^{T-1} \sum_{k=1}^{K} \theta_k a_k(t) \\
& \text{s.t. C1:} \quad Q_k(t+1) = \Big(Q_k(t) + a_k(t) \\
& \quad - d_k(t) R_s^k(t) \Big)^+, \quad \forall k, t, \\
& \text{C2:} \quad 0 \le a_k(t) \le A_k(t), \quad \forall k, t, \\
& \text{C3:} \quad \lim_{T\to\infty} \frac{1}{T} \sum_{t=0}^{T-1} \sum_{k=1}^{K} d_k(t) \Big(||\boldsymbol{w}_k(t)||^2 \\
& \quad + ||z_k(t)||^2 \Big) \le \bar{P}, \\
& \text{C4:} \quad ||\boldsymbol{w}_k(t)||^2 + ||z_k(t)||^2 \le \hat{P}, \quad \forall t, k, \\
& \text{C5:} \quad d_k(t) \in \{0, 1\}, \quad \forall k, t, \\
& \text{C6:} \quad \sum_{k=1}^{K} d_k(t) = 1, \quad \forall t,
\end{aligned}$$

where $\bar{P}$ and $\hat{P}$ is the maximum allowed long-term average transmit power budget and the peak transmit power at the AP, respectively. C1 stands for the practical data queue evolution constraint. C2 indicates that, during each time slot, the amount of data for each user actually placed in the corresponding data buffer cannot exceed the amount of data from the upper layer applications or by the AP. C3 and C4 stands for the long-term average and peak transmit power constraint, respectively. C5 and C6 specify the user selection constraint in each time slot.

Since the feasible set of C3 is non-convex, and $d_k(t)$ is binary, the above time average optimization problem **P0** is non-convex. It is very difficult to directly solve it by using traditional convex optimization tools. In the next section, we will transform the above time average problem into a real-time optimization problem by using Lyapunov optimization framework, and then decompose it into several sub-problems to separately obtain the effective flow control, the information signal and artificial noise beamforming vector, as well as the user selection strategy.

III. Adaptive Transmission Design

A. Virtual Queue for Average Power Consumption

To incorporate our analysis into the Lyapunov optimization framework, we define $E(t)$ as the average power consumption virtual queue, and its queue evolution is given by

$$E(t+1) = \Big(E(t) + P(t) - \bar{P} \Big)^+, \quad \forall t, \tag{7}$$

where $P(t)$ is the transmit power of the AP at time t, and

$$P(t) = \sum_{k=1}^{K} d_k(t) \Big(||\boldsymbol{w}_k(t)||^2 + ||z_k(t)||^2 \Big). \tag{8}$$

It is worth noting that the virtual queue size $E(t)$ grows as the transmit power of the AP increases. This indicates that, when $E(t)$ is large enough, the AP should reduce its transmit power to fulfill the average power constraint C3.

Lemma 1: If all the data queues $Q_k(t)$, $k \in \mathcal{K}$, and the virtual queue $E(t)$ are rate stable, i.e., $\lim_{T\to\infty} \frac{Q_k(T)}{T} = \lim_{T\to\infty} \frac{E(T)}{T} = 0$, we have the following relationships

$$\lim_{T\to\infty} \frac{1}{T} \sum_{t=0}^{T-1} a_k(t) \le \lim_{T\to\infty} \frac{1}{T} \sum_{t=0}^{T-1} d_k(t) R_s^k(t), \quad \forall k \in \mathcal{K}, \tag{9}$$

$$\lim_{T\to\infty} \frac{1}{T} \sum_{t=0}^{T-1} P(t) \le \bar{P}. \tag{10}$$

Proof: See Appendix A. ∎

Lemma 1 implies that, we can transform the average power consumption constraint into a virtual queue stability problem. Moreover, from (9), one may easily observe that, all the confidential message stored in the data buffer can be safely sent out if the data queue is rate stable. Thus, the original optimization problem **P0** can be transformed into maximizing the average weighted secrecy sum-rate under the constraints of stabilizing all queues, which can be effectively solved by employing the Lyapunov optimization framework.

B. Lyapunov Optimization Framework

Based on the data queue and virtual power consumption queue states, we define the following quadratic Lyapunov function

$$L(\boldsymbol{\Theta}(t)) = \frac{1}{2} \sum_{k=1}^{K} Q_k(t)^2 + \frac{\xi}{2} E(t)^2, \quad \forall t, \tag{11}$$

where $\xi > 0$ is a weighting coefficient and $\boldsymbol{\Theta}(t) = [Q_1(t), Q_2(t), \ldots, Q_K(t), E(t)]$ represents the concatenated vector of all involved queues at the beginning of time slot t. The value of $L(\boldsymbol{\Theta}(t))$ measures the current backlog of all queues, which grows with the increase of $Q_k(t)$ and $E(t)$. The Lyapunov drift represents the expected change of Lyapunov function in two consecutive time slots, which can be expressed as

$$\Delta(\boldsymbol{\Theta}(t)) = \mathbb{E}\big[L(\boldsymbol{\Theta}(t+1)) - L(\boldsymbol{\Theta}(t)) | \boldsymbol{\Theta}(t) \big], \quad \forall t, \tag{12}$$

where the expectation is taken over the randomness of CSIs and transmission control decisions. For the given current queue state $\boldsymbol{\Theta}(t)$ in each time slot, we should minimize the Lyapunov drift to ensure the stability of all queues. Meanwhile, our objective is to maximize the achievable secrecy rate region. Thus we can follow the Lyapunov optimization framework to minimize the following Lyapunov drift-plus-penalty

$$\Delta(\boldsymbol{\Theta}(t)) - V \mathbb{E}\Big[\sum_{k=1}^{K} \theta_k a_k(t) \Big| \boldsymbol{\Theta}(t) \Big], \tag{13}$$

where $V > 0$ is a non-negative weighting coefficient. It is worth noting that the Lyapunov drift-plus-penalty is a multi-objective function, in which, the first item is to ensure all queues are stable, while the second item is the desired objective function. By minimizing the Lyapunov drift-plus-penalty, the stability of all queues and the maximum achievable secrecy rate region can be achieved at the same time [25], [26]. Moreover, we can realize a tradeoff between the queue stability and the achievable secrecy rate region by effectively controlling the parameter V.

Lemma 2: The Lyapunov drift-plus-penalty function has the following upper bound,

$$\begin{aligned}\Delta(\boldsymbol{\Theta}(t)) - V\mathbb{E}\Big[\sum_{k=1}^{K}\theta_k a_k(t)\Big|\boldsymbol{\Theta}(t)\Big] &\le B + \sum_{k\in\mathcal{K}} Q_k(t)\mathbb{E}\Big[a_k(t) - d_k(t)R_s^k(t)\big|\boldsymbol{\Theta}(t)\Big] \\ &+ \xi E(t)\mathbb{E}\Big[P(t) - \bar{P}\big|\boldsymbol{\Theta}(t)\Big] - V\mathbb{E}\Big[\sum_{k=1}^{K}\theta_k a_k(t)\Big|\boldsymbol{\Theta}(t)\Big],\end{aligned} \tag{14}$$

where $B = \frac{1}{2}\Big(\sum_{k=1}^{K}\big(\hat{A}_k^2 + \hat{R}_s^{k2}\big) + \xi\hat{P}^2 + \xi\bar{P}^2\Big)$ *is a constant independent of* V, $\hat{A}_k$ *and* $\hat{R}_s^k$ *stands for the maximal arrival rate and the maximal secrecy rate of* U_k, *respectively.*

Proof: See Appendix B. ∎

Lemma 2 provides us with an upper bound on the Lyapunov drift-plus-penalty. Based on the Lyapunov optimization framework, our transmission control decision is to minimize the above upper bound instead of directly minimizing the Lyapunov drift-plus-penalty. In each time slot t, for the given CSI and queue states $\boldsymbol{\Theta}(t)$, we will make transmission control decisions on the flow control, the information signal beamforming and artificial noise beamforming, and the user selection by solving the following optimization problem:

$$\begin{aligned}\mathbf{P1}: \quad \min_{a_k(t),\boldsymbol{w_k}(t),\boldsymbol{z_k}(t),d_k(t)} \quad &: \sum_{k=1}^{K} Q_k(t)\Big(a_k(t) - d_k(t)R_s^k(t)\Big) \\ &- V\sum_{k=1}^{K}\theta_k a_k(t) + \xi E(t)P(t) \\ \text{s.t. } &\text{C2, C4, C5, and C6.}\end{aligned}$$

One may notice that we have transformed the time average optimization problem **P0** into a real-time optimization problem **P1**. In addition, the time average power consumption constraint C3 has been transformed into the queue stability problem of $E(t)$. However, **P1** is still a non-convex optimization problem. Next, we will decompose **P1** into several sub-problems to design the effective flow control scheme, the information signal beamforming, the artificial noise beamforming, and the user selection policy, respectively.

C. Flow Control Scheme

It is worth noting that, the flow control variable $a_k(t)$ is independent of other optimization variables in **P1**, thus we can obtain the effective flow control scheme by decomposing **P1** into the following optimization sub-problem:

$$\begin{aligned}\mathbf{P2}: \quad \min_{a_k(t)} \quad &: \sum_{k=1}^{K}\big(Q_k(t) - \theta_k V\big)a_k(t) \\ \text{s.t. } &0 \le a_k(t) \le A_k(t), \quad \forall k, t.\end{aligned}$$

With the linear objective function and linear constraint conditions, **P2** is a standard linear programming problem, and the optimal solution can be obtained at the boundary only. Thus, we can derive the optimal flow control scheme in Lemma 3.

Lemma 3: The optimal flow control scheme of U_k *is given by*

$$a_k(t) = \begin{cases} A_k(t), & \text{if } Q_k(t) \le \theta_k V, \\ 0, & \text{otherwise.}\end{cases} \tag{15}$$

From Lemma 3, we may observe that the data of U_k will be placed in the data buffer only when $Q_k(t) \le \theta_k V$. Once the data queue length exceeds $\theta_k V$, the AP will stop to receive the data of U_k for the sake of data queue stability. In other words, the data queue length at AP for all K users can be effectively controlled via controlling the value of V.

