Secure Downlink Transmission in the Internet of Things: How Many Antennas Are Needed?

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

***Abstract*—Physical layer security is a promising way to secure the wireless communications in the Internet of Things. Motivated by the fact that the limited feedback resources in the IoT network would degrade the secrecy advantage of the multiple-antenna technique, we attempt to investigate the problem of how many transmit antennas should be utilized to perform secure communications. In particular, we consider the heterogeneous IoT downlink network and design a multiuser secure transmission scheme. In this scheme, the zero-forcing beamforming technique is adopted to serve the IoT legitimate users, and the remaining spatial freedoms are utilized to send artificial noise (AN) for confusing the passive eavesdroppers. Given the secrecy outage constraints, we derive the closed-form expression for the network secrecy throughput and formulate a non-convex optimization problem with multiple parameters, e.g., the number of transmit antennas, the wiretap codes, the feedback bits allocation strategy, and the power allocation ratio between the information bearing signal and the AN. To effectively tackle this problem, we develop an optimization framework involving the block coordinate descent (BCD) algorithm and the one-dimensional search method. Simulation results validate the effectiveness of our proposed optimization framework and show that the optimal number of transmit antennas increases as the secrecy outage constraints become stricter, or the feedback resources become scarcer.**

***Index Terms*—Physical layer security, Internet of Things, optimal number of antennas, feedback bits allocation.**

I. Introduction

A. Security for the Internet of Things

The fifth generation (5G) network is recognized as the panacea of the current cellular network to meet the ever-increasing demands of mobile broadcast traffic and massive connections [1]. As an ongoing paradigm of the 5G network, the Internet of Things (IoT) is expected to provide connectivity for massive public and private sectors, thus serving as a promising cornerstone for the future intelligent society [2]. This promise generates enormous interest in exploring future IoT applications such as smart cities, home automation, wearable electronics, environmental monitoring, industrial IoT, and the Internet of Vehicles (IoV) [3, 4].

Note that the IoT would involve an enormous amount of sensitive and confidential information exchanged via wireless channels, e.g., personal privacy, trade secrets, financial files, and military secrets, such that providing the security service is one of the top priorities in the design of IoT networks [5, 6]. Traditionally, the security of data transmission has been entrusted to cryptographic techniques at the network layer. However, the dynamic and heterogeneous nature of IoT networks would raise issues such as key distribution for symmetric cryptosystems, and high computational complexity of asymmetric cryptosystems [7]. Additionally, all cryptographic measures are based on the premise that it is computationally infeasible for them to be deciphered without knowledge of the secret key, which remains mathematically unproven. Thus, the vulnerability of cryptographic schemes and the lack of a fundamental proof for perfect secrecy motivate new security mechanisms that are provably unbreakable to secure the wireless communications in IoT networks.

Different from the conventional cryptographic techniques, physical layer security provides a promising method to secure the IoT networks by exploring the inherent randomness at the physical layer [7–9]. On one hand, with appropriately designed coding and transmit precoding schemes in addition to the use of any available channel state information (CSI), physical layer security schemes enable secure communications over the wireless medium without the aid of an encryption key. This keyless advantage of physical layer security makes it particularly suitable to implement in the future IoT networks that may have no guarantee of security protocols. On the other hand, no limitations are assumed for the eavesdroppers in terms of computational resources or network parameter knowledge. As a result, even if the eavesdroppers are equipped with power computational devices, the secure communications can still be guaranteed. Therefore, physical layer security, operating essentially independently of the higher layers, is now commonly expected to complement the existing security measures to provide security service for the IoT networks [9].

B. Related Work and Motivation

A promising technique in the research field of physical layer security is the multiple-antenna technique [10]. By exploiting the spatial degrees of freedom, the multiple-antenna technique can enhance the reception performance of legitimate users and simultaneously degrade the reception performance of eavesdroppers. Since the eavesdroppers generally keep silent to hide their existence, the artificial noise (AN) technique is usually incorporated to design multi-antenna secure transmission schemes for the secrecy performance enhancement [11, 12]. The key of AN lies in sending noise signals in the null space of the legitimate user's channel to confuse the passive eavesdroppers. Typically, the secrecy performance of the AN-aided transmission scheme is directly concerned with the channel state information at the transmitter (CSIT). For example, in a three-node point-to-point scenario, the imperfect

Manuscript received September 15, 2017; revised January 31, 2018; accepted February 16, 2018. The work of J. Hu was supported by the China Scholarship Council (CSC No. 201603170124). The work of Y. Cai was supported by the National Natural Science Foundation of China under Grant 61771487, Grant 61371122, and Grant 61471393. The work of N. Yang was supported by the Australian Research Council Discovery Project under Grant DP150103905. *(Corresponding author: Yueming Cai.)*

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

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

CSIT incurred from the limited feedback would lead to the noise leakage to the legitimate receiver, causing a loss to the secrecy performance [13–15].

The multiple-antenna technique is also widely used in the multiuser secure transmission scenario [16]. Compared to the conventional point-to-point scenario, the inter-user interference makes the secure transmission design in the multiuser scenario more complicated. Moreover, the multiuser transmission also results in more opportunities of information leakage to the eavesdroppers, thus increasing the risk of being eavesdropped [17]. To decrease the risk of information leakage, the massive MIMO technique has been incorporated to design the multiuser secure transmission schemes [18–20]. In [18], a linear precoder based on regularized channel inversion was proposed to perform large-system secure communications in the broadcast channels. In [19], the massive MIMO and AN techniques were utilized to perform secure transmission in the multi-cell downlink network. In such a scenario, the authors further optimized the power allocation between the legitimate signal and the AN signal under different linear precoding schemes in [20]. These studies concluded that if there is a large enough number of antennas, the network secrecy performance can be improved.

The downlink traffic in IoT is inundated with the significant and sensitive control information, which should be kept secrecy against eavesdropping to avoid serious consequences. Since the IoT downlink network is a broadcast scenario, the multi-antenna technique is applicable and needs to be considered for designing secure transmission schemes. However, due to the limited feedback resources shared by enormous IoT users, the secrecy advantage incurred from the multi-antenna technique should be reexamined in the IoT network. Specifically, on one hand, increasing the number of antennas provides more spatial freedoms for sending AN to degrade the reception performance of the eavesdroppers. On the other hand, the limited feedback resources make the CSIT become less accurate as the number of antennas increases, such that each IoT user would suffer from more inter-user interference and experience the weakened reception performance. Motivated by this, in this work we aim to perform the multi-user secure transmission design for the IoT downlink network and address the following problem: "*How many antennas are needed to perform secure transmission in the IoT downlink network?*"

C. Our Contributions

In this work, we consider the heterogeneous IoT downlink network, where the multi-antenna controller intends to simultaneously serve secure communications to multiple IoT users in the presence of randomly distributed eavesdroppers. Given the limited feedback resources in the IoT network, we design an AN-aided multi-user secure transmission scheme and characterize the network secrecy throughput performance. In order to maximize the network secrecy throughput, many system parameters need to be carefully optimized, e.g., the number of transmit antennas, the power allocation ratio, the wiretap code parameters, and the amounts of feedback resources allocated to different users. Although this optimization problem is non-concave and difficult to solve, we propose an efficient method to handle it. The main contributions of this work can be summarized as follows.

1) We design a multi-user secure transmission scheme for the heterogeneous IoT downlink network by combing the zero-forcing beamforming and AN techniques. Under the fixed-rate scheme, we derive the closed-form expression for the network secrecy throughput and facilitate the comprehensive optimization of the number of transmit antennas, the power allocation ratio, the wiretap code parameters, as well as the feedback bits allocation strategy.
2) We develop an optimization framework to solve the non-concave optimization problem of maximizing the network secrecy throughput. In particular, we decompose the original problem into two steps. In the first step, we fix the number of antennas and design a block coordinate descent (BCD) algorithm to determine the optimal power allocation ratio, the optimal wiretap code parameters, and the optimal feedback bits allocation strategy. In the second step, the optimal number of antennas is solved by a one-dimensional search.
3) Our findings highlight that in the IoT downlink network, it is not the case that the more transmit antennas the better network secrecy performance. Moreover, we show that the optimal number of transmit antennas increases in the following cases: 1) The eavesdroppers' abilities become strengthened; 2) The IoT users need stricter secrecy requirements; 3) The feedback resources in the IoT network become scarcer.

D. Organization

The remainder of this work is organized as follows. In Section II, we describe the IoT secure downlink transmission scenario. In Section III, we characterize the statistics of the received SINRs at the IoT users and eavesdroppers. In Section IV, we design an on-off-based multiuser secure transmission scheme. In Section V, we propose a BCD-based one-dimensional search method to solve the optimization problem of maximizing the network secrecy throughput. Finally, we provide our numerical simulations and main findings in Section VI and VII, respectively.

Notation: Matrices and column vectors are denoted by uppercase and lowercase boldface letters. A complex Gaussian random variable x with zero mean and unit variance is denoted as $x \sim \mathcal{CN}(0,1)$. An Exponent-distributed random variable y with parameter a is denoted as $y \sim \mathrm{Exp}(a)$. A Gamma-distributed random variable z with parameters (b,c) is denoted as $z \sim \mathrm{Gamma}(b,c)$. $(\cdot)^{\mathrm{T}}$ and $(\cdot)^{\dagger}$ stand for transpose operation and conjugate transpose operation. $null(\cdot)$ stands for spanning the null space of matrix. $|\cdot|$ and $\|\cdot\|$ represent the norm of scalar and vector. $\log_2(\cdot)$ and $\ln(\cdot)$ represent the base 2 logarithm and natural logarithm, respectively.

II. System Model

We consider the secure downlink transmission in a typical IoT network [21, 22], where an M-antenna central controller

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2825483, IEEE Journal on Selected Areas in Communications

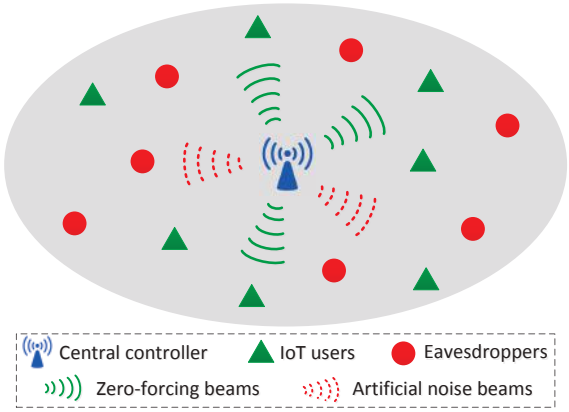

Fig. 1. Secure downlink transmission in a local IoT deployment.

transmits independent confidential messages to K single-antenna IoT users ($K \leq M$), in the presence of randomly located single-antenna eavesdroppers, as illustrated in Fig. 1. We assume that the eavesdroppers can only passively overhear the transmitted information without malicious attacks. Since there are a large number of IoT users but the feedback time slots are relatively small, the feedback resources in the IoT scenarios are fundamentally limited. Motivated by this, in this work we aim to design a multiuser secure transmission scheme for the IoT network and address the problem of how to determine the number of transmit antennas, as well as how to allocate the limited feedback resources to these IoT legitimate users.

