Secure Transmission Design With Feedback Compression for the Internet of Things

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

***Abstract*—Physical layer security is an emerging technique to protect the wireless communications in the Internet of Things (IoT). Motivated by the fact that a single IoT terminal usually occupies a very small fraction of feedback resources, we propose a novel secure transmission design with feedback compression to improve the feedback resources utilization for secure communications. Specifically, we first introduce a multiperiod one-feedback (MPOF) scheme to exploit the channel temporal correlation existing in the IoT scenarios, making the IoT terminal convey its channel knowledge to the central controller in a more efficient manner. Under this MPOF scheme, we then put forward a virtual quantizer model and design a generalized fixed-rate secure ON–OFF transmission scheme, where the central controller adaptively adjusts the transmission parameters in one feedback interval. By averaging the total secrecy throughput of one feedback interval over all the coherence periods thereof, we further characterize the secrecy throughput of our proposed transmission scheme and facilitate the joint optimization design of the feedback interval length, the wiretap codes, and the power allocation ratios. To handle this nonconvex problem, we develop an efficient approach involving the block coordinate descent algorithm and the 1-D search method. Numerical results show that when the channel temporal correlation is high, our proposed secure transmission design achieves a significantly higher secrecy throughput than the conventional design constrained by the same amount of feedback resources.**

***Index Terms*—Internet of things, secure transmission design, feedback compression, virtual quantization.**

I. Introduction

THE rapid growth in wireless data usage and wireless connectivity poses a huge burden on existing cellular networks and triggers the next major evolution in wireless communications, e.g., the fifth generation (5G) wireless, which is expected to envision magnitudes of increase in data rates and connectivity, along with a significant decrease in end-to-end latency and energy consumption [1]. As 5G wireless communications hold the potential to support an enormous number of connected devices, the Internet of Things (IoT) is recognized as one of the emerging applications that could be eventually realized with the development of 5G technologies [2].

The IoT enables any physical device with processing, computing and sensorial capabilities to see, hear, think and perform tasks by connecting it to the Internet via heterogeneous access networks [3], [4]. This ubiquitous connectivity of IoT forms the basic architecture of 5G networks [5]. Over time, the IoT is expected to involve a wide range of public and private sectors (e.g., agriculture, transportation, healthcare, and smart homes), transforming the human-centric communications to machine-centric communications [6]. Such a revolutionary change will no doubt be a great tribute to the quality of our work and life.

A. Security for the Internet of Things

It is anticipated that the IoT would encompass private, commercial, financial, and military applications. Any disclosure of these sensitive information (e.g., personal privacy, trade secrets, financial files, and military secrets) is bound to bring serious consequences. Therefore, security is a fundamental enabling factor in the IoT, and appropriate mechanisms need to be established for secure communications in the context of IoT [7]. It is noted that the large number of IoT devices generally have limited hardware and significant energy constraints. For these devices, the most computation and energy should be used for executing core application and therefore, there may be little left for supporting security [8]. Traditional cryptographic methods need to consume a giant amount of communication resources for key distribution and management, and thus being inappropriate for securing the IoT.

Against this background, the physical layer security technique becomes a promising alternative to provide security for the IoT [9], [10]. Different from cryptographic technologies implemented at upper layers, physical layer security can achieve confidentiality by exploring the randomness nature at the physical layer. Rather than consuming some communication resources for setting up encrypted protocols amongst legitimate entities, physical layer security guarantees the message confidentiality via channel coding techniques. Therefore, it provides a standalone security solution without secret key distribution and management. The seminal work in physical layer security can be traced back to Wyner, who proposed the fundamental

Manuscript received April 3, 2017; revised August 8, 2017 and October 15, 2017; accepted December 2, 2017. Date of publication December 18, 2017; date of current version February 7, 2018. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Rui Zhang. The work of J. Hu was supported by the China Scholarship Council (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 (e-mail: nan.yang@anu.edu.au).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSP.2017.2784412

wiretap model and clarified that perfect secrecy is available without a shared secret key [11]. Since then, numerous studies have focused on the design of signal processing methods to enhance physical layer security, e.g., transmit beamforming [12], [13], cooperation techniques [14], [15], and artificial-noise-aided transmission [16], [17]. Most of these studies have a common assumption, e.g., the channel state information (CSI) of the legitimate receiver and/or the eavesdropper is perfectly known at the transmitter. However, this dependence on the perfect CSI at the transmitter (CSIT) is a recognized obstacle to implement physical layer security in some emerging wireless applications. Coincidentally, the IoT is such an application. Specifically, due to the limited feedback resources imposed by enormous IoT devices, the CSIT is rather imprecise in the IoT scenarios, which usually leads to a significant degradation on the achievable secrecy performance. Therefore, to deploy physical layer security in the IoT scenarios, it is necessary to design a secure transmission scheme that satisfies the feedback constraints while is also capable of achieving good secrecy performance.