D. The Design of Information Signal Beamforming and Artificial Noise Beamforming

To simplify the problem, we first assume that U_k is selected to receive the confidential message from the AP, *i.e.*, $d_k(t) = 1$ and $d_i(t) = 0$, $i \in \mathcal{K} \setminus \{k\}$. Let $\boldsymbol{H}_k(t) = \boldsymbol{h}_k^H(t)\boldsymbol{h}_k(t)$, $\boldsymbol{W}_k(t) = \boldsymbol{w}_k(t)\boldsymbol{w}_k^H(t)$, and $\boldsymbol{Z}_k(t) = z_k(t)z_k^H(t)$, then the optimal information signal beamforming and the artificial noise beamforming design problem for U_k can be equivalently transformed into the following sub-problem:

$$\begin{aligned}\mathbf{P3}: \quad \min_{\boldsymbol{W}_k(t),\boldsymbol{Z}_k(t)} \quad &: -Q_k(t)\Big(\tilde{C}_k(t) - \max_{i\in\mathcal{K}\setminus\{k\}}\tilde{C}_{e,i}(t)\Big) \\ &+ \xi E(t)\mathrm{Tr}\big(\boldsymbol{W}_k(t) + \boldsymbol{Z}_k(t)\big) \\ \text{s.t. } &\mathrm{Tr}\big(\boldsymbol{W}_k(t) + \boldsymbol{Z}_k(t)\big) \le \hat{P}, \quad \boldsymbol{W}_k(t) \succeq \boldsymbol{0}, \\ &\boldsymbol{Z}_k(t) \succeq \boldsymbol{0}, \\ &\mathrm{rank}(\boldsymbol{W}_k(t)) \le 1, \quad \mathrm{rank}(\boldsymbol{Z}_k(t)) \le 1,\end{aligned}$$

where

$$\tilde{C}_k(t) = \log_2\left(1 + \frac{\mathrm{Tr}\big(\boldsymbol{H}_k(t)\boldsymbol{W}_k(t)\big)}{1 + \mathrm{Tr}\big(\boldsymbol{H}_k(t)\boldsymbol{Z}_k(t)\big)}\right), \tag{16}$$

$$\tilde{C}_{e,i}(t) = \log_2\left(1 + \frac{\mathrm{Tr}\big(\boldsymbol{H}_i(t)\boldsymbol{W}_k(t)\big)}{1 + \mathrm{Tr}\big(\boldsymbol{H}_i(t)\boldsymbol{Z}_k(t)\big)}\right), \quad \forall i \ne k. \tag{17}$$

It should be addressed that, the non-negative operation of $R_s^k(t)$ has been ignored in the objective function of **P3**. This can be interpreted as follows: (i) We jointly consider the information signal and artificial noise beamforming design for **P3**, and the objective function value of **P3** is zero when $\boldsymbol{W}_k(t) = \boldsymbol{Z}_k(t) = \boldsymbol{0}$; (ii) If the secrecy rate of U_k is negative, the objective function value of **P3** is larger than zero; (iii) Since our goal is to minimize the objective function value of **P3** by jointly optimizing $\boldsymbol{W}_k(t)$ and $\boldsymbol{Z}_k(t)$, the optimal value of $\tilde{C}_k(t) - \max_{i\in\mathcal{K}\setminus\{k\}}\tilde{C}_{e,i}(t)$ must be non-negative. One may readily observe that, unlike the conventional beamforming

design problem, now both the information signal beamforming and the artificial noise beamforming design not only depend on current CSIs, but also rely on the current data queue and the virtual power consumption queue state.

From the objective function of **P3**, we can observe that the data queue size $Q_k(t)$ can be regarded as the weighting coefficient of the secrecy rate of U_k, and $\xi E(t)$ can be treated as the weighting coefficient of the power consumption of U_k. When $Q_k(t)$ is large enough, the term $-Q_k(t)\Big(\tilde{C}_k(t) - \max_{i\in\mathcal{K}\setminus\{k\}} \tilde{C}_{e,i}(t)\Big)$ dominates the value of the objective function. In this case, the system may expect to achieve a higher secrecy rate of U_k, and the AP will tend to allocate more power to generate the information beamforming and artificial noise beamforming. On the other hand, if $\xi E(t)$ is large enough, the term $\xi E(t)\mathrm{Tr}\big(\boldsymbol{W}_k(t)+\boldsymbol{Z}_k(t)\big)$ plays a decisive role in the value of the objective function. In this case, the AP tends to allocate less power to generate the information beamforming and the artificial noise beamforming.

In addition, we may notice that **P3** is still non-convex. To make problem easier to handle, we introduce the following slack variable α to simplify the maximum function of the objective function

$$\alpha = \max_{i\in\mathcal{K}\setminus\{k\}} \frac{1+\mathrm{Tr}\big(\boldsymbol{H}_i(t)(\boldsymbol{W}_k(t)+\boldsymbol{Z}_k(t))\big)}{1+\mathrm{Tr}\big(\boldsymbol{H}_i(t)\boldsymbol{Z}_k(t)\big)}. \tag{18}$$

By further relaxing the constraints of $\mathrm{rank}(\boldsymbol{W}_k(t)) \le 1$ and $\mathrm{rank}(\boldsymbol{Z}_k(t)) \le 1$, **P3** can be rewritten as **P3_1**:

$$\begin{aligned}\textbf{P3\_1}: \quad \min_{\boldsymbol{W}_k,\boldsymbol{Z}_k,\alpha\ge 1} \quad & : Q_k(t)\Big(\log_2\alpha - \tilde{C}_k(t)\Big) \\ & \quad + \xi E(t)\mathrm{Tr}\big(\boldsymbol{W}_k(t)+\boldsymbol{Z}_k(t)\big) \\ \text{s.t. } & \mathrm{Tr}\big(\boldsymbol{H}_i(t)\boldsymbol{W}_k(t)\big) \le (\alpha-1) \\ & \quad \Big(1+\mathrm{Tr}\big(\boldsymbol{H}_i(t)\boldsymbol{Z}_k(t)\big)\Big), \quad \forall i\ne k, \qquad (19a) \\ & \mathrm{Tr}\big(\boldsymbol{W}_k(t)+\boldsymbol{Z}_k(t)\big) \le \hat{P}, \quad \boldsymbol{W}_k(t)\succeq\boldsymbol{0}, \\ & \boldsymbol{Z}_k(t)\succeq\boldsymbol{0}. \qquad (19b)\end{aligned}$$

Next, we will show that **P3_1** can be further decomposed into a two-stage optimization problem, and the external problem is a single-variable optimization problem on α, which can be solved by using an appropriate line search method. To reduce the complexity of the line search, we need to find an appropriate search interval for α. We can obtain an upper bound of α, which is given by

$$\begin{aligned}\alpha &\overset{(a)}{\le} = 1+\frac{\mathrm{Tr}\big(\boldsymbol{H}_k(t)\boldsymbol{W}_k(t)\big)}{1+\mathrm{Tr}\big(\boldsymbol{H}_k(t)\boldsymbol{Z}_k(t)\big)} \\ &\overset{(b)}{\le} 1+\mathrm{Tr}\big(\boldsymbol{H}_k(t)\boldsymbol{W}_k(t)\big) \overset{(c)}{\le} 1+\hat{P}\mathrm{Tr}\big(\boldsymbol{H}_k(t)\big), \end{aligned} \tag{20}$$

where step (a) follows from the fact that the secrecy rate is non-negative; step (b) follows the fact that $\mathrm{Tr}\big(\boldsymbol{H}_k(t)\boldsymbol{Z}_k(t)\big) \ge 0$; step (c) follows the fact that $\mathrm{Tr}\big(\boldsymbol{H}_k(t)\boldsymbol{W}_k(t)\big) \le \mathrm{Tr}\big(\boldsymbol{H}_k(t)\big)\mathrm{Tr}\big(\boldsymbol{W}_k(t)\big)$ for any $\boldsymbol{W}_k(t)\succeq\boldsymbol{0}$ and $\mathrm{Tr}\big(\boldsymbol{W}_k(t)\big) \le \hat{P}$. Then we can rewrite the problem **P3_1** as below

$$\begin{aligned}\textbf{P3\_2}: \quad \min_{\alpha} \quad & : \varphi(\alpha) + Q_k(t)\log_2\alpha \\ \text{s.t. } & 1 \le \alpha \le 1+\hat{P}\mathrm{Tr}\big(\boldsymbol{H}_k(t)\big),\end{aligned}$$

where

$$\begin{aligned}\textbf{P3\_3}: \quad \varphi(\alpha) = \min_{\boldsymbol{W}_k,\boldsymbol{Z}_k,} \quad & : -Q_k(t)\tilde{C}_k(t) + \xi E(t) \\ & \quad \mathrm{Tr}\big(\boldsymbol{W}_k(t)+\boldsymbol{Z}_k(t)\big) \\ \text{s.t. } & (19).\end{aligned}$$

Now, we have split **P3_1** into the two-stage optimization problem, namely the external problem **P3_2** and the internal problem **P3_3**. Although the function $\varphi(\alpha)$ does not have a closed-form expression, it is numerically tractable. We may notice that **P3_3** still remains non-convex due to the fact that, $\tilde{C}_k(t)$ is a non-concave function of the optimization variables $(\boldsymbol{W}_k(t), \boldsymbol{Z}_k(t))$. However, $\tilde{C}_k(t)$ can be rewritten in the form of the difference of two concave functions, namely,

$$\begin{aligned}\tilde{C}_k(t) = \log_2\Big(1+\mathrm{Tr}\big(\boldsymbol{H}_k(t)(\boldsymbol{W}_k(t)+\boldsymbol{Z}_k(t))\big)\Big) \\ - \log_2\Big(1+\mathrm{Tr}\big(\boldsymbol{H}_k(t)\boldsymbol{Z}_k(t)\big)\Big). \end{aligned} \tag{21}$$

Therefore, **P3_3** can be effectively solved by using the DC programming algorithm. Since $\log_2\Big(1+\mathrm{Tr}\big(\boldsymbol{H}_k(t)\boldsymbol{Z}_k(t)\big)\Big)$ is concave function, on the basis of Taylor series expansion, for any $\boldsymbol{Z}_k^{(l)}(t)\succeq\boldsymbol{0}$, we have

$$\begin{aligned}&\log_2\Big(1+\mathrm{Tr}\big(\boldsymbol{H}_k(t)\boldsymbol{Z}_k(t)\big)\Big) \\ &\le \log_2\Big(1+\mathrm{Tr}\big(\boldsymbol{H}_k(t)\boldsymbol{Z}_k^{(l)}(t)\big)\Big) \\ &\quad + \frac{\mathrm{Tr}\Big(\boldsymbol{H}_k(t)\big(\boldsymbol{Z}_k(t)-\boldsymbol{Z}_k^{(l)}(t)\big)\Big)}{\Big(1+\mathrm{Tr}\big(\boldsymbol{H}_k(t)\boldsymbol{Z}_k^{(l)}(t)\big)\Big)\ln 2} \\ &\triangleq F\Big(\boldsymbol{Z}_k(t), \boldsymbol{Z}_k^{(l)}(t)\Big). \end{aligned} \tag{22}$$