We assume that the IoT users and the eavesdroppers experience independent flat Rayleigh fading [23, 24]. We denote $h_{i,k} \sim \mathcal{CN}(0,1)$ as the channel coefficient between the k-th user and the i-th transmit antenna at the central controller, which facilitates us to denote $\mathbf{h}_k = [h_{1,k}, h_{2,k}, \cdots, h_{M,k}]$ as the channel vector between the k-th user and the central controller. As such, the received signal at the k-th IoT user can be given by

$$y_k = \sqrt{\varsigma_k}\mathbf{h}_k\mathbf{x} + n_k, \tag{1}$$

where ς_k denotes the path loss coefficient between the k-th IoT user and the central controller, $\mathbf{x}$ is the transmitted symbol vector containing information symbols carried by all M beams with an average power constraint $\mathbb{E}\{\|\mathbf{x}\|^2\} = \rho$, and $n_k \sim \mathcal{CN}(0,1)$ denotes the additive white Gaussian noise (AWGN) at the k-th IoT user.

For a robust secure transmission design, we assume that the eavesdroppers' locations are unavailable to the network. In the literature, the homogeneous Poisson point process (PPP) has been widely used to examine the impact of random eavesdroppers' locations on secrecy performance [25–28]. In this work, we model the eavesdroppers' locations to be distributed on the infinite two-dimensional plane according to a homogeneous PPP Φ of intensity λ. Also, we denote $g_{i,l} \sim \mathcal{CN}(0,1)$ as the channel coefficient between the l-th eavesdropper and the i-th transmit antenna at the central controller, which facilitates us to denote $\mathbf{g}_l = [g_{1,l}, g_{2,l}, \cdots, g_{M,l}]$ as the channel vector between the l-th eavesdropper and the central controller. As such, the received signal at the l-th eavesdropper can be given by

$$z_l = \sqrt{\varrho_l}\mathbf{g}_l\mathbf{x} + w_l, \tag{2}$$

where ϱ_l denotes the path loss coefficient between the l-th eavesdropper and the central controller, and $w_l \sim \mathcal{CN}(0,1)$ denotes the AWGN at the l-th eavesdropper.

In each coherent block, the central controller first broadcasts pilot symbols to enable the IoT users to perform channel estimation. In this work, we assume that there is no estimation error at the user side, i.e., the k-th IoT user has perfect knowledge of $\mathbf{h}_k$, and the l-th eavesdropper has perfect knowledge of $\mathbf{g}_l$. Moreover, we consider that the central controller is able to acquire partial knowledge about $\mathbf{h}_k$ with the help of some feedback information from the IoT users. However, since the eavesdroppers perform as passive users, the central controller cannot obtain any instantaneous knowledge about $\mathbf{g}_l$.

For a robust secure transmission design, we consider the worst-case scenario where we assume that if an eavesdropper intends to intercept one message stream, he/she is capable of canceling the interference caused by the message streams transmitted from the central controller to other IoT users [26]. To guarantee security under this scenario, it is advisable to use certain dimensions of beams to send AN for confusing the eavesdroppers' reception. Motivated by this, in the following we perform the secure transmission design by exploiting K out of M beams to serve the IoT users and using the remaining $M-K$ dimensions of beams to send AN for secrecy enhancement.

A. Limited Feedback and CDI Quantization Model

Prior to the secure message transmission, the central controller first sends pilot symbols, and then the K IoT users perform channel estimation and convey back their channel knowledge to the central controller for the subsequent beamforming design. However, a common fact in the IoT network is that the feedback resources available for the IoT users are quite limited. Practically, the feedback resources allocated to a single IoT user determines the accuracy of its corresponding CSIT, which directly affects the secure transmission design for this user. Therefore, how to allocate the feedback resources to these IoT users has an important impact on the network secrecy performance.

We assume that all IoT users share a common feedback channel with a capacity of B_{total} bits per coherence block, and the number of feedback bits allocated to the k-th IoT user is B_k, leading to the constraint $\sum_{k=1}^{K} B_k = B_{\text{total}}$. Since the channel direction information (CDI) is especially vital for beamforming design in the multi-user system, we further assume that all the feedback load per user, e.g., B_k, is used to capture the CDI knowledge, e.g., $\mathbf{d}_k = \mathbf{h}_k/\|\mathbf{h}_k\|$. Specifically, in each coherence block the k-th IoT user chooses the optimal quantized CDI vector from a 2^{B_k}-sized codebook $\mathcal{C}_k = \{\mathbf{c}_{1,k}, \mathbf{c}_{2,k}, \cdots, \mathbf{c}_{2^{B_k},k}\}$, yielding

$$\tilde{\mathbf{d}}_k = \underset{\mathbf{c}_{n,k} \in \mathcal{C}_k}{\arg\max} |\mathbf{d}_k \mathbf{c}_{n,k}^{\dagger}|^2. \tag{3}$$

Then the k-th IoT user conveys back the index of $\tilde{\mathbf{d}}_k$ to the central controller by using B_k feedback bits. We clarify that the codebooks at different users (e.g., $\mathcal{C}_{k_1}$ and $\mathcal{C}_{k_2}$, $k_1 \neq k_2$) are independent with each other.

To guarantee a good quantization codebook, e.g., $\mathcal{C}_k$, [29] and [30] have concluded that an optimal codebook is the one which minimizes the maximum correlation between any pair of beamforming vectors. In this work, we adopt this criterion to independently generate the quantization codebook at each IoT user and resort to the quantization cell approximation used in [29, 30] to characterize the codebooks generated by this criterion. Using this method, if we define $\cos^2\theta_k = |\mathbf{d}_k\tilde{\mathbf{d}}_k^{\dagger}|^2$, the cumulative distribution function (CDF) of $\cos^2\theta_k$ is approximated as

$$F_{\cos^2\theta_k}(x) = \begin{cases} 0, & 0 \leq x < 1-\varepsilon_k, \\ 1-2^{B_k}(1-x)^{M-1}, & 1-\varepsilon_k \leq x \leq 1, \end{cases} \quad (4)$$

where $\varepsilon_k = 2^{-\frac{B_k}{M-1}}$ reflects the maximum quantization error of the codebook (e.g., $\mathcal{C}_k$) used at the k-th IoT user.

B. Artificial Noise Beams Construction

After receiving the channel feedback from K IoT users, the central controller can acquire an $M \times K$ CDI matrix as $\tilde{\mathbf{D}} = [\tilde{\mathbf{d}}_1^{\mathrm{T}}, \tilde{\mathbf{d}}_2^{\mathrm{T}}, \cdots, \tilde{\mathbf{d}}_K^{\mathrm{T}}]$. To degrade the reception performance at the passive eavesdroppers, we introduce the AN technique for secrecy enhancement. In particular, we exploit the remaining $M-K$ beams for AN transmission and construct these AN beams, e.g., $\{\mathbf{f}_1, \mathbf{f}_2, \cdots, \mathbf{f}_{M-K}\}$, $\mathbf{f}_j \in \mathbb{C}^{M\times 1}$, by finding an orthonormal basis for the null space of $\tilde{\mathbf{D}}$. Therefore, these AN beams form an $M \times (M-K)$ matrix $\mathbf{F} = [\mathbf{f}_1, \mathbf{f}_2, \cdots, \mathbf{f}_{M-K}]$, satisfying $\mathbf{F} = \mathrm{null}(\tilde{\mathbf{D}})$.

C. Zero-Forcing Beams Construction

To avoid significant interference affecting the IoT users, in this work we consider that the central controller simultaneously serves K IoT users through the zero-forcing beamforming (ZFBF) technique. To keep the ZF beams independent with the AN beams, we first generate an $M \times (M-K)$ matrix as $\hat{\mathbf{D}} = [\hat{\mathbf{d}}_1, \hat{\mathbf{d}}_2, \cdots, \hat{\mathbf{d}}_{M-K}]$, where $\hat{\mathbf{d}}_i \in \mathbb{C}^{M\times 1}$ is a randomly generated unit vector. Then we define $\mathbf{D} = [\tilde{\mathbf{D}}, \hat{\mathbf{D}}]$ and construct the K unit ZF beams, e.g., $\mathbf{w}_i \in \mathbb{C}^{M\times 1}$, from the pseudo-inverse

$$\mathbf{E} = \mathbf{D}^{\dagger}(\mathbf{D}\mathbf{D}^{\dagger})^{-1}. \quad (5)$$

In particular, $\mathbf{w}_i$ can be obtained by normalizing the i-th column of $\mathbf{E}$. It is worth mentioning that since we only have K IoT users and add $M-K$ dimensions of randomness into $\mathbf{D}$, only the first K columns of $\mathbf{E}$ are meaningful. These ZF beams form an $M \times K$ matrix $\mathbf{W} = [\mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_K]$.

D. Transmitted Symbol Vector

Based on the construction of AN and ZF beams, the precoding matrix at the central controller can be written as $\mathbf{P} = [\mathbf{W}, \mathbf{F}]$. We define $\mathbf{s} = [u_1, u_2, \cdots, u_K, v_1, v_2, \cdots, v_{M-K}]^{\mathrm{T}}$ as the signal vector, where u_i is the information-bearing signal intended for the i-th IoT user, and v_j is a randomly generated complex Gaussian signal intended for confusing the passive eavesdroppers. As such, the transmitted symbol vector $\mathbf{x}$ is formulated as

$$\mathbf{x} = \mathbf{P}\mathbf{s} = \mathbf{W}\mathbf{u} + \mathbf{F}\mathbf{v}, \quad (6)$$

where $\mathbf{u} = [u_1, u_2, \cdots, u_K]^{\mathrm{T}}$, and $\mathbf{v} = [v_1, v_2, \cdots, v_{M-K}]^{\mathrm{T}}$. In this work, we consider that the transmit power of each ZF beam is ρ_u, and the transmit power of each AN beam is ρ_v, such that we have $K\rho_u + (M-K)\rho_v = \rho$. By defining $\rho_v = \rho_u\phi$, we formulate ρ_u and ρ_v as $\rho_u = \frac{\rho}{K+(M-K)\phi}$ and $\rho_v = \frac{\rho\phi}{K+(M-K)\phi}$, respectively. Note that ϕ acts as an important parameter in the process of secure transmission design.

III. Statistical Characterization of SINR

Prior to the secure transmission design, in this section we focus on characterizing the statistics of the received SINRs at the IoT users and the eavesdroppers.