B. Related Work

In the literature, several studies have investigated the secure transmission design with limited feedback overhead. Using the artificial-noise-aided beamforming scheme, [18] investigated the impact of quantized channel feedback on the achievable secrecy rate for multiple antenna wiretap channels, while [19] optimized the transmission to guarantee secrecy with quantized channel feedback in Rayleigh fading channels. For the block fading channels, [20] and [21] examined the non-trivial tradeoff between the feedback overhead and the effective communication resources for secure data transmission. These studies demonstrated that the limited feedback overhead leads to a significant decrease in the secrecy performance.

Note that the aforementioned studies [18]–[21] have adopted a common assumption, e.g., the independent block fading channels, which ignores the possible channel temporal correlation among adjacent channel blocks [22], [23]. However, there generally exists high channel temporal correlation in the IoT scenarios, since the IoT devices usually stay still or move slowly. Fortunately, this high channel temporal correlation is probably not a bad thing. In particular, a good correlation means that the channel experiences a slow change, such that there is no need for the receiver to frequently feed back its channel knowledge to the transmitter. In other words, the channel temporal correlation provides the possibility to more efficiently utilize the feedback resources via using the feedback compression technique [24]. Motivated by this, in this work we aim to design a secure transmission scheme for the IoT with feedback compression, aiming to achieve secrecy performance improvements without consuming extra feedback resources.

C. Our Contributions

In this work, we consider the downlink transmission from the multi-antenna controller to a single-antenna actuator in a local IoT scenario. The information flow from the transmitter to the legitimate receiver is overheard by the randomly located single-antenna eavesdroppers. By exploiting the benefits of channel temporal correlation, we provide an artificial-noise-aided secure ON-OFF transmission design with more productive utilization of the feedback resources. Compared to our existing work [21], the key contributions of this work are summarized as the following three aspects:

1) Different from the independent block fading assumption in [21], we integrate the channel temporal correlation into our secure transmission design to improve the feedback resources utilization for secrecy performance enhancement, thus applying to the IoT scenarios. In particular, the multi-period one-feedback (MPOF) scheme is proposed to permit only one feedback for multiple coherence periods, which facilitates a more efficient use of the feedback resources.
2) We extend the fixed-rate secure transmission design in [21] to a more generalized scenario. Since the MPOF scheme leads to the CSIT increasingly outdated with channel evolution, we need to individually construct wiretap codes for the different coherence periods of one feedback interval. We highlight that this challenging task is successfully solved via establishing a virtual quantizer model that converts the channel temporal correlation into equivalent quantization bits.
3) We develop a new framework to characterize the secrecy throughput of our designed transmission scheme, by averaging the total secrecy throughput over the number of coherence periods in one feedback interval. Since maximizing this secrecy throughput is a mixed integer nonlinear programming problem and difficult to handle, we solve this optimization problem in two steps. For the first step, a block coordinate descent (BCD) algorithm is provided to determine the optimal wiretap codes and power allocation ratios while fixing the feedback interval length. And for the second step, the optimal feedback interval length is solved by a one-dimensional search.

Numerical results demonstrate that compared to the conventional scheme, our secure transmission design can achieve a higher secrecy throughput by integrating the feedback resources of multiple coherence periods. Or rather, in achieving the same secrecy throughput, our secure transmission design requires fewer feedback resources for CSIT acquisition when the channel temporal correlation is good.

D. Organizations

The rest of this paper is organized as follows. In Section II, we introduce the considered system model and present the basic principle of the MPOF scheme. In Section III, we put forward a virtual quantizer model for the following theoretic analysis. In Sections IV and V, we provide the secure ON-OFF transmission design and characterize the maximization of the secrecy throughput. Finally, we give our numerical simulations in Section VI and conclude in Section VII.

Notation: Matrices and column vectors are denoted by uppercase and lowercase boldface letters. A circularly symmetric complex Gaussian random variable z with variance σ^2 is

denoted as $z \sim \mathcal{CN}(0, \sigma^2)$. A Exponent-distributed random variable x with parameter t is denoted as $x \sim \mathrm{Exp}(t)$. A Gamma-distributed random variable y with parameters (a, b) is denoted as $y \sim \mathrm{Gamma}(a, b)$. $|\cdot|$ and $\|\cdot\|$ represent the norm of scalar and vector, respectively. $\log_2(\cdot)$ and $\ln(\cdot)$ represent the base 2 logarithm and natural logarithm, respectively.

II. System Model

We consider the typical IoT downlink transmission from the central controller (Alice) to a legitimate actuator (Bob) in the presence of randomly located single-antenna passive eavesdroppers (Eves). We assume that Alice is equipped with M antennas ($M > 1$), while Bob only has a single antenna. We model the eavesdroppers' locations to be distributed on the infinite two-dimensional plane according to a homogeneous Poisson point process (PPP) Φ of intensity λ. Given that an individual IoT device can only hold a tiny trickle of feedback resources, in this work we aim to design a new secure transmission scheme with feedback compression to improve the feedback resources utilization on secure communications.