Based on the above approximation, we can formulate the approximation problem of **P3_4** at iteration $l+1$ as follows

$$\begin{aligned}\textbf{P3\_4}: \quad \min_{\boldsymbol{W}_k,\boldsymbol{Z}_k,} \quad & : -Q_k(t)\log_2\Big(1+\mathrm{Tr}\big(\boldsymbol{H}_k(t)(\boldsymbol{W}_k(t) \\ & \quad + \boldsymbol{Z}_k(t))\big)\Big) + Q_k(t)F\Big(\boldsymbol{Z}_k(t), \boldsymbol{Z}_k^{(l)}(t)\Big) \\ & \quad + \xi E(t)\mathrm{Tr}\big(\boldsymbol{W}_k(t)+\boldsymbol{Z}_k(t)\big) \\ \text{s.t. } & (19).\end{aligned}$$

We can observe that, for the given α, all the constraint functions of (19) are linear, and the objective function is convex. Thus the optimization problem **P3_4** can be effectively solved by using the convex optimization softwares, for instance, *CVX*. The proposed algorithm for deriving $\varphi(\alpha)$ (**P3_3**) is an iterative process that solves the sequence of convex programming (**P3_4**) until convergence, which is outlined in Algorithm 1.[1]

1) Convergence Analysis of Algorithm 1: We can prove that Algorithm 1 guarantees convergence. This can be established by proving that the proposed iterative scheme monotonically reduces the objective function value of **P3_3** in each iteration. To simplify the description, let $U\big(\boldsymbol{Z}_k(t)\big)$ and $V\big(\boldsymbol{Z}_k(t), \boldsymbol{Z}_k^{(l)}(t)\big)$ denote the objective function of the problem

[1]Here we drop time index t for brevity.

Algorithm 1 Compute $\varphi(\alpha)$

Input: H_k, Q_k, E, α, ξ, $\hat{P}$, and tolerated-error ε;

1: Initialize $l = 0$ and $\boldsymbol{Z}_k^{(0)} = \mathbf{0}$;

2: **repeat**

3: Set $\left(\boldsymbol{W}_k^{(l+1)}, \boldsymbol{Z}_k^{(l+1)}\right) = \arg\min_{\boldsymbol{W}_k, \boldsymbol{Z}_k}: \; Q_k F\left(\boldsymbol{Z}_k, \boldsymbol{Z}_k^{(l)}\right) + \xi E\left(\mathrm{Tr}(\boldsymbol{W}_k + \boldsymbol{Z}_k) - Q_k \log_2\left(1 + \mathrm{Tr}\left(\boldsymbol{H}_k(\boldsymbol{W}_k + \boldsymbol{Z}_k)\right)\right)\right)$ s.t. (19).

4: Set $l = l + 1$;

5: **until** $||\boldsymbol{Z}_k^{(l)} - \boldsymbol{Z}_k^{(l-1)}||_F \leq \varepsilon$;

6: Set $\varphi(\alpha) = \xi E \mathrm{Tr}\left(\boldsymbol{W}_k^{(l)} + \boldsymbol{Z}_k^{(l)}\right) - Q_k \log_2\left(1 + \frac{\mathrm{Tr}\left(\boldsymbol{H}_k \boldsymbol{W}_k^{(l)}\right)}{1 + \mathrm{Tr}\left(\boldsymbol{H}_k \boldsymbol{Z}_k^{(l)}\right)}\right)$;

Output: $\varphi(\alpha)$;

P3_3 and **P3_4**, respectively. Based on Algorithm 1, we have

$$U\left(\boldsymbol{Z}_k^{(l+1)}(t)\right) \overset{(a)}{\leq} V\left(\boldsymbol{Z}_k^{(l+1)}(t), \boldsymbol{Z}_k^{(l)}(t)\right) \overset{(b)}{\leq} V\left(\boldsymbol{Z}_k^{(l)}(t), \boldsymbol{Z}_k^{(l)}(t)\right) \overset{(c)}{\leq} U\left(\boldsymbol{Z}_k^{(l)}(t)\right), \quad (23)$$

where step (a) follows the fact that $V\left(\boldsymbol{Z}_k(t), \boldsymbol{Z}_k^{(l)}(t)\right)$ is the upper bound of $U\left(\boldsymbol{Z}_k(t)\right)$; step (b) follows the fact that $\boldsymbol{Z}_k^{(l+1)}(t)$ is the optimal solution of **P3_4** at iteration $l + 1$; step (c) uses the fact that $F\left(\boldsymbol{Z}_k^{(l)}(t), \boldsymbol{Z}_k^{(l)}(t)\right) = \log_2\left(1 + \mathrm{Tr}\left(\boldsymbol{H}_k(t)\boldsymbol{Z}_k^{(l)}(t)\right)\right)$. Due toe the peak power constraint, the objective function of **P3_3** has a lower bound, Algorithm 1 is convergent.

For any fixed α, since Algorithm 1 provides us with an effective approach to calculate $\varphi(\alpha)$, and α has the lower and upper bound, the single-variable optimization problem **P3_2** can be effectively solved by using the appropriate one-dimensional line search algorithm over α. In this paper, the golden Section search is used to obtain α^*, and the detailed process is outlined in Algorithm 2.

Algorithm 2 Calculate α^*

Input: $\varphi(\alpha)$, $\hat{P}$, $\boldsymbol{H}_k(t)$, and tolerance error ϵ_e;

1: Initialization: $a = 1$, $b = 1 + \hat{P}\mathrm{Tr}\left(\boldsymbol{H_k}(t)\right)$, $\alpha_1 = a + 0.382(b - a)$,$\alpha_2 = a + 0.618(b - a)$;

2: **while** $\alpha_2 - \alpha_1 > \epsilon_e$ **do**

3: **if** $\varphi(\alpha_2) > \varphi(\alpha_1)$ **then**

4: $b = \alpha_2$, $\alpha_2 = \alpha_1$, and $\alpha_1 = a + 0.382(b - a)$;

5: **else**

6: $a = \alpha_1$, $\alpha_1 = \alpha_2$, and $\alpha_2 = a + 0.618(b - a)$;

7: **end if**

8: **end while**

9: Set $\alpha^* = \frac{\alpha_1 + \alpha_2}{2}$;

Output: α^*;

Once **P3_2** is solved, we can obtain the corresponding solution $\left(\boldsymbol{W}_k^*(t), \boldsymbol{Z}_k^*(t)\right)$, which will be used to recover the information signal and artificial noise beamformig vector $(\boldsymbol{w}_k^*(t), \boldsymbol{z}_k^*(t))$ according to the following Algorithm 3.

2) Complexity Analysis: The computational complexity of the information signal and artificial noise beamforming design comes mainly from the golden Section search for deriving α^* and the DC algorithm for solving **P3_3**. For the golden section search, the search space is reduced by 38.2% after each iteration. Thus, for the given accuracy ϵ_e, the number of iteration $N_g^{\max}$ satisfies $\hat{P}\mathrm{Tr}\left(\boldsymbol{H}_k(t)\right)0.618^{N_g^{\max}} \leq \epsilon_e$, *i.e.*, $N_g^{\max} \geq 2.0778 \log\left(\frac{\hat{P}\mathrm{Tr}(\boldsymbol{H}_k(t))}{\epsilon_e}\right)$, hence the computation complexity is in the order of $O(\log(\frac{1}{\epsilon_e}))$. In addition, since the optimization problem **P3_3** is not a standard convex problem, by using the DC algorithm, **P3_3** is transformed to solve the sequences of convex problem (**P3_4**). Since **P3_4** has $\frac{N(N+1)}{2}$ independent real parts and $\frac{N(N-1)}{2}$ independent imaginary parts in the Hermitian matrix $\boldsymbol{W}_k(t)$ and $\boldsymbol{Z}_k(t)$, respectively, there are $2N^2$ independent variables in **P3_4**. Thus, when the interior point algorithm is used to solve the convex problem **P3_4**, the computation complexity is $O(N^7)$ [40]. On the other hand, since we have proven that Algorithm 1 is convergent for solving **P3_3**, it must converge within a finite number of iterations. Therefore, the total computation complexity of deriving the information signal and artificial noise beamforming vector is $O(N_{dc}^{\max} N^7 \log(\frac{1}{\epsilon_e}))$, where $N_{dc}^{\max}$ is the maximum iteration number in solving **P3_3**.

Algorithm 3 Calculate $\boldsymbol{w}_k^*(t)$ and $\boldsymbol{z}_k^*(t)$

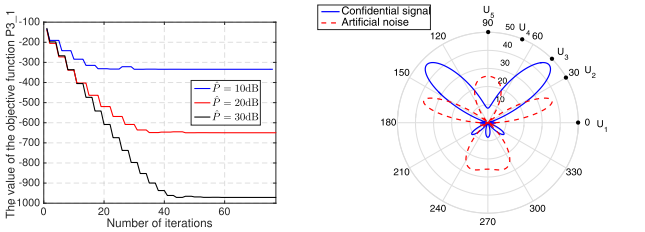
Input: $\boldsymbol{W}_k^*(t)$ and $\boldsymbol{Z}_k^*(t)$;

1: Calculate the eigen-decomposition of $\boldsymbol{W}_k^*(t)$ and $\boldsymbol{Z}_k^*(t)$;

2: Find the maximum eigenvalues (λ_w, λ_z) and the corresponding eigenvectors $(\boldsymbol{q}_w, \boldsymbol{q}_z)$ of $\boldsymbol{W}_k^*(t)$ and $\boldsymbol{Z}_k^*(t)$;

3: Set $\boldsymbol{w}_k^*(t) = \sqrt{\lambda_w}\boldsymbol{q}_w$ and $\boldsymbol{z}_k^*(t) = \sqrt{\lambda_z}\boldsymbol{q}_z$;

Output: $\boldsymbol{w}_k^*(t)$ and $\boldsymbol{z}_k^*(t)$



(a) (b)

Fig. 2. (a). The convergence of iterative process for the proposed information signal and artificial noise beamforming design, and (b). the antenna radiation patterns of the uniform linear.