1) Received SINRs at IoT Users: Aided by (6), the received signal at the k-th IoT user in (1) can be rewritten as

$$y_k = \sqrt{\varsigma_k}\left(\mathbf{h}_k\mathbf{w}_k u_k + \sum_{i=1,i\neq k}^{K}\mathbf{h}_k\mathbf{w}_i u_i + \sum_{j=1}^{M-K}\mathbf{h}_k\mathbf{f}_j v_j\right) + n_k. \quad (7)$$

Since the ZF beams and AN beams are independently chosen orthogonal to the quantized CDI of other IoT users but not the actual CDI, the interference terms in (7) are not completely eliminated. More specifically, the second term in (7) is the interference from the $K-1$ message streams intended for other IoT users, and the third term is the interference from the transmitted AN. Thus, the received SINR at the k-th IoT user is given by

$$\begin{aligned}\gamma_{t,k} &= \frac{\varsigma_k\rho_u|\mathbf{h}_k\mathbf{w}_k|^2}{1+\varsigma_k\left(\rho_u\sum\limits_{i=1,i\neq k}^{K}|\mathbf{h}_k\mathbf{w}_i|^2+\rho_v\sum\limits_{j=1}^{M-K}|\mathbf{h}_k\mathbf{f}_j|^2\right)} \\ &= \frac{\varsigma_k\rho_u|\mathbf{h}_k\mathbf{w}_k|^2}{1+\varsigma_k\|\mathbf{h}_k\|^2\left(\rho_u\sum\limits_{i=1,i\neq k}^{K}|\mathbf{d}_k\mathbf{w}_i|^2+\rho_v\sum\limits_{j=1}^{M-K}|\mathbf{d}_k\mathbf{f}_j|^2\right)}.\end{aligned} \quad (8)$$

As depicted in Fig. 2, we decompose $\mathbf{d}_k$ as

$$\mathbf{d}_k = (\cos\theta_k)\tilde{\mathbf{d}}_k + (\sin\theta_k)\mathbf{e}_k, \quad (9)$$

where $\mathbf{e}_k \in \mathbb{C}^{1\times M}$ is an unit vector orthogonal to $\tilde{\mathbf{d}}_k$. By applying $\tilde{\mathbf{d}}_k\mathbf{w}_i = 0$ and $\tilde{\mathbf{d}}_k\mathbf{f}_j = 0$, we rewrite (8) as

$$\gamma_{t,k} = \frac{\varsigma_k\rho_u|\mathbf{h}_k\mathbf{w}_k|^2}{1+\varsigma_k\|\mathbf{h}_k\|^2(\sin^2\theta_k)\Theta}, \quad (10)$$

where

$$\Theta = \rho_u\sum_{i=1,i\neq k}^{K}|\mathbf{e}_k\mathbf{w}_i|^2 + \rho_v\sum_{j=1}^{M-K}|\mathbf{e}_k\mathbf{f}_j|^2. \quad (11)$$

Note that $\mathbf{e}_k$ and $\mathbf{w}_i$ are independent unit vectors on the $M-1$ dimensional hyperplane orthogonal to $\tilde{\mathbf{d}}_k$, implying that $|\mathbf{e}_k\mathbf{w}_i|^2$ is a Beta-distributed random variable with parameters $(1, M-2)$. Similarly, $|\mathbf{e}_k\mathbf{f}_j|^2$ is also a Beta-distributed random

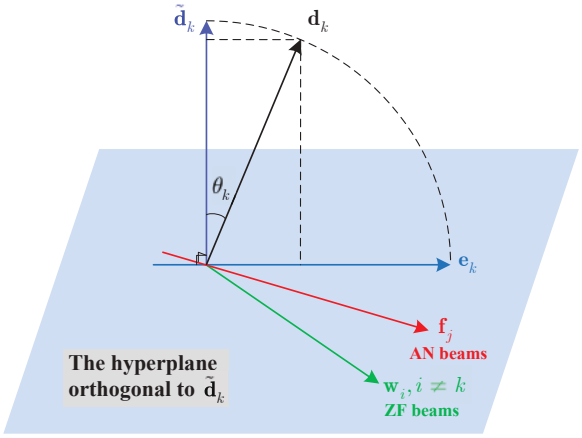

Fig. 2. The geometric illustration of $\mathbf{d}_k$, $\tilde{\mathbf{d}}_k$, $\mathbf{e}_k$, $\mathbf{f}_j$ and $\mathbf{w}_i$.

variable with parameters $(1, M-2)$. As such, for a given $\mathbf{h}_k$, the expected SINR at the k-th IoT user is given by

$$\mathbb{E}\{\gamma_{t,k}|\mathbf{h}_k\} = \frac{\varsigma_k \rho_u |\mathbf{h}_k \mathbf{w}_k|^2}{1 + \varsigma_k \|\mathbf{h}_k\|^2 (\sin^2 \theta_k) \mathbb{E}\{\Theta\}}, \tag{12}$$

where

$$\begin{aligned}\mathbb{E}\{\Theta\} &= \mathbb{E}\left\{\rho_u \sum_{i=1, i\neq k}^{K} |\mathbf{e}_k \mathbf{w}_i|^2 + \rho_v \sum_{j=1}^{M-K} |\mathbf{e}_k \mathbf{f}_j|^2\right\} \\ &= \rho_u \frac{K-1}{M-1} + \rho_v \frac{M-K}{M-1} = \frac{\rho - \rho_u}{M-1}.\end{aligned} \tag{13}$$

For simplicity, we adopt the similar approximation method proposed in [31] by directly formulating $\gamma_{t,k} = \mathbb{E}\{\gamma_{t,k}|\mathbf{h}_k\}$ for the following analysis. Since determining $\mathbf{w}_k$ is irrelevant to $\tilde{\mathbf{d}}_k$, $\mathbf{w}_k$ and $\mathbf{h}_k$ are independent, implying that $|\mathbf{h}_k \mathbf{w}_k|^2 \sim \text{Exp}(1)$. We further note that $\|\mathbf{h}_k\|^2 (\sin^2 \theta_k) \sim \text{Gamma}(M-1, \varepsilon_k)$, which has been proved in Appendix I of [31]. Thus, we can derive the CDF of $\gamma_{t,k}$ as

$$F_{\gamma_{t,k}}(x) = 1 - e^{-\frac{x}{\varsigma_k \rho_u}} (1 + \tau(\phi) \varepsilon_k x)^{1-M}, \tag{14}$$

where $\tau(\phi) = \frac{(M-K)\phi + K - 1}{M-1}$.

2) Received SINRs at Eavesdroppers: If the l-th eavesdropper intends to intercept the k-th IoT user, the received signal in (2) can be rewritten as

$$z_l = \sqrt{\varrho_l} \left(\mathbf{g}_l \mathbf{w}_k u_k + \sum_{i=1, i\neq k}^{K} \mathbf{g}_l \mathbf{w}_i u_i + \sum_{j=1}^{M-K} \mathbf{g}_l \mathbf{f}_j v_j \right) + w_l. \tag{15}$$

Since in this work we consider the worst-case eavesdropping scenario, we cannot make any assumptions that may limit the eavesdroppers' abilities to decode information [26, 32]. Based on this consideration, we assume that the eavesdroppers can cancel the interference caused by the $K-1$ messages streams intended for other IoT users, i.e., the second term in (15) should be assumed to be zero. As such, the received SINR at the l-th eavesdropper is given by

$$\gamma_{e,l} = \frac{\varrho_l \rho_u |\mathbf{g}_l \mathbf{w}_k|^2}{1 + \varrho_l \rho_v \sum_{j=1}^{M-K} |\mathbf{g}_l \mathbf{f}_j|^2}. \tag{16}$$

Since either $\mathbf{w}_k$ or $\mathbf{f}_j$ is merely determined according to the quantized channel knowledge of the IoT users, e.g., $\tilde{\mathbf{D}}$, they are independent of $\mathbf{g}_l$, implying $|\mathbf{g}_l \mathbf{w}_k|^2 \sim \text{Exp}(1)$ and $|\mathbf{g}_l \mathbf{f}_j|^2 \sim \text{Exp}(1)$. Conditioned on a fixed ϱ_l, we use the same method for deriving $\gamma_{t,k}$ and formulate the CDF of $\gamma_{e,l}$ as

$$F_{\gamma_{e,l}}(x|\varrho_l) = 1 - e^{-\frac{x}{\varrho_l \rho_u}} (1 + \phi x)^{K-M}. \tag{17}$$

Note that the eavesdropper with the maximum received SINR has the strongest eavesdropping ability, and thus we next characterize the statistic of $\gamma_e = \max_{l \in \Phi} \gamma_{e,l}$. For analytical tractability, we denote the distance between the l-th eavesdropper and the central controller as d_l and apply the classical unbounded path loss model, e.g., $\varrho_l = d_l^{-\alpha}$, where α denotes the path loss exponent. Since we consider the randomly located eavesdroppers in the network, we derive the CDF of γ_e as

$$F_{\gamma_e}(x) = \exp\left(\frac{-2\lambda\pi}{\alpha (1 + \phi x)^{M-K}} \left(\frac{\rho_u}{x}\right)^{\frac{2}{\alpha}} \Gamma\left(\frac{2}{\alpha}\right) \right). \tag{18}$$

For the detailed derivation process of (18), readers may refer to [33] for the complete proof.

IV. Secure Transmission Design

In this section, we present the secure transmission design in our considered IoT scenario. To guarantee the design with low complexity, we first describe how to facilitate the fixed-rate wiretap codes design. Since this fixed-rate design makes the on-off scheme be a natural candidate for use, we then develop an on-off-based secure transmission scheme and characterize the network secrecy throughput.

A. Wiretap Codes Design

To perform the secure transmission in our considered IoT scenario, we need to determine the wiretap code parameters for different legitimate users, i.e., the codeword transmission rate $R_{t,k}$, and the rate redundancy $R_{e,k}$ [34, 35]. To be specific, for the k-th IoT user, an n-length wiretap code is constructed by generating $2^{nR_{t,k}}$ codewords $x^n(w, v)$, where $w \in \{1, \cdots, 2^{n(R_{t,k} - R_{e,k})}\}$, and $v \in \{1, \cdots, 2^{nR_{e,k}}\}$. When the central controller intends to transmit a message indexed by w, it randomly selects v from $\{1, \cdots, 2^{nR_{e,k}}\}$ with uniform probability and transmits the codeword $x^n(w, v)$. Note that the IoT devices generally have limited hardware and cost less; thus, the sophisticated decoding or encoding may be not available at the receiver side. Motivated by this, in this work we adopt the fixed-rate scheme to design the wiretap codes. Since K IoT users are simultaneously served by the central controller, we need to construct K sets of code pair, e.g., $(R_{t,k}, R_{e,k})$, for different IoT users.

B. Secure Transmission to the k-th IoT User

1) Transmission Probability: To implement the fixed-rate design, we propose an on-off-based secure transmission scheme. Specifically, the secure transmission to the k-th IoT user happens only when the instantaneous channel quality at the k-th IoT user, e.g., $C_{t,k} = \log_2(1 + \gamma_{t,k})$, can support

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2825483, IEEE Journal on Selected Areas in Communications

$R_{t,k}$. This is the so-called transmission condition, and the corresponding transmission probability is given by $p_{\mathrm{tm},k} = \Pr\{C_{t,k} \geq R_{t,k}\}$. To simplify denotations, we define $R_{t,k} = \log_2(1+\xi_{t,k})$ and express $p_{\mathrm{tm},k}$ as $p_{\mathrm{tm},k} = \Pr\{\gamma_{t,k} \geq \xi_{t,k}\}$. Aided by the CDF of $\gamma_{t,k}$ in (14), the transmission probability is mathematically derived as

$$p_{\mathrm{tm},k} = 1 - F_{\gamma_{t,k}}(\xi_{t,k}) = e^{-\frac{\xi_{t,k}}{\varsigma_k \rho_u}} (1+\tau(\phi)\varepsilon_k \xi_{t,k})^{1-M}.$$

Notably, in every transmission block, each IoT user should also convey back an extra bit identifying the on/off state. However, this 1-bit feedback overhead is relatively small, such that it is omitted in our work.