*Proposition 1: For the optimization problem **P3_1**, the covariance matrix of the confidential message by using Algorithm 1 is rank-one, i.e., rank$(\boldsymbol{W}_k(t)) = 1$.*

Proof: See Appendix C. ■

Proposition 1 indicates that, the proposed information signal beamforming and the artificial noise beamforming design algorithm can guarantee the information signal covariance matrix $\boldsymbol{W}_k^*(t)$ with rank-one. In Fig. 2, we illustrate the proposed information signal and the artificial noise beamforming design. In Fig. 2, a uniform linear array is assumed and the AP is provisioned with $N = 4$ antennas. The channel coefficient vector is molded as $h_k = [1 \; e^{j\vartheta} \; e^{j2\vartheta} \ldots \; e^{j(N-1)\vartheta}]$ and $\vartheta = -\frac{2\pi d \sin(\omega_k)}{\lambda}$, where λ is the wavelength of transmitted signal, d

is the distance between successive antenna elements, and ω_k is the direction of U_k to the AP. We assume that there are $K = 5$ users distributed around the AP, in which U_3 is a scheduled user and the others are potential eavesdroppers in the current time slot. We set $d = \frac{\lambda}{2}$ and $\omega_k = \{0^o, 30^o, 45^o, 67.5^o, 90^o\}$. In Fig. 2(a), we illustrate the convergence of the iterative procedure of the proposed information signal and artificial noise beamforming design. We can observe that the iterative process converges within a limited number of iterations with different peak transmit power constraint. In Fig. 2(b), we illustrate the relationship between the information signal beamforming, the artificial noise beamforming, and the users' placement according to the proposed beamforming design. As shown in Fig. 2(b), one can observe that, the information signal beams mainly direct to the scheduled user U_3. At the same time, the artificial noise beams primarily align to those potential eavesdroppers, which verifies the effectiveness of the proposed beamforming algorithm.

E. User Selection Scheme

Since the optimization variable $d_k(t)$ is binary, and at most one user can be selected to receive the confidential message from the AP in each time slot, we can enumerate K different cases to obtain the corresponding objective function value of **P3**. When we obtain the information signal and artificial noise beamforming vector, by substituting them into the objective function of **P3**, we can get the following user selection scheme.

Lemma 4: The user selection scheme is given by

$$d_k(t) = \begin{cases} 1, & \text{if } k = \arg\min_{i\in\mathcal{K}} \Lambda_i(t), \\ 0, & \text{otherwise}, \end{cases} \tag{24}$$

where $\Lambda_k(t)$ is a user selection metric, which is given by

$$\Lambda_k(t) = -Q_k(t)\Big(\tilde{C}_k(t) - \max_{i\in\mathcal{K}\setminus\{k\}} \tilde{C}_{e,i}(t)\Big) + \xi E(t) Tr\big(\boldsymbol{W}_k(t) + \boldsymbol{Z}_k(t)\big)\Big|_{\boldsymbol{Z}_k(t)=\boldsymbol{Z}_k^*(t)}^{\boldsymbol{W}_k(t)=\boldsymbol{W}_k^*(t)}. \tag{25}$$

If two users or more users happen to have the same user selection metric, uniform tie-braking can be used.

From the user selection metric, we may notice that, the proposed user selection scheme is not only related to the secrecy rate of each user, but also depends on the corresponding data queue. The data queue size $Q_k(t)$ can be regarded as weight of the secrecy rate of U_k. If one user has a larger data backlog at the AP, the AP prefers to selecting this user to receive the confidential message, just as expected.

F. Performance Analysis

In this subsection, we analyze the upper bound of data queue size and the average secrecy rate region achieved by the proposed transmission scheme.

Theorem 1: When the proposed scheme is used, for any $V \geq 0$, there exist $\epsilon > 0$ and $\Psi(\epsilon)$, $\Psi(\epsilon)$ is less than the optimal average weighted secrecy sum rate R_{sum}^*, such that it can achieve the following features:

(1). *All the data queues $Q_k(t)$, $k = 1, 2, \cdots, K$, and the virtual power consumption queue $E(t)$ are rate stable, such that (9) and (10) can be satisfied.*

(2). *The average data queue size and the average weighted secrecy sum rate fulfill the following constraints:*

$$\lim_{T\to\infty} \frac{1}{T} \sum_{t=0}^{T-1} \sum_{k=1}^{K} \mathbb{E}\big[Q_k(t)\big] \leq \frac{B + V\big(R_{sum}^* - \Psi(\epsilon)\big)}{\epsilon}, \tag{26}$$

$$R_{sum}^* - \frac{B}{V} \leq \lim_{T\to\infty} \frac{1}{T} \sum_{t=0}^{T-1} \sum_{k=1}^{K} \theta_k \mathbb{E}\big[a_k(t)\big] \leq R_{sum}^*. \tag{27}$$

Proof: See Appendix D. ∎

One may easily observe from Theorem 1 that, the proposed transmission scheme can guarantee all the data queues and virtual power consumption queues are rate stable. Combined with Lemma 1, we may see that all the confidential message stored in the data buffer can be sent out and the average power consumption of the AP can be ensured, *i.e.*, constraint C3 can be satisfied. Moreover, the data queue size increases linearly with V, and the gap between R_{sum}^* and the average secrecy sum rate achieved by the proposed transmission scheme is inversely proportional to V. According to the Little's law, the average queueing delay is proportional to the average data queue size, which means that the proposed transmission scheme can arbitrarily approach R_{sum}^* at the cost of a larger average queueing delay. Thus, we can obtain $[O(V), O(1/V)]$ tradeoff between the average queueing delay and the achieved average secrecy rate region.

IV. Adaptive Transmission Design of Colluding Eavesdroppers

In this section, we consider the worst-case scenario, in which all unintended users are assumed to collude in eavesdropping. In this case, all unintended users can be approximately considered as a single eavesdropper equipped with $K - 1$ antennas. Namely, the system model can be regarded as a wiretap channel model with a multiple-antenna transmitter (AP), a single-antenna legitimate user, and a multiple-antenna eavesdropper. Since the beamforming scheme without artificial noise has been shown to be optimal in terms of maximizing the secrecy rate of wiretap channel [3], [4], we only consider the information signal beamforming design in this section. Thus, for the given scheduled user U_k, the received signals of U_k and $K - 1$ colluding eavesdroppers can be given by

$$y_k(t) = \boldsymbol{h}_k(t)\boldsymbol{x}_k(t) + n_k(t), \tag{28}$$

$$\boldsymbol{y}_{e,k}(t) = \boldsymbol{G}_{e,k}(t)\boldsymbol{x}_k(t) + \boldsymbol{n}_{e,k}(t), \tag{29}$$

where $\boldsymbol{x}_k(t) = \boldsymbol{w}_k(t)s_k(t)$ is the transmit signal by the AP, $\boldsymbol{G}_{e,k}(t) = \big(\boldsymbol{h}_1^T(t), \ldots, \boldsymbol{h}_{k-1}^T(t), \boldsymbol{h}_{k+1}^T(t) \ldots, \boldsymbol{h}_K^T(t)\big)^T \in \mathbb{C}^{(K-1)\times N}$ is the channel gain matrix between the $K - 1$ colluding eavesdroppers and the AP, and $\boldsymbol{n}_{e,k} \sim \mathcal{CN}(\boldsymbol{0}, \boldsymbol{I}) \in \mathbb{C}^{(K-1)\times 1}$ denotes the additive white Gaussian noise at $K - 1$ colluding eavesdroppers. Therefore, the maximum achievable secrecy rate of U_k is given by

$$R_s^k(t) = (\hat{C}_k(t) - \hat{C}_{e,k}(t))^+, \tag{30}$$

where

$$\hat{C}_k(t) = \log_2\Big(1 + \mathrm{Tr}\big(\boldsymbol{H}_k(t)\boldsymbol{W}_k(t)\big)\Big), \tag{31}$$

$$\hat{C}_{e,k}(t) = \log_2 \det\Big(\boldsymbol{I} + \boldsymbol{G}_{e,k}(t)\boldsymbol{W}_k(t)\boldsymbol{G}_{e,k}^H(t)\Big), \tag{32}$$

where $\boldsymbol{H}_k(t) = \boldsymbol{h}_k^H(t)\boldsymbol{h}_k(t)$ and $\boldsymbol{W}_k(t) = \boldsymbol{w}_k(t)\boldsymbol{w}_k^H(t)$.

Even in the presence of colluding eavesdroppers, the flow control and user selection schemes for maximizing the achievable secrecy rate are the same as those without colluding eavesdroppers in Section III. The only difference lies in the information signal beamforming design. Similar to the problem **P3**, if U_k is scheduled to receive confidential messages from the AP, the information signal beamforming design in the case of colluding eavesdroppers can be simplified as

$$\begin{aligned}\mathbf{P4}: \quad \min_{\boldsymbol{W}_k} \ & : \xi E(t)\mathrm{Tr}\big(\boldsymbol{W}_k(t)\big) - Q_k(t)\Big(\hat{C}_k(t) - \hat{C}_{e,k}(t)\Big) \\ \text{s.t. } & \mathrm{Tr}\big(\boldsymbol{W}_k(t)\big) \le \hat{P}, \quad \boldsymbol{W}_k(t) \succeq \boldsymbol{0}, \ \mathrm{rank}(\boldsymbol{W}_k(t)) \le 1.\end{aligned}$$

To handle the optimization problem **P4**, we introduce a slack variable β to simplify the objective function and relax the constraint of $\mathrm{rank}(\boldsymbol{W}_k(t))) \le 1$, thus **P4** can be rewritten as

$$\begin{aligned}\mathbf{P4\_1}: \quad \min_{\boldsymbol{W}_k,\beta} \ & : \xi E(t)\mathrm{Tr}\big(\boldsymbol{W}_k(t)\big) - Q_k(t)\Big(\hat{C}_k(t) - \log_2\beta\Big) \\ \text{s.t. } & \log_2 \det\Big(\boldsymbol{I} + \boldsymbol{G}_{e,k}(t)\boldsymbol{W}_k(t)\boldsymbol{G}_{e,k}^H(t)\Big) \le \log_2\beta, \\ & \beta \ge 1, \quad \mathrm{Tr}\big(\boldsymbol{W}_k(t)\big) \le \hat{P}, \ \boldsymbol{W}_k(t) \succeq \boldsymbol{0},\end{aligned} \tag{33}$$

where $\log_2\beta$ can be considered as the maximum allowed mutual information of colluding eavesdroppers' link. However, since the constraint (33) is non-convex, the above optimization problem is still difficult to solve. Fortunately, by applying the existing result, we can replace constraint (33) with an easy-to-handle inequality. Based on Lemma 1 in [17], we can derive the following inequality from the constraint (33)

$$\mathrm{Tr}\Big(\boldsymbol{G}_{e,k}(t)\boldsymbol{W}_k(t)\boldsymbol{G}_{e,k}^H(t)\Big) \le \beta - 1. \tag{34}$$

In particular, the constraint (33) and (34) are equivalent when $\mathrm{rank}(\boldsymbol{W}_k(t)) \le 1$. In addition, we can see that (34) is a linear matrix inequality with respect to $\boldsymbol{W}_k(t)$. Now the objective functions of **P4_1** is convex for any given β, Thus, if we use (34) instead of (33) and fix the value of β, the optimization problem **P4_1** can be transformed into a convex one, which can be effectively solved by using *CVX* optimization software. By employing the similar beamforming design for the non-colluding eavesdroppers in Section III, we can decompose **P4_1** into a two-stage optimization problem, the external problem is to search the optimal β by using exact line search methods, and the internal problem is to obtain the opitmal information signal beamforming covariance matrix $\boldsymbol{W}_k(t)$ by solving the convex problem. The detailed algorithm for obtaining $\boldsymbol{w}_k^*(t)$ is similar to the beamforming algorithm in Section III, and we omit it here to save space.

V. Numerical Results

In this section, we evaluate the performance of the proposed adaptive transmission scheme (ATS) in both non-colluding eavesdropper and colluding eavesdropper scenarios. Moreover, we compare the performance of the proposed scheme with two benchmark schemes, namely the buffer-aided ZF-based information signal beamforming scheme and the existing work without buffering in [4]. Unless otherwise stated, we assume that the arrival rate of each user $A_k(t)$, $k = 1, 2, \cdots, K$ follows the same Poisson process with mean 10 bits/slot. The peak transmit power of the AP $\hat{P} = 3\bar{P}$. All the simulation results are obtained for $T = 10^4$ time slots.

A. Benchmark Schemes

1) ZF Based Information Signal Beamforming Scheme: To evaluate the performance of the proposed information signal and artificial noise beamforming design, we use the zero-forcing based information signal beamforming in the buffer-aided MISO network as our first benchmark scheme (for brevity, we refer it to as buffer-aided ZF). In this case, the flow control and user selection schemes for maximizing the achievable secrecy rate are the same as the proposed adaptive transmission scheme in Section III. The only difference is the information signal beamforming design problem. Since the AP knows perfect CSIs of all users, it can align the transmitted information signal within the null space of unintended users ($N \ge K$ is assumed here), such that all unintended users can not receive any useful information. Therefore, in this case, the secrecy rates of non-colluding eavesdropper and colluding eavesdropper are the same. If U_k is scheduled in time slot t, the singular-value decomposition of the channel matrix of the $K-1$ unscheduled users $\boldsymbol{G}_{e,k}(t)$ is given by

$$\boldsymbol{G}_{e,k}(t) = \boldsymbol{U}_{e,k}(t)\boldsymbol{\Sigma}_{e,k}(t)\boldsymbol{V}_{e,k}^H(t), \tag{35}$$

where $\boldsymbol{U}_{e,k}(t) \in \mathbb{C}^{(K-1)\times(K-1)}$ and $\boldsymbol{V}_{e,k}(t) \in \mathbb{C}^{N\times N}$ are unitary matrices, and $\boldsymbol{\Sigma}_{e,k}(t) \in \mathbb{C}^{(K-1)\times N}$ is a diagonal matrix. When $N > K-1$, the last $N-K+1$ columns of $\boldsymbol{V}_{e,k}(t)$ span the null space of $\boldsymbol{G}_{e,k}(t)$. Thus, in this case, the information signal beamforming vector can be defined as

$$\boldsymbol{w}_k(t) = \frac{\sqrt{P(t)}\widetilde{\boldsymbol{V}}_{e,k}(t)\boldsymbol{c}_{e,k}(t)}{||\boldsymbol{c}_{e,k}(t)||}, \tag{36}$$

where $\widetilde{\boldsymbol{V}}_{e,k}(t) \in \mathbb{C}^{N\times(N-K+1)}$ is a matrix consisting of the last $N-K+1$ columns of $\boldsymbol{V}_{e,k}(t)$ and $\boldsymbol{c}_{e,k}(t) \in \mathbb{C}^{(N-K+1)\times 1}$ is the coefficient vector corresponding to each column of $\widetilde{\boldsymbol{V}}_{e,k}(t)$. In addition, to improve the secrecy rate, the selected coefficient vector $\boldsymbol{c}_{e,k}^*(t)$ should make the transmitted information signal direct to the scheduled user U_k as much as possible, *i.e.*,

$$\boldsymbol{c}_{e,k}^*(t) = \arg\min_{\boldsymbol{c}_{e,k}(t)} ||\widetilde{\boldsymbol{V}}_{e,k}(t)\boldsymbol{c}_{e,k}(t) - \boldsymbol{h}_k^H(t)||^2. \tag{37}$$

By using least squares method to solve the above optimization problem, the optimal coefficient vector $\boldsymbol{c}_{e,k}^*(t)$ is given by

$$c_{e,k}^*(t) = \big(\widetilde{\boldsymbol{V}}_{e,k}^H(t)\widetilde{\boldsymbol{V}}_{e,k}(t)\big)^{-1}\widetilde{\boldsymbol{V}}_{e,k}^H(t)\boldsymbol{h}_k^H(t) = \widetilde{\boldsymbol{V}}_{e,k}^H(t)\boldsymbol{h}_k^H(t).$$

Thus, the ZF based information signal beamforming vector is

$$\boldsymbol{w}_k(t) = \frac{\sqrt{P(t)}\widetilde{\boldsymbol{V}}_{e,k}(t)\widetilde{\boldsymbol{V}}_{e,k}^H(t)\boldsymbol{h}_k^H(t)}{||\widetilde{\boldsymbol{V}}_{e,k}^H(t)\boldsymbol{h}_k^H(t)||}. \tag{38}$$

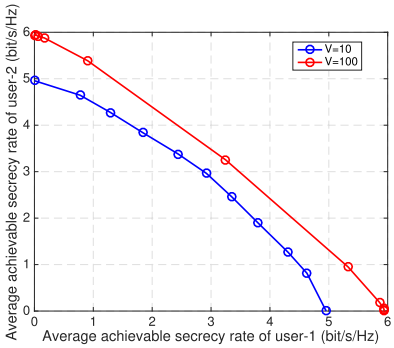
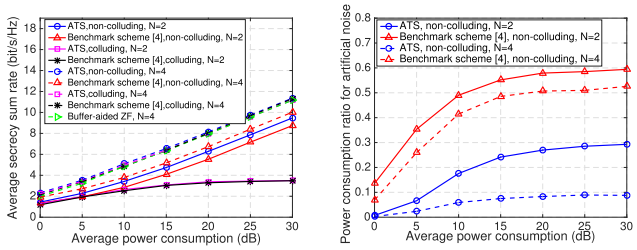


Fig. 3. Capacity region with different choice of V when $N = K = 2$, and $\bar{P} = 20$ dB.



(a) (b)

Fig. 4. (a). Average achievable secrecy sum rate v.s. average power consumption, and (b).optimal power portion for artificial noise v.s. average power consumption, $K = 3$.

Furthermore, since the unintended users can not receive any user information, the achievable secrecy rate of U_k is

$$R_k(t) = d_k(t) \log_2 \left(1 + P(t)|\boldsymbol{h}_k(t)\boldsymbol{w}_k(t)|^2\right). \tag{39}$$

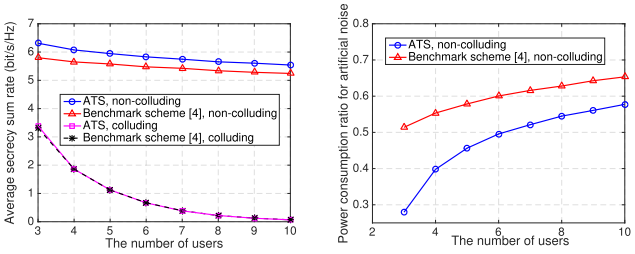
Thus, similar to the problem **P3**, when U_k is scheduled to receive the confidential message, the power allocation problem in this case can be formulated as

$$\min_{P(t)} \ : -Q_k(t) \log_2 \left(1 + P(t)|\boldsymbol{h}_k(t)\boldsymbol{w}_k(t)|^2\right) + \xi E(t) P(t)$$
$$\text{s.t. } 0 \le P(t) \le \hat{P}.$$

Since the objective function is convex and the constraint is linear, the above optimization problem is convex. By using Karush-Kuhn-Tucker (KKT) conditions, we can obtain the optimal power allocation scheme as follows

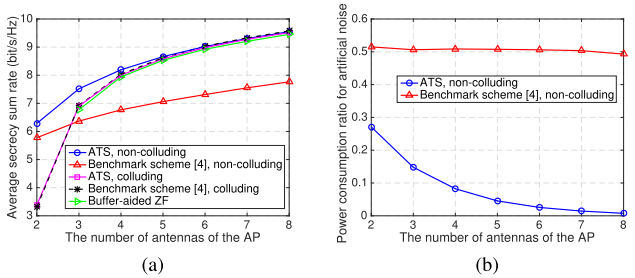
$$P^*(t) = \min \left\{ \left(\frac{Q_k(t)}{\xi E(t) \ln 2} - \frac{1}{|\boldsymbol{h}_k(t)\boldsymbol{w}_k(t)|^2} \right)^+, \hat{P} \right\}. \tag{40}$$

2) MRT Based Information Signal Beamforming and ZF Based Artificial Noise Beamforming: We consider the scheme proposed in [4] as the second benchmark scheme. For the non-colluding eavesdropping, the MRT and ZF schemes are used to generate information signal and artificial noise beamforming, respectively. In the colluding case, the information signal beamforming vector corresponds to the eigenvector of the largest eigenvalue of matrix $(\boldsymbol{I} + \hat{P}\boldsymbol{G}_{e,k}^H \boldsymbol{G}_{e,k})^{-1}(\boldsymbol{I} + \hat{P}\boldsymbol{h}_k^H(t)\boldsymbol{h}_k(t))$. In each time slot, the user with the largest secrecy rate is selected to receive the confidential message.