2) Secrecy Outage Probability: In the passive eavesdropping scenario, perfect secrecy is not always available due to the lack of eavesdroppers' channel knowledge. When the transmission condition is met but the designed rate redundancy is below the channel capacity of the strongest eavesdropper, the information leakage occurs. This is the so-called secrecy outage event conditioned on transmission. Conversely, for the secure transmission to the k-th IoT user, the secrecy outage probability is expressed as

$$p_{\mathrm{so},k} = \Pr\{C_e \geq R_{e,k} | C_{t,k} \geq R_{t,k}\}, \tag{19}$$

where $C_e = \log_2(1+\gamma_e)$ denotes the instantaneous channel capacity of the strongest eavesdropper. Due to our fixed-rate design, the secrecy outage event is independent of the transmission condition, which yields $p_{\mathrm{so},k} = \Pr\{C_e \geq R_{e,k}\}$. Also, we define $R_{e,k} = \log_2(1+\xi_{e,k})$ and express $p_{\mathrm{so},k}$ as $p_{\mathrm{so},k} = \Pr\{\gamma_e \geq \xi_{e,k}\}$. Aided by the CDF of $\gamma_{e,k}$ in (18), we derive $p_{\mathrm{so},k}$ as

$$p_{\mathrm{so},k} = 1 - F_{\gamma_e}(\xi_{e,k}) = 1 - \exp\left(\frac{-\chi(\rho_u/\xi_{e,k})^{\beta}}{(1+\phi\xi_{e,k})^{M-K}}\right), \tag{20}$$

where $\beta = 2/\alpha$, and $\chi = \lambda\pi\Gamma(\beta+1)$.

3) Secrecy Throughput: To find the optimal wiretap codes, the secrecy throughput is often formulated as the optimization goal. In our considered scenario, the secrecy throughput of the k-th IoT user is defined as the product of the transmission probability and the secrecy rate, e.g., $\eta_{t,k} = p_{\mathrm{tm},k}(R_{t,k} - R_{e,k})$, yielding

$$\eta_{t,k} = \frac{e^{-\xi_{t,k}/(\varsigma_k\rho_u)}}{(1+\tau(\phi)\varepsilon_k\xi_{t,k})^{M-1}} \log_2\left(\frac{1+\xi_{t,k}}{1+\xi_{e,k}}\right). \tag{21}$$

C. Network Secrecy Throughput

Since in this work we consider the IoT downlink network, the network secrecy throughput should be used as the optimization target to determine the system parameters. Aided by (21), the network secrecy throughput is expressed as

$$\eta = \sum_{k=1}^{K} \eta_{t,k} = \sum_{k=1}^{K} \frac{e^{-\xi_{t,k}/(\varsigma_k\rho_u)}}{(1+\tau(\phi)\varepsilon_k\xi_{t,k})^{M-1}} \log_2\left(\frac{1+\xi_{t,k}}{1+\xi_{e,k}}\right). \tag{22}$$

In the following, we aim to discuss how to determine the optimal M, ϕ, $\mathbf{B} = [B_1, B_2, \cdots, B_K]$, $\boldsymbol{\xi}_t = [\xi_{t,1}, \xi_{t,2}, \cdots, \xi_{t,K}]$, and $\boldsymbol{\xi}_e = [\xi_{e,1}, \xi_{e,2}, \cdots, \xi_{e,K}]$ maximizing the network secrecy throughput subject to the pre-specified secrecy outage constraints, e.g., $\boldsymbol{\delta} = [\delta_1, \delta_2, \cdots, \delta_K]$.

V. Network Secrecy Throughput Maximization

In this section, we show that the optimization problem of maximizing the network secrecy throughput can be solved by two steps. Specifically, we first fix M and determine the optimal ϕ, $\mathbf{B}$, $\boldsymbol{\xi}_t$, and $\boldsymbol{\xi}_e$ by developing a BCD algorithm. Then we directly use the one-dimensional search method to tackle the optimal M.

A. Problem Formulation

***Problem** 1:* The joint optimization of M, ϕ, $\mathbf{B}$, $\boldsymbol{\xi}_t$, and $\boldsymbol{\xi}_e$ maximizing the secrecy throughput under the given secrecy outage constraints can be formulated as

$$\max_{M,\phi,\mathbf{B},\boldsymbol{\xi}_t,\boldsymbol{\xi}_e} \quad \eta(M,\phi,\mathbf{B},\boldsymbol{\xi}_t,\boldsymbol{\xi}_e), \tag{23a}$$

$$\text{s.t.} \quad \mathbf{p}_{\mathrm{so}} \leq \boldsymbol{\delta}, \tag{23b}$$

$$\boldsymbol{\xi}_t \geq \boldsymbol{\xi}_e, \tag{23c}$$

$$M \geq K, \tag{23d}$$

$$\sum\nolimits_{k=1}^{K} B_k = B_{\mathrm{total}}, \tag{23e}$$

where $\mathbf{p}_{\mathrm{so}} = [p_{\mathrm{so},1}, p_{\mathrm{so},2}, \cdots, p_{\mathrm{so},T}]$ and $\boldsymbol{\delta} = [\delta_1, \delta_2, \cdots, \delta_K]$. To clarify, the constraint (23b) guarantees the secrecy outage probability of each IoT user meets its individual requirement, and the constraint (23c) guarantees a positive secrecy rate for the k-th IoT user.

We find from (23) that ***Problem** 1* is a typical mixed integer nonlinear programming (MINLP) problem, and very few effective methods can be used to solve it efficiently. To facilitate an effective method to solve it, we first carry on the following equivalent transformation

$$\max_{M,\phi,\mathbf{B},\boldsymbol{\xi}_t,\boldsymbol{\xi}_e} \eta \Leftrightarrow \max_{M} \max_{\phi,\mathbf{B},\boldsymbol{\xi}_t,\boldsymbol{\xi}_e} \eta. \tag{24}$$

This transformation implies that we can handle ***Problem** 1* by decomposing it into two optimization problems. In particular, we can first maximize η over ϕ, $\mathbf{B}$, $\boldsymbol{\xi}_t$, and $\boldsymbol{\xi}_e$ subject to a fixed M, and then maximize η over the one-dimensional variable M. In the following, we provide the detailed procedures to handle these two optimization problems.

B. BCD Algorithm Design for Solving the First Problem

***Problem** 2:* Subject to a fixed M, what are the optimal ϕ, $\mathbf{B}$, $\boldsymbol{\xi}_t$, and $\boldsymbol{\xi}_e$ that maximize η under the given secrecy outage constraints? This problem is formulated as

$$\max_{\phi,\mathbf{B},\boldsymbol{\xi}_t,\boldsymbol{\xi}_e} \quad \eta(\phi,\mathbf{B},\boldsymbol{\xi}_t,\boldsymbol{\xi}_e), \tag{25a}$$

$$\text{s.t.} \quad \text{(23b), (23c), and (23e).} \tag{25b}$$

Prior to solving ***Problem** 2*, we first transform the constraint in (23b) into a more explicit form. In particular, aided by the monotonicity of $F_{\gamma_{e,k}}$, we obtain

$$p_{\mathrm{so},k} \leq \delta_k \Leftrightarrow \xi_{e,k} \geq F_{\gamma_e}^{-1}(1-\delta_k), \tag{26}$$

where $F_{\gamma_e}^{-1}(\cdot)$ denotes the inverse function of $F_{\gamma_e}(\cdot)$. For ease of notation, we define $\Theta_k(\phi) = F_{\gamma_e}^{-1}(1-\delta_k)$. It is easy to find that to maximize η in (22), $\xi_{e,k}$ needs to be set to its minimum

value, e.g., $\xi_{e,k} = \Theta_k(\phi)$, which enables us to re-express (22) as

$$\eta = \sum_{k=1}^{K} \frac{e^{-\xi_{t,k}/(\varsigma_k \rho_u)}}{\left(1+\tau(\phi)\varepsilon_k \xi_{t,k}\right)^{M-1}} \log_2\left(\frac{1+\xi_{t,k}}{1+\Theta_k(\phi)}\right). \quad (27)$$

Although $\Theta_k(\phi)$ is an implicit function of ϕ, it is not hard to calculate its value by numerically searching the unique root of $F_{\gamma_e}(\Theta_k(\phi)) = 1-\delta_k$ subject to an arbitrary ϕ.

The above analysis demonstrates that $\boldsymbol{\xi}_e$ can be determined together with ϕ, such that we can decrease the dimensions of the optimization variables in ***Problem 2***. However, this simplified problem is still non-convex and difficult to solve. In the following, we propose an efficient BCD algorithm to solve this joint optimization problem [36, 37]. Specifically, we decouple all the optimization variables into three blocks, e.g., $\{\boldsymbol{\xi}_t\}$, $\{\phi, \boldsymbol{\xi}_e\}$, and $\{\mathbf{B}\}$, and alternatively optimize one block of variables by fixing other blocks of variables at their values from the last iteration. Each iteration of the proposed algorithm involves solving three subproblems as follows.

1) Subproblem 1: In the n-th iteration, we first intend to optimize $\boldsymbol{\xi}_t[n]$ subject to $\phi[n-1]$ and $\mathbf{B}[n-1]$ by considering the following problem

$$\max_{\boldsymbol{\xi}_t[n]} \ \eta\left(\boldsymbol{\xi}_t[n], \phi[n-1], \mathbf{B}[n-1]\right). \quad (28)$$

By observing the expression for η in (27), we find that the maximization of η can be facilitated by respectively maximizing its general term, e.g., $\eta_{t,k}$. Moreover, in the term of $\eta_{t,k}$, $\xi_{t,k}$ is merely coupled with ϕ and B_k, which implies that we only need to characterize the maximization of $\eta_{t,k}$ to determine the optimal $\xi_{t,k}[n]$ with the fixed $\phi[n-1]$ and $B_k[n-1]$. In the following, we show that $\eta_{t,k}$ is a quasi-concave function of $\xi_{t,k}$ when $\phi \leq 1$ holds true[1].

We take the first derivative of $\eta_{t,k}$ in (21) on $\xi_{t,k}$, yielding

$$\frac{\partial \eta_{t,k}}{\partial \xi_{t,k}} = \frac{e^{-\frac{\xi_{t,k}}{\varsigma_k \rho_u}} \Xi(\xi_{t,k})}{\ln 2 \cdot \left(1+\tau(\phi)\varepsilon_k \xi_{t,k}\right)^{M}}, \quad (29)$$

where $\Xi(\xi_{t,k})$ is expressed by

$$\Xi(\xi_{t,k}) = \frac{1+\tau(\phi)\varepsilon_k\xi_{t,k}}{1+\xi_{t,k}} - \frac{1+\tau(\phi)\varepsilon_k\xi_{t,k}}{\varsigma_k\rho_u} \ln\left(\frac{1+\xi_{t,k}}{1+\Theta_k(\phi)}\right) - (M-1)\tau(\phi)\varepsilon_k \ln\left(\frac{1+\xi_{t,k}}{1+\Theta_k(\phi)}\right). \quad (30)$$

Since the sign of $\frac{\partial \eta_{t,k}}{\partial \xi_{t,k}}$ follows that of $\Xi(\xi_{t,k})$, the monotonicity of $\eta_{t,k}$ can be examined by analyzing the sign of $\Xi(\xi_{t,k})$. Under the constraint $\phi \leq 1$, $\tau(\phi) \leq 1$ always holds true, implying that the three terms in the right-hand side (RHS) of (30) are all decreasing functions of $\xi_{t,k}$, i.e., $\Xi(\xi_{t,k})$ is a decreasing function of $\xi_{t,k}$. Therefore, we state that $\eta_{t,k}$ is a quasi-concave function of $\xi_{t,k}$.