(a) (b)

Fig. 5. (a). Average achievable secrecy sum rate v.s. the number of users, and (b). optimal power portion for artificial noise v.s. the number of users, $N = 2$ and $\bar{P} = 20$dB.



(a) (b)

Fig. 6. (a). Average achievable secrecy sum rate v.s. the number of antennas of the AP, and (b). optimal power portion for artificial noise v.s. the number of antennas of the AP. $K = 3$ and $\bar{P} = 20$ dB.

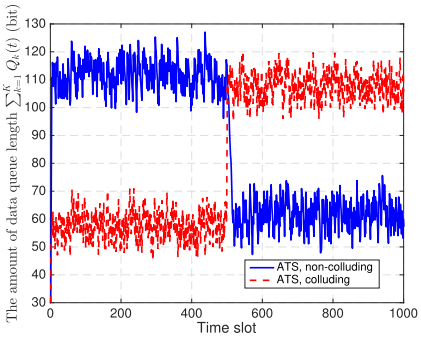


Fig. 7. The time evolution of data queue length when $N = 2$, $K = 3$, and $\bar{P} = 20$ dB.

B. Performance Assessment

Fig. 3 illustrates the average achievable secrecy rate region of the proposed adaptive transmission scheme in the non-colluding eavesdropper scenario. One may observe that, the average secrecy rate region expands with the increase in V. This can be explicated by the fact that, based on Lemma 3, a larger V means that AP can allow more data to be stored in the data buffer, so that more confidential messages can be firstly stored and transmitted when the CSI is good enough, leading to higher transmission efficiency.

Fig. 4 depicts the average achievable secrecy sum rate and the optimal power ratio allocated for artificial noise in different average power consumption cases when $K = 3$. One may easily observe that, the average achievable secrecy sum rate of the proposed adaptive transmission scheme is always superior to the benchmark scheme in non-colluding eavesdropper scenario. In the colluding eavesdropper scenario, the proposed adaptive transmission scheme performs on par with

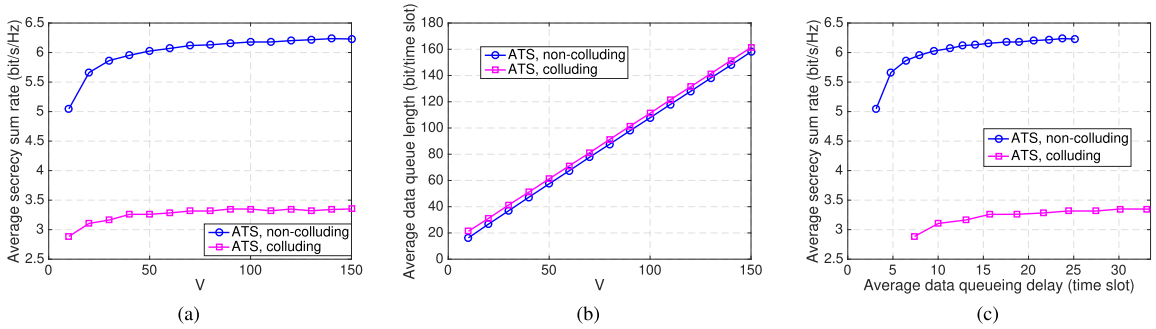


Fig. 8. (a) Average achievable secrecy sum rate v.s. V, (b) average data queue length v.s. V, and (c) tradeoff between average queueing delay and average secrecy sum rate, when $N = 2$, $K = 3$, and $\bar{P} = 20$dB.

the benchmark scheme in [4]. Moreover, we can observe that, when $N > K$, the achievable secrecy rate of the buffer-aided ZF scheme is slightly lower than the adaptive transmission scheme. More interestingly, when $N > K$, the average secrecy rate of all transmission schemes in the colluding eavesdropping scenario is significantly superior to that of the benchmark scheme in the non-colluding scenario. One can also observe from Fig. 4(b) that, the power allocated to artificial noise increases as the allowed average power consumption increases. Power allocated for artificial noise in the adaptive transmission scheme is always less than that in the benchmark scheme. This fact can be intuitively explained. With the increase in the allowed transmit power, potential eavesdroppers can receive stronger information signals, so the AP has to transmit more artificial noise to interfere with potential eavesdroppers. Since the artificial noise beamforming of the benchmark scheme is aligned to the null space of the legitimate user and cannot be accurately focused on potential eavesdroppers, the AP has to allocate more power to the artificial noise to ensure that the potential eavesdroppers can receive enough interference. This verifies that the proposed information signal and artificial noise beamforming design is more efficient.

Fig. 5 presents the average secrecy sum rate and the optimal power ratio allocated to the artificial noise for different number of users when $N = 2$ and $\bar{P} = 20$ dB. We may find that, in non-colluding case, the achievable secrecy sum rate of the proposed adaptive transmission scheme is always larger than that of the benchmark scheme. And the achievable secrecy rate gradually decreases as the number of users increases. Besides, the optimal power allocated ratio for artificial noise beamforming increases with the increase in the number of users. This is because, with the increase in the number of potential eavesdroppers, the AP prefers to transmitting more artificial noise to interfere with potential eavesdroppers, so as to guarantee that the legitimate user can achieve a relatively high secrecy rate.

Fig. 6 shows the average achievable secrecy sum rate and the optimal power allocation ratio for the artificial noise with different antenna number at the AP when $K = 3$ and $\bar{P} = 20$ dB. One may easily observe that, the secrecy rate gradually increases with the increase in the number of antennas at the AP. Moreover, for the proposed adaptive transmission scheme, when the number of antennas at the AP is large enough, the performance in the presence of colluding eavesdroppers can be arbitrarily close to that of non-colluding eavesdroppers. Furthermore, when $N \geq K$, we can find that the secrecy rates of the proposed adaptive transmission scheme and the buffer-aided ZF scheme in colluding eavesdropping case will be noticeably superior to that of the benchmark scheme of the non-colluding eavesdropping scenario. From Fig. 6(b), we may observe that, the optimal power ratio allocated to artificial noise will decrease as the antenna number at the AP increases. For the proposed adaptive transmission scheme, the power ratio allocated to the artificial noise will be gradually reduced to zero. However, the power ratio allocated to the artificial noise will only decrease slightly in the benchmark scheme. This can be interpreted as follows: (i) For the benchmark scheme, since the MRT is used to generate the information signal beamforming, which is a suboptimal solution and the information signal beam is not efficiently aligned to the legitimate user, resulting in the fact that, AP has to allocate relatively high power to the artificial noise. (ii) For the proposed adaptive transmission scheme, the information signal and artificial noise beams can be adaptively determined based on current CSIs and data queue state information. As the antenna number increases, the information signal beams can be effectively aligned to the scheduled user, resulting in the gradual reduction in the required power allocated to artificial noise.

The time evolution of the data queue length is shown in Fig. 7. At time $t = 0$, the value of V in the non-colluding and colluding eavesdropping scenario are set to $V = 100$ and $V = 50$, respectively. At time $t = 500$, the value of V in the non-colluding and colluding eavesdropping scenario are changed to $V = 50$ and $V = 100$, respectively. We can observe that, there exists an upper bound on the data queue length. Moreover, the data queue length can quickly arrive at a new stable state when the value of V changes. All these indicate that, there will be no overflow if the data buffer size is large enough, and when the appropriate V value is set according to the actual data buffer size, the proposed adaptive transmission scheme also applies to the case of finite size buffer.

The effect of different choice V on the average achievable secrecy sum rate in both non-colluding eavesdroppers and colluding eavesdroppers scenarios are shown in Fig. 8(a). One may readily observe that, the secrecy sum rate gradually grows with the increase in V. However, the performance

improvement tends to be negligible when V is large enough. Fig. 8(b) illustrates the relationship between average data queue lengths and V, and we can see that, the average queue sizes are proportional to V. The inherent tradeoff between the average data queueing delay and the average achievable secrecy sum rate is shown in Fig. 8(c). One can observe that, the average achievable secrecy sum rate increases as the average queueing delay increases. All these simulation results comply with Theorem 1, which shows that a larger average secrecy rate can be realized by using the proposed adaptive transmission scheme if a larger queueing delay is tolerable.

VI. Conclusions

In this paper, we study the achievable average secrecy rate region for the buffer-aided multiuser MISO network, in which all the unintended users are potential eavesdroppers. Firstly, the flow control, the information signal and artificial noise beamforming, and the user scheduling are considered in the proposed adaptive transmission scheme to maximize the long-term average achievable secrecy rate region. Secondly, by using the Lyapunov optimization framework, we transform the time average optimization problem into a real-time one, which cam be further decomposed into several sub-problems by using the optimization decomposition technique. Moreover, we extend the average secrecy rate region maximization problem to the worst-case scenario, in which all unintended users collude in eavesdropping. Our analysis discloses that, there is an inherent tradeoff between the average achievable secrecy rate region and the average queueing length. And it is shown that, a larger average secrecy rate region can be achieved if certain queueing delay is tolerable. Numerical results are presented to verify the effectiveness of the proposed adaptive transmission scheme. Finally, for the realistic buffer-aided multiuser MISO networks, the CSI may be either imperfect or outdated. This urges us to design a robust adaptive transmission policy to approach the achievable secrecy rate region with ideal CSIs, which will be explored in our future work.

Appendix A
Proof of Lemma 1

According to the data and virtual power consumption queue evolution equation (6) and (7), we can obtain

$$Q_k(t+1) \geq Q_k(t) + a_k(t) - d_k(t)R_s^k(t), \quad \forall, k, t, \quad (41)$$

$$E(t+1) \geq E(t) + P(t) - \bar{P}, \quad \forall t, \quad (42)$$

By summing (41) and (42) from 0 to $T-1$ time slots, dividing it by T and taking $\lim_{T\to\infty}$ on both side, we have

$$\lim_{T\to} \infty \frac{Q_k(T) - Q_k(0)}{T} \geq \lim_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1}\Big(a_k(t) - d_k(t)R_s^k(t)\Big), \quad (43)$$

$$\lim_{T\to\infty} \frac{E(T) - E(0)}{T} \geq \lim_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} P(t) - \bar{P}. \quad (44)$$

Without loss of generality, it is assumed that the initial states of all queues are zero. Since $Q_k(t), k \in \mathcal{K}$, and $E(t)$ are rate stable, i.e., $\lim_{T\to\infty} \frac{Q_k(T)}{T} = \lim_{T\to\infty} \frac{E(T)}{T} = 0$, we can conclude the Lemma 1 by substituting them into (43) and (44).