Subject to the constraint of $\xi_{t,k} \geq \xi_{e,k}$, the feasible region of $\xi_{t,k}$ is $[\Theta_k(\phi), \infty)$. Since $\Xi(\Theta_k(\phi)) > 0$ and $\Xi(\infty) < 0$ always hold true, $\Xi(\xi_{t,k})$ is first positive then negative. That is, $\eta_{t,k}$ first increases then decreases with $\xi_{t,k}$, such that the maximum is achieved at $\xi_{t,k} = \xi^*_{t,k}$, satisfying $\Xi(\xi^*_{t,k}) = 0$. Although the explicit expression for $\xi^*_{t,k}$ is difficult to derive, we clarify that we can adopt the bisection method to calculate it. In this way, the optimal $\boldsymbol{\xi}_t[n]$ subject to the fixed $\phi[n-1]$ and $\mathbf{B}[n-1]$ can be determined.

2) Subproblem 2: In the n-th iteration, we then intend to optimize $\phi[n]$ subject to $\boldsymbol{\xi}_t[n]$ and $\mathbf{B}[n-1]$ by considering the following problem

$$\max_{\phi[n]} \ \eta\left(\phi[n], \boldsymbol{\xi}_t[n], \mathbf{B}[n-1]\right). \quad (31)$$

This subproblem is more difficult to solve due to the implicit expression for $\Theta_k(\phi)$. Fortunately, we can provide the monotonicity and concavity of $\Theta_k(\phi)$ in the following lemma.

Lemma 1: $\Theta_k(\phi)$ is a monotonically decreasing function and also is a convex function of ϕ.

Proof: The proof is given in Appendix A. ■

We take the first derivative of η in (27) on ϕ and formulate $\frac{\partial \eta}{\partial \phi}$ as

$$\frac{\partial \eta}{\partial \phi} = \sum_{k=1}^{K} \frac{e^{-\frac{\xi_{t,k}}{\varsigma_k \rho_u}} \Psi_k(\phi)}{\ln 2 \cdot \tau(\phi)\left(1+\tau(\phi)\varepsilon_k\xi_{t,k}\right)^{M-1}}, \quad (32)$$

where $\Psi_k(\phi)$ is expressed by

$$\Psi_k(\phi) = -\frac{\Theta_k^{'}(\phi)\tau(\phi)}{1+\Theta_k(\phi)} - \frac{(M-K)\tau(\phi)\xi_{t,k}}{\varsigma_k\rho} \ln\left(\frac{1+\xi_{t,k}}{1+\Theta_k(\phi)}\right) - \frac{(M-K)\tau(\phi)\varepsilon_k\xi_{t,k}}{1+\tau(\phi)\varepsilon_k\xi_{t,k}} \ln\left(\frac{1+\xi_{t,k}}{1+\Theta_k(\phi)}\right). \quad (33)$$

Aided by the monotonicity of $\tau(\phi)$, $\Theta_k(\phi)$, and $\Theta_k^{'}(\phi)$, it is not hard to find that $\Psi_k(\phi)$ is a decreasing function of ϕ. Given the constraint $\Theta_k(\phi) \leq \xi_{t,k}$, the feasible region of ϕ in (33) is $[\phi_k^\circ, \infty)$[2], where ϕ_k° is the solution of ϕ satisfying $F_{\gamma_e}(\xi_{t,k}) = 1-\delta_k$. Since $\Psi_k(\phi_k^\circ) > 0$ and $\Psi_k(\infty) < 0$ hold true, $\Psi_k(\phi)$ is first positive and then negative. That is, there exists a unique root of $\Psi_k(\phi) = 0$, and we refer to it as ϕ_k^*. As such, for different $\Psi_k(\phi)$, we can obtain an optimal set $\boldsymbol{\phi} = \{\phi_1^*, \phi_2^*, \cdots, \phi_K^*\}$. By respectively defining $\phi_{\min}$ and $\phi_{\max}$ as the minimum element and maximum element of $\boldsymbol{\phi}$, we state that η is an increasing function when $\phi < \phi_{\min}$, but a decreasing function when $\phi > \phi_{\max}$. Therefore, the optimal ϕ maximizing η, e.g., ϕ^*, must lie in the region of $[\phi_{\min}, \phi_{\max}]$. However, it is difficult to characterize the monotonicity of η in this region, and we directly use a one-dimensional search to find ϕ^*. Since the search space has been significantly reduced, we highlight that using the one-dimensional search method is reasonable and efficient.

In this way, the optimal $\phi[n]$ subject to $\boldsymbol{\xi}_t[n]$ and $\mathbf{B}[n-1]$ can be determined. By using the relationship between $\xi_{e,k}$ and ϕ, e.g., $\xi_{e,k} = \Theta_k(\phi)$, the optimal $\boldsymbol{\xi}_e[n]$ can also be together determined after some algebraic manipulations.

[1]The condition $\phi \leq 1$ ensures that $\rho_v \leq \rho_u$ holds true, thus limiting the artificial noise leaked into the legitimate users. As such, we clarify that $\phi \leq 1$ is a reasonable choice for the secure transmission design.

[2]We temporarily put the constraint $\phi \leq 1$ aside to ease the difficulty of finding solution, and we alternatively impose this constraint on the final solution, such that $\phi \leq 1$ still holds true.

3) Subproblem 3: In the n-th iteration, we finally optimize $\mathbf{B}[n]$ subject to $\phi[n]$ and $\boldsymbol{\xi}_t[n]$ by considering the following problem

$$\max_{\mathbf{B}[n]} \ \eta\left(\mathbf{B}[n], \boldsymbol{\xi}_t[n], \phi[n]\right). \tag{34}$$

To solve the problem in (34), we adopt a continuous relaxation technique to relax the integer constraint. However, this relaxed problem is not always a convex optimization problem, which is easy to find by deriving the second-order derivative of η on B_k. Although the globally optimal solution can be obtained by the exhaustive search method, the computational complexity would significantly increase with B_{total}. In what follows, we show that we can determine a local optimum by solving its Lagrange dual problem with an efficient algorithm.

Specifically, the Lagrange function of the problem in (34) is expressed by

$$L(\mathbf{B}, \mu) = \sum_{k=1}^{K} \frac{\Lambda_k}{\left(1+\tau(\phi)\xi_{t,k}\varepsilon_k\right)^{M-1}} - \mu\left(\sum_{k=1}^{K} B_k - B_{\text{total}}\right), \tag{35}$$

where

$$\Lambda_k = e^{-\frac{\xi_{t,k}}{\varsigma_k \rho_u}} \log_2\left(\frac{1+\xi_{t,k}}{1+\Theta_k(\phi)}\right), \tag{36}$$

and $\mu \geq 0$ is the nonnegative Lagrange multiplier associated with the constraint on the total feedback bits. Then the dual problem of (34) can be defined as

$$\min_{\mu \geq 0} g(\mu), \tag{37}$$

where

$$g(\mu) = \max_{\mathbf{B}} G(\mathbf{B}, \mu) + \mu B_{\text{total}}, \tag{38}$$

and

$$G(\mathbf{B}, \mu) = \sum_{k=1}^{K} \left(\frac{\Lambda_k}{\left(1+\tau(\phi)\xi_{t,k}\varepsilon_k\right)^{M-1}} - \mu B_k\right). \tag{39}$$

To solve this dual problem, we iteratively apply the following Step 1 and Step 2 until a pre-specified convergence criterion is met.

Step 1: The first step is to solve the problem in (38) with a given μ. By relaxing $\{B_k\}$ to the continuous variables, we find that the optimal $\{B_k\}$ can be obtained by using the conventional method of calculating the maximum of a continuous differential function.

Step 2: The second step is to update the value of μ by using the results obtained in **Step 1** and solving the dual problem in (37). If $\sum_{k=1}^{K} B_k > B_{\text{total}}$, μ should be increased; If $\sum_{k=1}^{K} B_k \leq B_{\text{total}}$, μ should be decreased. This update procedure builds on the monotonicity of $\sum_{k=1}^{K} B_k$ relative to μ, which is proved in ***Lemma* 2**.

***Lemma** 2:* For the problem in (38), the sum feedback $\sum_{k=1}^{K} B_k$ is a monotonically decreasing function of μ.

Proof: The proof is given in Appendix B. ∎

In conclusion, a two-step iterative algorithm can be developed to solve the dual problem in (37), which is summarized in **Algorithm 1**.

Algorithm 1 A Two-Step Iterative Algorithm for Solving the Dual Problem in (37).

1: Initialize $\mu_{\min} = 0$ and $\mu_{\max} = 1$.
2: Given $\mu = \mu_{\max}$, determine $\mathbf{B} = \arg\max_{\mathbf{B}} G(\mathbf{B}, \mu_{\max})$.
3: **while** $\sum_{k=1}^{K} B_k > B_{\text{total}}$ **do**
4: $\quad \mu_{\max} = 2\mu_{\max}$.
5: $\quad$ Given $\mu = \mu_{\max}$, determine $\mathbf{B} = \arg\max_{\mathbf{B}} G(\mathbf{B}, \mu_{\max})$.
6: **end while**
7: Set the accuracy tolerance $\epsilon_\mu > 0$.
8: **while** $|\mu_{\max} - \mu_{\min}| > \epsilon_\mu$ **do**
9: $\quad \mu = (\mu_{\min} + \mu_{\max})/2$.
10: $\quad$ Given μ, determine $\mathbf{B} = \arg\max_{\mathbf{B}} G(\mathbf{B}, \mu_{\max})$.
11: $\quad$ Check $\sum_{k=1}^{K} B_k$: If $\sum_{k=1}^{K} B_k > B_{\text{total}}$, set $\mu_{\min} = \mu$; If otherwise, set $\mu_{\max} = \mu$.
12: **end while**
13: Output $\mu_{\max}$ and $\mathbf{B}$.

This algorithm starts by finding the upper bound on μ, e.g., $\mu_{\max}$. Typically, this procedure can be completed within a few iterations and has a negligible impact on the computational complexity of this algorithm. In fact, the complexity mainly results from the bisection method for searching the optimal μ to ensure that the feedback constraint is tight. Given the accuracy ϵ_μ, this bisection search requires $\log_2(\mu_{\max}/\epsilon_\mu)$ iterations. Moreover, in each iteration K evaluations are required to obtain the local optimal $\mathbf{B}$. As such, the total complexity of **Algorithm 1** is $\mathcal{O}(K \cdot \log_2(\mu_{\max}/\epsilon_\mu))$. Aided by this algorithm, we clarify that $\mathbf{B}[n]$ can be optimized subject to the fixed $\phi[n]$ and $\boldsymbol{\xi}_t[n]$.

Based on the above analysis to the three subproblems, a BCD algorithm can be developed to iteratively optimize $\{\boldsymbol{\xi}_t\}$, $\{\phi, \boldsymbol{\xi}_e\}$, and $\{\mathbf{B}\}$, which is summarized in **Algorithm 2**.

Algorithm 2 The BCD Algorithm for Solving ***Problem** 2*.

1: Initialize $\phi[1]$, $\mathbf{B}[1]$, $\boldsymbol{\xi}_t[1]$, and $\boldsymbol{\xi}_e[1]$.
2: Set $n = 1$ and the accuracy tolerance $\epsilon_\eta > 0$.
3: Calculate $\eta[1]$.
4: **repeat**
5: $\quad n = n + 1$.
6: $\quad$ Given $\phi[n-1]$, $\boldsymbol{\xi}_e[n-1]$, and $\mathbf{B}[n-1]$, determine the optimal $\boldsymbol{\xi}_t[n]$ maximizing η.
7: $\quad$ Given $\boldsymbol{\xi}_t[n]$ and $\mathbf{B}[n-1]$, determine the optimal $\phi[n]$ and $\boldsymbol{\xi}_e[n]$ maximizing η.
8: $\quad$ Given $\phi[n]$, $\boldsymbol{\xi}_e[n]$, and $\boldsymbol{\xi}_t[n]$, determine the optimal $\mathbf{B}[n]$ by using **Algorithm 1**.
9: **until** Convergence: $|\eta[n] - \eta[n-1]| < \epsilon_\eta$.
10: Output.