Appendix B
Proof of Lemma 2

Based on the data and virtual power consumption queue evolution in (6) and (7), we have

$$Q_k(t+1)^2 \leq Q_k(t)^2 + 2Q_k(t)\Big(a_k(t) - d_k(t)R_s^k(t)\Big) + \hat{A}_k^2 + \hat{R}_s^{k^2}, \quad \forall k, \quad (45)$$

$$E(t+1)^2 \leq E(t)^2 + 2E(t)\Big(P(t) - \bar{P}\Big) + \hat{P}^2 + \bar{P}^2. \quad (46)$$

By substituting them into (13), we can conclude Lemma 2.

Appendix C
Proof of Proposition 1

Since the proposed algorithm for deriving $(\boldsymbol{W}_k, \boldsymbol{Z}_k)$ is an iterative process that solves the sequence of convex programming **P3_4** until convergence.[2] We prove $\text{rank}(\boldsymbol{W}_k) = 1$ by using KKT conditions of the optimization problem **P3_4**. The Lagrange function for **P3_4** is given by

$$\begin{aligned}\mathcal{L}&(\boldsymbol{W}_k, \boldsymbol{Z}_k, \boldsymbol{\lambda}, \mu, \boldsymbol{A}, \boldsymbol{B})\\ &= -\text{Tr}\big(\boldsymbol{A}\boldsymbol{W}_k\big) - \text{Tr}\big(\boldsymbol{B}\boldsymbol{Z}_k\big)\\ &\quad -Q_k \log_2\Big(1 + \text{Tr}\big(\boldsymbol{H}_k(\boldsymbol{W}_k + \boldsymbol{Z}_k)\big)\Big) + Q_k F\Big(\boldsymbol{Z}_k, \boldsymbol{Z}_k^{(l)}\Big)\\ &\quad +\xi E\ \text{Tr}\big(\boldsymbol{W}_k + \boldsymbol{Z}_k\big) + \sum_{i\in\mathcal{K}\setminus\{k\}} \lambda_i\Big(\text{Tr}\big(\boldsymbol{H}_i\boldsymbol{W}_k\big)\\ &\quad -(\alpha-1)\Big(1 + \text{Tr}\big(\boldsymbol{H}_i\boldsymbol{Z}_k\big)\Big)\Big) + \mu\Big(\text{Tr}\big(\boldsymbol{W}_k + \boldsymbol{Z}_k\big) - \hat{P}\Big),\end{aligned} \quad (47)$$

where $\lambda_i \geq 0$, $\forall i \in \mathcal{K}\setminus\{k\}$, $\mu \geq 0$, $\boldsymbol{A} \succeq \boldsymbol{0}$, and $\boldsymbol{B} \succeq \boldsymbol{0}$ are Lagrange multipliers associated with constraints in (19). Based on the KKT conditions, we have

$$\frac{\partial\mathcal{L}}{\partial\boldsymbol{W}_k} = -\frac{Q_k}{\ln 2}\frac{\boldsymbol{H}_k}{1 + \text{Tr}\big(\boldsymbol{H}_k(\boldsymbol{W}_k + \boldsymbol{Z}_k)\big)} + \boldsymbol{C} - \boldsymbol{A} = \boldsymbol{0} \quad (48)$$

$$\boldsymbol{A}\boldsymbol{W}_k = \boldsymbol{0}, \quad (49)$$

where $\boldsymbol{C} \triangleq (\xi E + \mu)\boldsymbol{I} + \sum_{i\in\mathcal{K}\setminus\{k\}} \lambda_i \boldsymbol{H_i}$. By combining (49) with (48), we have

$$\boldsymbol{C}\boldsymbol{W}_k = \frac{Q_k}{\ln 2}\frac{\boldsymbol{H}_k\boldsymbol{W}_k}{1 + \text{Tr}\big(\boldsymbol{H}_k(\boldsymbol{W}_k + \boldsymbol{Z}_k)\big)}. \quad (50)$$

On the other hand, since $\boldsymbol{C} \succ 0$ and $\boldsymbol{H}_k = \boldsymbol{h}_k^H\boldsymbol{h}_k$, where $\boldsymbol{h}_k$ is a row vector such that $\text{rank}(\boldsymbol{H}_k) = 1$, we can obtain

$$\text{rank}(\boldsymbol{W}_k) = \text{rank}(\boldsymbol{C}\boldsymbol{W}_k) = \text{rank}(\boldsymbol{H}_k\boldsymbol{W}_k) \leq \text{rank}(\boldsymbol{H}_k) = 1.$$

Thus, by removing the trivial solution $\boldsymbol{W}_k = \boldsymbol{0}$, we can obtain $\text{rank}(\boldsymbol{W}_k) = 1$. This completes the proof of Proposition 1.

Appendix D
Proof of Theorem 1

With the same approach in [39], for the problem **P0**, there exists a stationary randomized transmission control scheme

[2]Here we drop the time index t for brevity.

$(a_k^*(t), \boldsymbol{w}_k^*(t), \boldsymbol{z}_k^*(t), d_k^*(t))$, which is independent of queue state $\boldsymbol{\Theta}(t)$ satisfies the following features [39],

$$\sum_{k=1}^{K} \mathbb{E}\big[\theta_k a_k^*(t)\big|\boldsymbol{\Theta}(t)\big] = \sum_{k=1}^{K} \mathbb{E}\big[\theta_k a_k^*(t)\big] = \Psi(\epsilon), \tag{51}$$

$$\mathbb{E}\big[a_k^*(t) - d_k^*(t) R_s^{k^*}(t)|\boldsymbol{\Theta}(t)\big] = \mathbb{E}\big[a_k^*(t) - d_k^*(t) R_s^{k^*}(t)\big] \leq -\epsilon, \ \forall k, \tag{52}$$

$$\mathbb{E}\big[P^*(t) - \bar{P}\big|\Theta(t)\big] = \mathbb{E}\big[P^*(t) - \bar{P}\big] \leq 0. \tag{53}$$

Since the proposed transmission scheme tries to minimize the right hand of (14), by substituting (51)-(53) into (14), we have

$$\Delta(\boldsymbol{\Theta}(t)) - V\mathbb{E}\left[\sum_{k=1}^{K} \theta_k a_k(t)\middle|\boldsymbol{\Theta}(t)\right] \leq B - V\Psi(\epsilon) - \epsilon\sum_{k=1}^{K} Q_k(t).$$

According to the law of iterated expectations, by taking conditional expectation for the above equation, we have

$$\mathbb{E}\big[L(\boldsymbol{\Theta}(t+1)) - L(\boldsymbol{\Theta}(t))\big] - V\sum_{k=1}^{K} \theta_k \mathbb{E}\big[a_k(t)\big] \leq B - V\Psi(\epsilon) - \epsilon\sum_{k=1}^{K} \mathbb{E}\big[Q_k(t)\big]. \tag{54}$$

Without loss of generality, it is assumed that the initial queue state is zero, i.e., $L(\boldsymbol{\Theta}(0)) = 0$. Then, by summing the above equation over T time slots, we can obtain

$$\frac{\xi\mathbb{E}\big[E(T)^2\big]}{2} \leq BT + V\Big(\sum_{t=0}^{T-1}\sum_{k=1}^{K} \theta_k \mathbb{E}\big[a_k(t)\big] - \Psi(\epsilon)T\Big).$$

Due to the weighted secrecy sum rate of the proposed transmission scheme cannot exceed the optimal R_{sum}^*, i.e., $\lim_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1}\sum_{k=1}^{K} \theta_k \mathbb{E}[a_k(t)] \leq R_{sum}^*$, and $\mathbb{E}[E(t)^2] \geq \mathbb{E}[E(t)]^2$. Thus, we have

$$\mathbb{E}\big[E(T)\big] \leq \sqrt{\frac{2}{\xi}\big(B + V(R_{sum}^* - \Psi(\epsilon))\big)T}. \tag{55}$$

By dividing by T and taking a limit as $T \to \infty$ for (55), we can obtain $\lim_{T\to\infty} \frac{\mathbb{E}[E(T)]}{T} = 0$, i.e., $E(t)$ is rate stable. Combined with Lemma 1, the average power consumption constraint of the AP can be guaranteed. Moreover, the similar process can be used to prove that all the data queues are rate stable, and we omit it here to save space.

Sum (54) over T time slots and divide it by T, we have

$$\frac{\mathbb{E}[L(\boldsymbol{\Theta}(T))] - \mathbb{E}[L(\boldsymbol{\Theta}(0))]}{T} - \frac{V}{T}\sum_{t=0}^{T-1}\sum_{k=1}^{K} \theta_k \mathbb{E}\big[a_k(t)\big] \leq B - V\Psi(\epsilon) - \frac{\epsilon}{T}\sum_{t=0}^{T-1}\sum_{k=1}^{K} \mathbb{E}\big[Q_k(t)\big]. \tag{56}$$

In addition, $L(\boldsymbol{\Theta}(t)) \geq 0$, $\forall t$, we can obtain

$$\frac{1}{T}\sum_{t=0}^{T-1}\sum_{k=1}^{K} \mathbb{E}\big[Q_k(t)\big] \leq \frac{B - V\Psi(\epsilon)}{\epsilon} + \frac{V}{\epsilon T}\sum_{t=0}^{T-1}\sum_{k=1}^{K} \theta_k \mathbb{E}\big[a_k(t)\big], \tag{57}$$

$$\frac{1}{T}\sum_{t=0}^{T-1}\sum_{k=1}^{K} \theta_k \mathbb{E}\big[a_k(t)\big] \geq \Psi(\epsilon) - \frac{B}{V}. \tag{58}$$

By taking a limit as $T \to \infty$ for (57), and taking a limit as $T \to \infty$ and $\Psi(\epsilon) \to R_{sum}^*$ as $\epsilon \to 0$ for (58), we can conclude the Theorem 1.

REFERENCES

[1] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.

[2] Y.-S. Shiu, S. Chang, H.-C. Wu, S. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

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

[4] M. A. Abbas, H. Song, and J.-P. Hong, "Opportunistic scheduling for average secrecy rate enhancement in fading downlink channel with potential eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 4, pp. 969–980, Apr. 2019.