The convergence of **Algorithm 2** can be proved by using the Bolzano-Weierstrass theorem [38], and the detailed proof is presented in the following proposition.

***Proposition** 1:* The solution generated by **Algorithm 2** is a stationary point of the optimization problem in ***Problem** 2*.

Proof: The proof is given in Appendix C. ∎

In the following, we provide the complexity analysis for this algorithm. Specifically, the computational complexity of **Algorithm 2** contains three parts, e.g., searching the optimal $\boldsymbol{\xi}_t$, searching the optimal ϕ, and searching the optimal $\mathbf{B}$. For each part, the worst case is that the optimum is obtained via the bisection search of K iterations. Assuming that the number of needed iterative steps for **Algorithm 2** is L, the total computational complexity of this algorithm is $\mathcal{O}(L \cdot K \cdot \log_2((\xi_{t,\max}/\epsilon_\xi)(\phi_{\max}/\epsilon_\phi)(\mu_{\max}/\epsilon_\mu)))$, where $\xi_{t,\max}$ and $\phi_{\max}$ are the preset search bound, and ϵ_ξ and ϵ_ϕ are the preset accuracy tolerance, respectively.

C. One-Dimensional Search for Finding the Optimal M

We clarify that M is a crucial parameter that plays an important role on the secrecy performance in the IoT scenario. On one hand, a small M means that only a small fraction of beams can be used for sending AN to confuse the eavesdroppers, implying that the eavesdroppers' reception cannot be effectively inhibited. On the other hand, a larger M may not necessarily bring the benefits on secrecy performance. To be specific, increasing M means that the CSIT becomes rather imprecise, which makes the amount of interference leakage becomes larger, severely degrading the IoT users' reception. Moreover, a very large M potentially wastes the network communication resources.

Since M has a major impact on the network secrecy performance, in this subsection we concentrate on the second problem, e.g., finding the optimal M maximizing η over its feasible region. Specifically, we formulate the optimization problem in the second step as follows.

***Problem** 3:* What is the optimal M that maximizes η under the given secrecy outage constraints? This problem is mathematically expressed as

$$\max_{M} \quad \eta(M, \phi_{\text{opt}}, \mathbf{B}_{\text{opt}}, \boldsymbol{\xi}_{t,\text{opt}}, \boldsymbol{\xi}_{e,\text{opt}}), \tag{40a}$$

$$\text{s.t.} \quad M \geq K. \tag{40b}$$

Here, ϕ_{opt}, $\mathbf{B}_{\text{opt}}$, $\boldsymbol{\xi}_{t,\text{opt}}$, and $\boldsymbol{\xi}_{e,\text{opt}}$ can be obtained via solving ***Problem** 2*. However, since ϕ_{opt}, $\mathbf{B}_{\text{opt}}$, $\boldsymbol{\xi}_{t,\text{opt}}$, and $\boldsymbol{\xi}_{e,\text{opt}}$ are not explicit functions of M, we clarify that ***Problem** 3* is a typical non-linear integer problem and difficult to handle. Fortunately, since the number of transmit antennas at the central controller is optimizing variable, the search space of this problem is quite limited. For example, to ensure an efficient use of the transmit antennas, the upper bound on M is generally less than $N = 10K$. Therefore, an exhaustive search is computationally tractable, such that we directly apply the one-dimensional search method to solve this problem.

Based on the above analysis for ***Problem** 2* and *3*, we have developed an efficient method involving the BCD algorithm and the one-dimensional search to solve ***Problem** 1*. Aided by the complexity analysis for **Algorithm 1**, we state that the total computational complexity of our proposed method is $\mathcal{O}(N \cdot L \cdot K \cdot \log_2((\xi_{t,\max}/\epsilon_\xi)(\phi_{\max}/\epsilon_\phi)(\mu_{\max}/\epsilon_\mu)))$.

VI. Numerical Results

In this section, numerical results are provided to illustrate the convergence of our proposed BCD algorithm, the optimal number of transmit antennas maximizing the network secrecy throughput, as well as the feedback bits allocation law among the heterogeneous IoT users. Unless otherwise stated, in the following we set the transmit power as $\rho = 20$ dB and set the path loss exponent as $\alpha = 4$. Moreover, we set the accuracy tolerance parameters in Algorithm 1 and 2, e.g., ϵ_μ, ϵ_η, ϵ_ξ, and ϵ_ϕ, as $\epsilon_\mu = \epsilon_\eta = \epsilon_\xi = \epsilon_\phi = 10^{-6}$. We also clarify that the following simulations are only for the single-tone transmission with a small number of IoT users. Through a straightforward extension, it is easy to obtain the multi-tone simulation with a large number of IoT users. Due to the space limitations, the multi-tone simulation is omitted in this work.

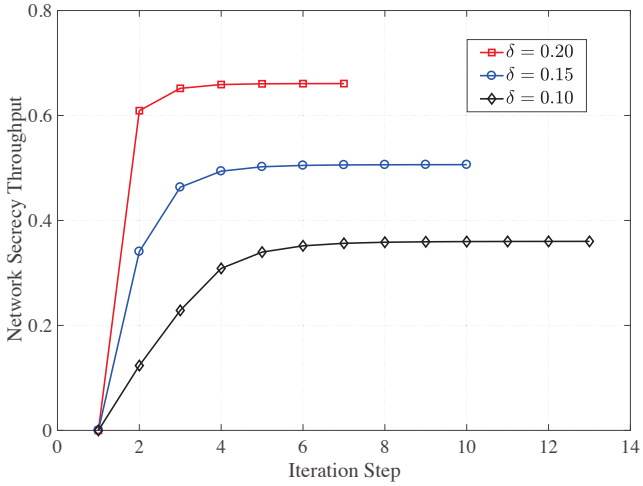

Fig. 3. The convergence rate of the BCD algorithm in a homogeneous scenario for $M = 16$, $K = 10$, $B_{\text{total}} = 200$, and $\lambda = 0.01$.

A. Convergence

Since our designed BCD algorithm is crucial to determine the optimal system parameters maximizing the network secrecy throughput, in this subsection we firstly examine its practicality by illustrating the convergence rate of this BCD algorithm in Figs. 3 and 4.

Specifically, we first provide Fig. 3 to depict the convergence rate of our proposed BCD algorithm in a homogeneous network, where all the IoT users are assumed to experience the same path loss coefficient and secrecy outage constraint, e.g., $\varsigma_1 = \varsigma_2 = \cdots = \varsigma_K = 1$, and $\delta_1 = \delta_2 = \cdots = \delta_K = \delta$. We first observe that for different values of δ, the iteration steps are generally small, which highlights the efficiency of this BCD algorithm. Furthermore, we observe that the iteration steps are directly related to the value of δ. For example, when $\delta = 0.2$, this algorithm requires 7 iteration steps; When $\delta = 0.1$, this algorithm requires 13 iteration steps. This indicates that when the secrecy outage constraint becomes stricter, our designed BCD algorithm needs more iteration steps.

To illustrate the convergence rate of our proposed BCD algorithm in the heterogeneous networks, we then provide Fig. 4 by randomly generating 50 system topologies where different users experience different path loss coefficients and secrecy outage constraints. We observe from this figure that the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2825483, IEEE Journal on Selected Areas in Communications

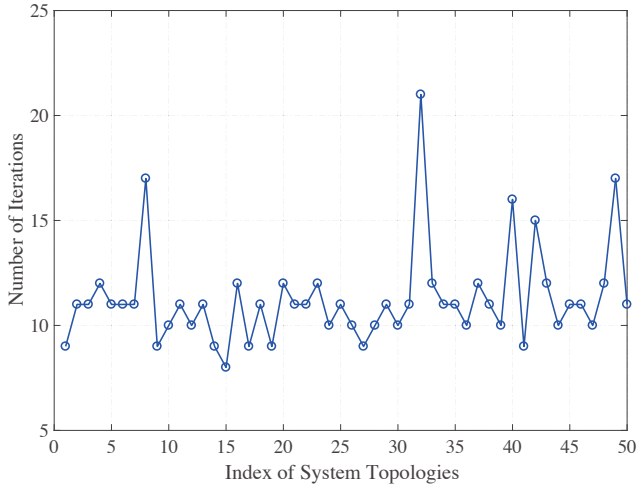

Fig. 4. The required number of iterations of the BCD algorithm in 50 randomly-selected system topologies for $M = 16$, $K = 10$, $B_{\text{total}} = 200$, and $\lambda = 0.01$.

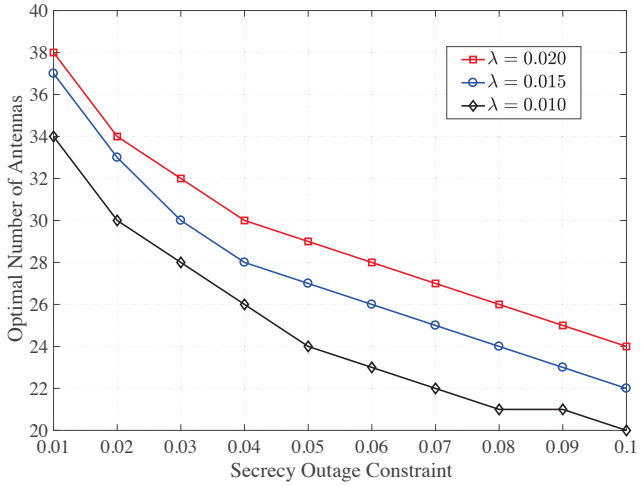

Fig. 6. The optimal number of transmit antennas versus the secrecy outage constraint for $K = 15$ and $B_{\text{total}} = 200$.

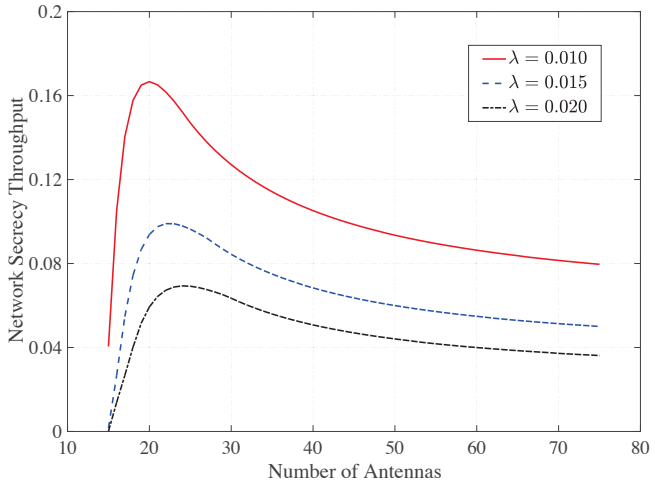

Fig. 5. The network secrecy throughput versus the number of transmit antennas for $K = 15$, $B_{\text{total}} = 200$, and $\delta = 0.1$.

maximum number of iteration steps is 21, and for most cases our proposed BCD algorithm converges within 15 steps. Fig. 4 highlights that our designed BCD algorithm can also converge very fast in the heterogeneous scenarios, which validates its practicality and generality on determining the optimal system parameters for secure transmission.

B. Optimal Number of Transmit Antennas

In this subsection, we focus on the homogeneous network and intend to illustrate the existence of the optimal number of transmit antennas, and investigate the impact of the secrecy outage constraint and the sum feedback bits constraint on the optimal number of transmit antennas.

Fig. 5 plots the maximum network secrecy throughput versus the number of transmit antennas for different values of λ. We clarify that the maximum network secrecy throughput with a fixed M, e.g., η_M, is obtained by applying our designed BCD algorithm. We first observe that η_M first increases then decreases as M increases, indicating that there exists an optimal M maximizing η_M. This phenomenon can be explained as follows. When M is relatively small, increasing M means more AN beams can be used for confusing eavesdroppers, thus leading to a higher η_M. However, when M is very large, this freedom advantage is outweighed by the interference leakage resulting from the limited feedback resources. To be specific, increasing M means the CDI quantization at each IoT user becomes more inaccurate, which consequently makes interference leakage problem become worse and thus degrades the reception performance of IoT users. We further observe that the maximum η_M decreases as λ increases, which is not surprising since the eavesdropping ability increases with λ. This figure highlights that the number of transmit antennas should be carefully optimized.

Fig. 6 plots the optimal number of transmit antennas versus the secrecy outage constraint for different values of λ. We clarify that the optimal number of transmit antennas, e.g., M_{opt}, is determined by using the BCD-based one-dimensional search method. We first observe that for a fixed λ, M_{opt} decreases as δ increases. This is because when δ becomes looser, using fewer AN beams can still keep the secrecy outage meeting its requirement, making possible to reduce the number of transmit antennas. We also observe that for a fixed δ, M_{opt} increases as λ increases. This is because when λ increases, more transmit antennas should be utilized for sending AN beams to confuse the eavesdroppers. This figure highlights that when the eavesdropping scenario becomes worse, e.g., a smaller δ or a lager λ, we need to increase the number of transmit antennas for secure transmission.

Fig. 7 plots the optimal number of transmit antennas versus the sum feedback bits constraint for different values of λ. We observe that for a fixed λ, M_{opt} decreases as B_{total} increases. This phenomenon can be explained as follows. When B_{total} is relatively small, the CDI quantization error at each IoT user is particularly serious. To avoid too much interference incurred

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JSAC.2018.2825483, IEEE Journal on Selected Areas in Communications

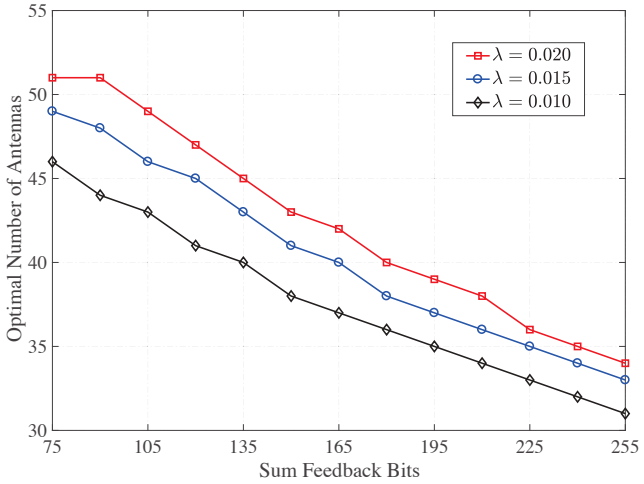

Fig. 7. The optimal number of transmit antennas versus the sum feedback bits constraint for $K = 15$ and $\delta = 0.01$.

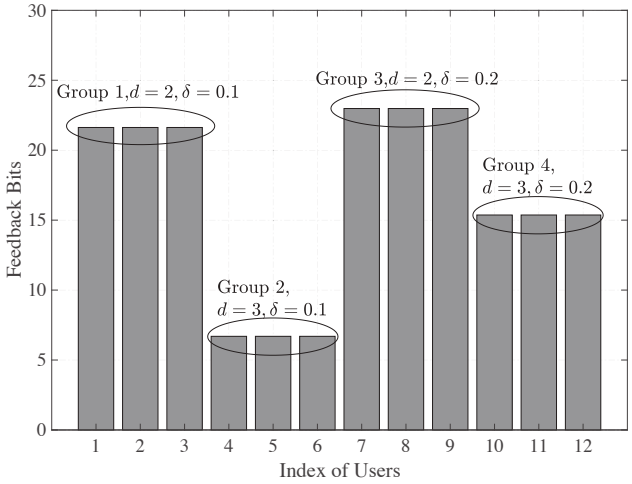

Fig. 8. The feedback bits allocation among the heterogeneous users for $K = 12$, $B_{\text{total}} = 200$, and $\lambda = 0.01$.

from the AN beams affecting the reception at the IoT users, it is necessary to reduce the transmit power allocated to the AN beams. In this case, to satisfy the pre-set secrecy outage constraint, more AN beams should be used to confuse the eavesdroppers' reception. As such, more transmit antennas are needed when B_{total} is small. This figure highlights that in the IoT scenario, we can utilize more transmit antennas for secure transmission to compensate the disadvantage of limit feedback resources.

C. Feedback Bits Allocation Law

Due to the equal status of each user in the homogeneous network, it is easy to find that under our proposed secure transmission design, the total feedback resources would be averagely distributed to all the IoT users. However, since in the heterogeneous network different users may experience different path loss coefficients and secrecy outage constraints, how to allocate the limited feedback resources among different users would have a major impact on the network secrecy performance. In this subsection, we aim to show the feedback bits allocation law under our secure transmission design.

Fig. 8 shows the optimal feedback bits allocation among the heterogeneous users with different path loss coefficients and secrecy outage constraints. We clarify that this figure is obtained together with the optimal number of transmit antennas by applying our proposed BCD-based one-dimension search method. In this figure, we provide four groups of users with different parameter settings, e.g., d and δ. Here, d denotes the distance between the user with the central controller, such that a larger d means a smaller path loss coefficient. It can be seen from this figure that for the users with the same path loss coefficient, e.g., Group 1 and 3, the users with looser secrecy outage constraint should use large shares of feedback resources. Moreover, for the users with the same secrecy outage constraint, e.g., Group 1 and 2, the users with larger path loss coefficient should use large shares of feedback resources. Therefore, we conclude that to obtain good network secrecy performance, the feedback bits allocation law is to allow the IoT users with looser secrecy outage constraint and larger path loss coefficient to share large shares of feedback resources.

VII. Conclusions

In this work, we concentrated on designing the IoT downlink secure transmission scheme. Constrained by the limited feedback resources, we designed an on-off-based multiuser secure transmission scheme and derived the closed-form expression for the network secrecy throughput. Then we proposed a BCD-based one-dimensional search method to optimize the number of transmit antennas, the wiretap codes, the power allocation ratio, and the feedback bits allocation strategy for maximizing the network secrecy throughput. Numerical results demonstrated that the optimal number of transmit antennas really exists, and this optimal antenna number tends to be larger when the IoT users need higher secrecy requirements, or the IoT network possesses scarcer feedback resources.

Appendix A
Proof of Lemma 1

To simplify the following notations, in this proof we omit ϕ from $\Theta_k(\phi)$. Since Θ_k is defined as $\Theta_k = F_{\gamma_e}^{-1}(1-\delta_k)$, we have

$$\Omega_1(\Theta_k, \phi) + C_k = 0 \tag{41}$$

where

$$\Omega_1(\Theta_k, \phi) = (1 + \phi\Theta_k)^{M-K}(\Theta_k/\rho_u)^{\beta}, \tag{42}$$

and $C_k = \chi/\ln(1-\delta_k)$. Using the derivative rule for implicit functions, we first derive the first-order derivative of Θ_k on ϕ as

$$\Theta_k^{'} = -\frac{\partial\Omega_1/\partial\phi}{\partial\Omega_1/\partial\Theta_k} = -\frac{(M-K)\Theta_k \mathrm{T}(\Theta_k, \phi)}{K + (M-K)\phi}, \tag{43}$$

where

$$\mathrm{T}(\Theta_k,\phi)=1+\frac{K\Theta_k}{(M-K)\phi\Theta_k+\beta(1+\phi\Theta_k)}. \tag{44}$$

It is obvious to find that $\Theta_k^{'}\leq 0$ always holds true, such that Θ_k is a decreasing function of ϕ. To characterize the concavity of Θ_k, we further need to examine the monotonicity of $\mathrm{T}(\Theta_k,\phi)$ relative to ϕ. In order to achieve this, we define $\mathrm{A}_k=\phi\Theta_k$ and characterize its monotonicity relative to ϕ. In particular, by substituting A_k into (41), we have

$$\Omega_2\left(\mathrm{A}_k,\phi\right)+C_k=0, \tag{45}$$

where

$$\Omega_2(\mathrm{A}_k,\phi)=(1+\mathrm{A}_k)^{M-K}\left(\frac{\mathrm{A}_k}{\phi\rho_u}\right)^{\beta}. \tag{46}$$

Similar to (43), we derive the the first-order derivative of A_k on ϕ as

$$\mathrm{A}_k^{'}=\frac{\beta K\mathrm{A}_k(1+\mathrm{A}_k)}{\phi(K+(M-K)\phi)((M-K+1)\mathrm{A}_k+1)}. \tag{47}$$

Since $\mathrm{A}_k^{'}>0$ always holds true, A_k is an increasing function of ϕ, implying that $\mathrm{T}(\Theta_k,\phi)$ decreases with the increase of ϕ. Aided by the monotonicity of Θ_k and $\mathrm{T}(\Theta_k,\phi)$, we conclude that $\Theta_k^{''}>0$ must hold true, i.e., Θ_k is a convex function of ϕ, which completes our proof.

APPENDIX B
PROOF OF LEMMA 2

Consider two Lagrangian multipliers μ_a and μ_b, satisfying $\mu_a\leq\mu_b$. Given μ_a and μ_b, we denote the corresponding optimal $\mathbf{B}$ maximizing $G(\mathbf{B},\mu)$ as $\mathbf{B}_a=\{B_k^a\}$ and $\mathbf{B}_b=\{B_k^b\}$, respectively. We define

$$A=G(\mathbf{B}_a,\mu_a) \tag{48a}$$
$$\hat{A}=G(\mathbf{B}_b,\mu_a) \tag{48b}$$
$$B=G(\mathbf{B}_b,\mu_b) \tag{48c}$$
$$\hat{B}=G(\mathbf{B}_a,\mu_b). \tag{48d}$$

Due to the optimality of $\mathbf{B}_a$ maximizing $G(\mathbf{B},\mu_a)$ and the optimality of $\mathbf{B}_b$ maximizing $G(\mathbf{B},\mu_b)$, we have $A\geq\hat{A}$ and $B\geq\hat{B}$. Moreover, by observing (39), we find that $\mu_a\leq\mu_b$ leads to $\hat{A}\geq B$. As such, we have the following relationship

$$A\geq\hat{A}\geq B\geq\hat{B}. \tag{49}$$

Note that (49) implies $A-\hat{B}\geq\hat{A}-B$, yielding

$$(\mu_b-\mu_a)\sum_{k=1}^{K}B_k^a\geq(\mu_b-\mu_a)\sum_{k=1}^{K}B_k^b. \tag{50}$$

Based on (50), we conclude that subject to $\mu_a\leq\mu_b$, $\sum_{k=1}^{K}B_k^a\geq\sum_{k=1}^{K}B_k^b$ holds true. That is, a larger μ leads to a smaller sum feedback consumption, e.g., $\sum_{k=1}^{K}B_k$. Therefore, we state that $\sum_{k=1}^{K}B_k$ is a decreasing function of μ.