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

[6] L. Hu *et al.*, "Cooperative jamming for physical layer security enhancement in Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 219–228, Feb. 2018.

[7] K. Lee, J.-P. Hong, H.-H. Choi, and M. Levorato, "Adaptive wireless-powered relaying schemes with cooperative jamming for two-hop secure communication," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2793–2803, Aug. 2018.

[8] X. Wang, Y. Chen, L. Cai, and J. Pan, "Minimizing secrecy outage probability in multiuser wireless systems with stochastic traffic," *IEEE Trans. Veh. Technol.*, vol. 66, no. 7, pp. 6449–6460, Jul. 2017.

[9] H. V. Poor and R. F. Shaefer, "Wireless physical layer security," *Proc. Nat. Acad. Sci. USA*, vol. 114, pp. 19–26, Jan. 2017.

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

[11] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[12] W. Mei, Z. Chen, L. Li, J. Fang, and S. Li, "On Artificial-Noise-Aided transmit design for multiuser MISO systems with integrated services," *IEEE Trans. Veh. Technol.*, vol. 66, no. 9, pp. 8179–8195, Sep. 2017.

[13] B. Wang, P. Mu, and Z. Li, "Secrecy rate maximization with Artificial-Noise-Aided beamforming for MISO wiretap channels under secrecy outage constraint," *IEEE Commun. Lett.*, vol. 19, no. 1, pp. 18–21, Jan. 2015.

[14] W. Wang, K. C. Teh, and K. H. Li, "Artificial noise aided physical layer security in multi-antenna small-cell networks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1470–1482, Jun. 2017.

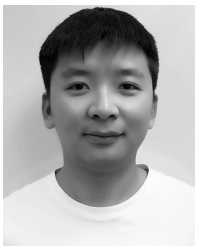
[15] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704–2717, May 2013.

[16] N. Yang, M. Elkashlan, T. Q. Duong, J. Yuan, and R. Malaney, "Optimal transmission with artificial noise in MISOME wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2170–2181, Apr. 2016.

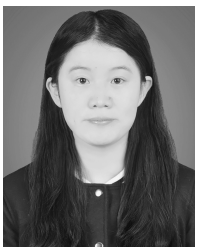
[17] Q. Li and W.-K. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming," *IEEE Trans. Signal Process.*, vol. 59, no. 8, pp. 3799–3812, Aug. 2011.

[18] M. Tian, X. Huang, Q. Zhang, and J. Qin, "Robust AN-aided secure transmission scheme in MISO channels with simultaneous wireless information and power transfer," *IEEE Signal Process. Lett.*, vol. 22, no. 6, pp. 723–727, Jun. 2015.

[19] D.-H. Chen, Y.-C. He, X. Lin, and R. Zhao, "Both worst-case and chance-constrained robust secure SWIPT in MISO interference channels," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 2, pp. 306–317, Feb. 2018.
[20] Z. Chu, H. Xing, M. Johnston, and S. Le Goff, "Secrecy rate optimizations for a MISO secrecy channel with multiple multiantenna eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 283–297, Jan. 2016.
[21] Z. Li, P. Mu, B. Wang, and X. Hu, "Optimal semiadaptive transmission with Artificial-Noise-Aided beamforming in MISO wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7021–7035, Sep. 2016.
[22] B. Akgun, O. O. Koyluoglu, and M. Krunz, "Exploiting full-duplex receivers for achieving secret communications in multiuser MISO networks," *IEEE Trans. Commun.*, vol. 65, no. 2, pp. 956–968, Feb. 2017.
[23] Q. Xiong, Y. Gong, Y.-C. Liang, and K. H. Li, "Achieving secrecy of MISO fading wiretap channels via jamming and precoding with imperfect channel state information," *IEEE Wireless Commun. Lett.*, vol. 3, no. 4, pp. 357–360, Aug. 2014.
[24] G. Chen, J. P. Coon, and M. Di Renzo, "Secrecy outage analysis for downlink transmissions in the presence of randomly located eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 5, pp. 1195–1206, May 2017.
[25] X. Lan, Q. Chen, X. Tang, and L. Cai, "Achievable rate region of the buffer-aided two-way energy harvesting relay network," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11127–11142, Nov. 2018.
[26] Y. Liu, Q. Chen, X. Tang, and L. X. Cai, "On the buffer energy aware adaptive relaying in multiple relay network," *IEEE Trans. Wireless Commun.*, vol. 16, no. 9, pp. 6248–6263, Sep. 2017.
[27] N. Zlatanov, R. Schober, and P. Popovski, "Buffer-aided relaying with adaptive link selection," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 8, pp. 1530–1542, Aug. 2013.
[28] N. Zlatanov, A. Ikhlef, T. Islam, and R. Schober, "Buffer-aided cooperative communications: Opportunities and challenges," *IEEE Commun. Mag.*, vol. 52, no. 4, pp. 146–153, Apr. 2014.
[29] V. Jamali, N. Zlatanov, A. Ikhlef, and R. Schober, "Achievable rate region of the bidirectional buffer-aided relay channel with block fading," *IEEE Trans. Inf. Theory*, vol. 60, no. 11, pp. 7090–7111, Nov. 2014.
[30] K. W. Choi and D. I. Kim, "Stochastic optimal control for wireless powered communication networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 686–698, Jan. 2016.
[31] M. Alkhawatrah, Y. Gong, G. Chen, S. Lambotharan, and J. A. Chambers, "Buffer-aided relay selection for cooperative NOMA in the Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5722–5731, Jun. 2019.
[32] J. Huang and A. L. Swindlehurst, "Buffer-aided relaying for two-hop secure communication," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 152–164, Jan. 2015.
[33] D. Wang, P. Ren, and J. Cheng, "Cooperative secure communication in two-hop buffer-aided networks," *IEEE Trans. Commun.*, vol. 66, no. 3, pp. 972–985, Mar. 2018.
[34] J. Wan, D. Qiao, H.-M. Wang, and H. Qian, "Buffer-aided two-hop secure communications with power control and link selection," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7635–7647, Nov. 2018.
[35] X. Liao, Y. Zhang, Z. Wu, Y. Shen, X. Jiang, and H. Inamura, "On security-delay trade-off in two-hop wireless networks with buffer-aided relay selection," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1893–1906, Mar. 2018.
[36] G. Chen, Z. Tian, Y. Gong, Z. Chen, and J. A. Chambers, "Max-ratio relay selection in secure buffer-aided cooperative wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 719–729, Apr. 2014.
[37] R. F. Schaefer and S. Loyka, "The secrecy capacity of compound Gaussian MIMO wiretap channels," *IEEE Trans. Inf. Theory*, vol. 61, no. 10, pp. 5535–5552, Oct. 2015.
[38] H. Ju and R. Zhang, "Optimal resource allocation in full-duplex wireless-powered communication network," *IEEE Trans. Commun.*, vol. 62, no. 10, pp. 3528–3540, Oct. 2014.
[39] M. J. Neely, "Stochastic network optimization with application to communication and queueing systems," *Synth. Lectures Commun. Netw.*, vol. 3, no. 1, pp. 1–211, Jan. 2010.
[40] Y. Ye, *Interior Point Algorithms: Theory and Analysis*. New York, NY, USA: Wiley, 1997.



Xiaolong Lan (Member, IEEE) received the B.S. degree in mathematics and applied mathematics from the Chengdu University of Technology in 2012 and the Ph.D. degree in information and communication engineering from Southwest Jiaotong University, China, in 2019. From 2017 to 2019, he was a Visiting Ph.D. Student with the University of Victoria, BC, Canada. He is currently an Associate Researcher with the College of Cybersecurity, Sichuan University, Chengdu, China. His current research interests include physical layer security, buffer-aided communication, energy-harvesting wireless communication, and mobile edge computing.



Juanjuan Ren (Student Member, IEEE) is currently pursuing the Ph.D. degree with the Key Laboratory of Information Coding and Transmission, School of Information Science and Technology, Southwest Jiaotong University, Chengdu, China. Her current research interests include buffer-aided communication, physical layer security, and nonorthogonal multiple access.

Qingchun Chen (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees (Hons.) from Chongqing University, China, in 1994 and 1997, respectively, and the Ph.D. degree from Southwest Jiaotong University, China, in 2004. He was with Southwest Jiaotong University from 2004 to 2018. He is currently a Full Professor at Guangzhou University, Guangzhou, China. He has authored and coauthored over 100 research articles, two book chapters, and 40 patents. His research interests include wireless communication, wireless network, information coding, and signal processing. He received the 2016 IEEE GLOBECOM Best Paper Award. He has been serving as an Associate Editor for IEEE ACCESS since 2015.

Lin Cai received the M.A.Sc. and Ph.D. degrees in electrical and computer engineering from the University of Waterloo, Waterloo, Canada, in 2002 and 2005, respectively. Since 2005, she has been with the Department of Electrical and Computer Engineering, University of Victoria, and she is currently a Professor. She is an NSERC E.W.R. Steacie Memorial Fellow. Her research interests span several areas in communications and networking, with a focus on network protocol and architecture design supporting emerging multimedia traffic and the Internet of Things.

She was a recipient of the NSERC Discovery Accelerator Supplement (DAS) Grants in 2010 and 2015, respectively, and the Best Paper Awards of IEEE ICC 2008 and IEEE WCNC 2011. She has co-founded and chaired the IEEE Victoria Section Vehicular Technology and Communications Joint Societies Chapter. She has been elected to serve the IEEE Vehicular Technology Society Board of Governors, from 2019 to 2021. She has served as a TPC Co-Chair of the IEEE VTC2020-Fall, and a TPC Symposium Co-Chair of the IEEE Globecom'10 and Globecom'13. She is a Registered Professional Engineer in British Columbia, Canada. She was awarded the Outstanding Achievement in Graduate Studies. She has served as an Area Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, a member of the Steering Committee of the IEEE TRANSACTIONS ON BIG DATA (TBD) and the IEEE TRANSACTIONS ON CLOUD COMPUTING (TCC), an Associate Editor of the IEEE INTERNET OF THINGS JOURNAL, the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE TRANSACTIONS ON COMMUNICATIONS, *EURASIP Journal on Wireless Communications and Networking*, the *International Journal of Sensor Networks*, and the *Journal of Communications and Networks* (JCN), and as the Distinguished Lecturer of the IEEE VTS Society.