APPENDIX C
PROOF OF PROPOSITION 1

By relaxing $\{B_k\}$ to continuous variables, we find from (25a) and (25b) that the objective function is continuously differentiable, and the feasible set is closed, nonempty, and convex. Since $\eta(\phi,\mathbf{B},\boldsymbol{\xi}_t,\boldsymbol{\xi}_e)$ is bounded, we learn from the Bolzano-Weierstrass theorem that as long as $\eta(\phi,\mathbf{B},\boldsymbol{\xi}_t,\boldsymbol{\xi}_e)$ is a monotonically nondecreasing function, the optimization variables (e.g., ϕ, $\mathbf{B}$, $\boldsymbol{\xi}_t$, and $\boldsymbol{\xi}_e$) must have limit points. That is, it is necessary to firstly prove the relationship given by

$$\begin{aligned}&\eta(\phi[n],\mathbf{B}[n],\boldsymbol{\xi}_t[n],\boldsymbol{\xi}_e[n])\\&\geq\eta(\phi[n-1],\mathbf{B}[n-1],\boldsymbol{\xi}_t[n-1],\boldsymbol{\xi}_e[n-1]).\end{aligned} \tag{51}$$

We note that (51) is easy to obtain by using the properties of the saddle points, yielding

$$\begin{aligned}&\eta(\phi[n],\mathbf{B}[n],\boldsymbol{\xi}_t[n],\boldsymbol{\xi}_e[n])\\&\geq\eta(\phi[n],\mathbf{B}[n],\boldsymbol{\xi}_t[n-1],\boldsymbol{\xi}_e[n])\\&\geq\eta(\phi[n-1],\mathbf{B}[n],\boldsymbol{\xi}_t[n-1],\boldsymbol{\xi}_e[n-1])\\&\geq\eta(\phi[n-1],\mathbf{B}[n-1],\boldsymbol{\xi}_t[n-1],\boldsymbol{\xi}_e[n-1]).\end{aligned} \tag{52}$$

According to the Corollary 2 concluded in [38], every limit point obtained by **Algorithm 2** is a stationary point of ***Problem 2***, which concludes our proof.

REFERENCES

[1] M. Shafi, A. F. Molisch, P. J. Smith, T. Haustein, P. Zhu, P. D. Silva, F. Tufvesson, A. Benjebbour, and G. Wunder, "5G: A tutorial overview of standards, trials, challenges, deployment, and practice," *IEEE J. Select. Areas Commun.*, vol. 35, no. 6, pp. 1201–1221, June 2017.

[2] Y. Mehmood, N. Haider, M. Imran, A. Timm-Giel, and M. Guizani, "M2M communications in 5G: State-of-the-art architecture, recent advances, and research challenges," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 194–201, Sep. 2017.

[3] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Commun. Surveys & Tutorials*, vol. 19, no. 2, pp. 855–873, 2nd Quart., 2017.

[4] J. Chen, K. Hu, Q. Wang, Y. Sun, Z. Shi, and S. He, "Narrowband Internet of Things: Implementations and applications," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 2309–2314, Dec. 2017.

[5] M. Elsaadany, A. Ali, and W. Hamouda, "Cellular LTE-A technologies for the future Internet of Things: Physical layer features and challenges," *IEEE Commun. Surveys & Tutorials*, vol. 19, no. 4, pp. 2544–2572, 4th Quart., 2017.

[6] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet of Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, May 2017.

[7] A. Mukherjee, "Physical-layer security in the Internet of things: Sensing and communication confidentiality under resource constraints," *Proc. IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct. 2015.

[8] W. Trappe, "The challenges facing physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, June 2015.

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

[10] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, Sep. 2013.

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

[12] S. Liu, Y. Hong, and E. Viterbo, "Artificial noise revisited," *IEEE Trans. Inf. Theory*, vol. 61, no. 7, pp. 3901–3911, July 2015.

[13] X. Zhang, M. R. McKay, X. Zhou, and R. W. Heath Jr., "Artificial-noise-aided secure multi-antenna transmission with limited feedback," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2742–2754, May 2015.

[14] H. Wang, C. Wang, and D. W. K. Ng, "Artificial noise assisted secure transmission under training and feedback," *IEEE Trans. Signal Process.*, vol. 63, no. 23, pp. 6285–6298, Dec. 2015.

[15] J. Hu, Y. Cai, N. Yang, X. Zhou, and W. Yang, "Artificial-noise-aided secure transmission scheme with limited training and feedback overhead," *IEEE Trans. Wireless Commun.*, vol. 16, no. 1, pp. 193–205, Jan. 2017.

[16] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H. H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surveys & Tutorials*, vol. 19, no. 2, pp. 1027–1050, 2nd Quart., 2017.

[17] X. Chen and Y. Zheng, "Mode selection in MU-MOMO downlink networks: A physical-layer security perspective," *IEEE Syst. Journal*, vol. 11, no. 2, pp. 1128–1136, June 2017.

[18] G. Geraci, R. Couillet, J. Yuan, M. Debbah, and I. B. Collings, "Large system analysis of linear precoding in MISO broadcast channels with confidential messages," *IEEE J. Select. Areas Commun.*, vol. 31, no. 9, pp. 1660–1671, Sep. 2013.

[19] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, Sep. 2014.

[20] J. Zhu, R. Schober, and V. K. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2245–2261, Mar. 2016.

[21] L. Hu, H. Wen, B. Wu, F. Pan, R.-F. Liao, H. Song, J. Tang, and X. Wang, "Cooperative jamming for physical layer security enhancement in Internet of Things," *IEEE Internet Things J.*, accepted for publication.

[22] Y. J. Tolossa, S. Vuppala, and G. Abreu, "Secrecy-rate analysis in multi-tier heterogeneous networks under generalized fading model," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 101–110, Feb. 2017.

[23] Y.-P. E. Wang, X. Lin, A. Adhikary, A. Grövlen, Y. Sui, Y. Blankenship, J. Bergman, and H. S. Razaghi, "A primer on 3GPP narrowband Internet of Things," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 117–123, Mar. 2017.

[24] A. Höglund, X. Lin, O. Liberg, A. Behravan, E. A. Yavuz, M. V. D. Zee, Y. Sui, T. Tirronen, A. Ratilainen, and D. Eriksson, "Overview of 3GPP release 14 enhanced NB-IoT," *IEEE Network*, vol. 31, no. 6, pp. 16–22, Nov./Dec. 2017.

[25] H. Wang, X. Zhou, and M. C. Reed, "Physical layer security in cellular networks: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2776–2787, June 2013.

[26] G. Geraci, S. Singh, J. G. Andrews, J. Yuan, and I. B. Collings, "Secrecy rates in broadcast channels with confidential messages and external eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 13, no. 5, pp. 2931–2943, May 2014.

[27] C. Liu, N. Yang, R. Malaney, and J. Yuan, "Artificial-noise-aided transmission in multi-antenna relay wiretap channels with spatially random eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7444–7456, Nov. 2016.

[28] G. Chen, J. P. Coon, and M. D. Renzo, "Secrecy outage analysis for downlink transmissions in the presence of randomly located eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 5, pp. 2931–2943, May 2014.

[29] K. K. Mukkavilli, A. Sabharwal, E. Erkip, and B. Aazhang, "On beamforming with finite rate feedback in multiple-antenna systems," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2562–2579, Oct. 2003.

[30] D. J. Love, R. W. Heath Jr., and T. Strohmer, "Grassmannian beamforming for multiple-input multiple-output wireless systems," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2735–2747, Oct. 2003.

[31] T. Yoo, N. Jindal, and A. Goldsmith, "Multi-antenna downlink channels with limited feedback and user selection," *IEEE J. Select. Areas Commun.*, vol. 25, no. 7, pp. 1478–1491, Sep. 2007.

[32] N. Yang, G. Geraci, J. Yuan, and R. Malaney, "Confidential broadcasting via linear precoding in non-homogeneous MIMO multiuser networks," *IEEE Trans. Commun.*, vol. 62, no. 7, pp. 2515–2530, July 2014.

[33] T. Samarasinghe, H. Inaltekin, and J. S. Evans, "On the outage capacity of opportunistic beamforming with random user locations," *IEEE Trans. Commun.*, vol. 62, no. 8, pp. 3015–3026, Aug. 2014.

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

[35] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, June 2008.

[36] H. Wang, C. Wang, D. W. K. Ng, M. H. Lee, and J. Xiao, "Artificial noise assisted secure transmission for distributed antenna systems," *IEEE Trans. Signal Process.*, vol. 64, no. 15, pp. 4050–4064, Aug. 2016.

[37] D. P. Bertsekas, *Nonlinear Programming*. Belmont, MA, USA: Athena Scientific, 1999.

[38] L. Grippo and M. Sciandrone, "On the convergence of the block nonlinear Gauss-Seidel method under convex constraints," *Oper. Res. Lett.*, vol. 26, pp. 127–136, 2000.

Jianwei Hu (S'14) received the B.S. degree in communication engineering from the PLA Army Engineering University, Nanjing, China, in 2012. Since 2014, he has been pursuing the Ph.D. degree in communications and information system at the College of Communications Engineering, PLA Army Engineering University. His current research interests include physical layer security and Internet of Things (particular emphasis on designing secure transmission schemes in the Internet of Things).

Nan Yang (S'09–M'11) received the B.S. degree in electronics from China Agricultural University in 2005, and the M.S. and Ph.D. degrees in electronic engineering from the Beijing Institute of Technology in 2007 and 2011, respectively. He has been with the Research School of Engineering at the Australian National University since July 2014, where he currently works as a Future Engineering Research Leadership Fellow and a Senior Lecturer. Prior to this, he was a Postdoctoral Research Fellow at the University of New South Wales from 2012 to 2014 and a Postdoctoral Research Fellow at the Commonwealth Scientific and Industrial Research Organization from 2010 to 2012. He received the Exemplary Reviewer Award of the IEEE TRANSACTIONS ON COMMUNICATIONS in 2015 and 2016, the Top Reviewer Award from the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY in 2015, the IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award and the Exemplary Reviewer Award of the IEEE WIRELESS COMMUNICATIONS LETTERS in 2014, and the Exemplary Reviewer Award of the IEEE COMMUNICATIONS LETTERS in 2013 and 2012. He is also a co-recipient of the Best Paper Awards from the IEEE GlobeCOM 2016 and the IEEE VTC 2013-Spring. He is currently serving in the Editorial Board of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES. His general research interests lie in the areas of communications theory and signal processing, with specific interests in massive multi-antenna systems, millimeter wave communications, ultra-reliable low latency communications, cyber-physical security, and molecular communications.

Yueming Cai (M'05–SM'12) received his B.S. degree in Physics from Xiamen University, Xiamen, China in 1982, the M.S. degree in Micro-electronics Engineering and the Ph.D. degree in Communications and Information Systems both from Southeast University, Nanjing, China in 1988 and 1996 respectively. His current research interest includes MIMO systems, cooperative communications, D2D communications, and physical layer security.