Throughout this paper, we refer to the Alice-Bob link as the main channel and the Alice-Eve link as the eavesdropper's channel. We assume a flat-varying rich-scattering environment. Under this assumption, the channel coefficients in the main and the eavesdropper's channels are independent identically distributed (i.i.d) complex Gaussian random variables with zero mean and unit variance during a specific coherence period. For the k-th coherence period, we denote $h_{i,k} \sim \mathcal{CN}(0, 1)$ as the channel coefficient between the i-th transmit antenna at Alice and the single received antenna at Bob, which facilitates us to denote $\mathbf{h}_k = [h_{1,k}, h_{2,k}, \ldots, h_{M,k}]$ as the main channel vector. As such, the received symbol at Bob is expressed by

$$y_k = \sqrt{d_b^{-\alpha}}\mathbf{h}_k \mathbf{x}_k + n_k, \tag{1}$$

where d_b denotes the distance between Alice and Bob, α denotes the path-loss exponent, $\mathbf{x}_k$ denotes the symbol vector sent from Alice, and $n_k \sim \mathcal{CN}\left(0, \sigma_b^2\right)$ denotes the additive white Gaussian noise (AWGN) at Bob. Moreover, we denote $g_{i,j,k} \sim \mathcal{CN}(0, 1)$ as the channel coefficient between the i-th transmit antenna at Alice and the j-th Eve, which facilitates us to denote $\mathbf{g}_{j,k} = [g_{1,j,k}, g_{2,j,k}, \ldots, g_{M,j,k}]$ as the j-th eavesdropper's channel vector. Therefore, the received symbol at the j-th Eve is expressed by

$$z_{j,k} = \sqrt{d_j^{-\alpha}}\mathbf{g}_{j,k} \mathbf{x}_k + w_{j,k}, \tag{2}$$

where d_j denotes the distance between Alice and the j-th Eve, and $w_{j,k} \sim \mathcal{CN}\left(0, \sigma_e^2\right)$ denotes the AWGN at the j-th Eve.

To concentrate on improving the efficiency of feedback resources for secure communications, in this work we assume that there is no channel estimation errors at Bob and Eves. That is, Bob has perfect knowledge about $\mathbf{h}_k$, while the j-th Eve has perfect knowledge about $\mathbf{g}_{j,k}$. Moreover, we consider that Alice is able to acquire partial knowledge about $\mathbf{h}_k$ with the help of a feedback controller at Bob. However, since the eavesdroppers perform as passive users (i.e., there are no reverse links between Alice and Eves), Alice cannot obtain any instantaneous knowledge about $\mathbf{g}_{j,k}$ from the j-th Eve.

In previous studies, the independent block fading channel model is often assumed for the simplicity of analysis, where each channel realization remains constant in one block and different realizations are independent. However, this assumption is unrealistic in the IoT scenarios, where the temporally-correlated channels are the norm cases. That is, there exists high channel correlation in the IoT scenarios. Motivated by this, in this work we focus on exploiting the channel temporal correlation to compress the feedback overhead for CSIT acquisition, which makes possible designing secure transmission schemes for the IoT with secrecy performance improvements. In particular, we model the time evolution of the main channel by a first-order Gauss-Markov process [25]

$$\mathbf{h}_k = \rho \mathbf{h}_{k-1} + \sqrt{1-\rho^2}\mathbf{e}_k, \tag{3}$$

where ρ quantifies the amount of the correlation between the elements of $\mathbf{h}_k$ and $\mathbf{h}_{k-1}$, and $\mathbf{e}_k$ is a random vector, whose entries are i.i.d complex Gaussian random variables with zero mean and unit variance.

A. MPOF Scheme

It is well known that by utilizing the channel knowledge at Alice, the physical layer can provide great secrecy performance. In practice, acquiring the channel knowledge at Alice is not easy, and the common method is to employ a reverse channel link. Specifically, at each coherence period Alice first sends a sequence of training symbols to help Bob perform estimation of $\mathbf{h}_k$. After this process, Bob obtains the channel direction information (CDI), e.g., $\mathbf{d}_k = \mathbf{h}_k / \|\mathbf{h}_k\|$, which plays a crucial role for the signal design at Alice side. However, due to the constrained rate of the practical reverse link, Alice can only typically learn about the partial knowledge of $\mathbf{d}_k$ with a small amount of feedback overhead.

In conventional feedback scheme, Bob performs CDI quantization and feeds back his quantized information to Alice using a small number of feedback bits at every coherence period. Although this scheme is easy to be used, it ignores the benefits of feedback compression in temporally correlated channels. From this perspective, we redesign the CDI feedback scheme for secure transmission by taking account of the channel temporal correlation. Aided by [26], we put forward a novel feedback scheme (e.g., the MPOF scheme) to help Bob convey back his quantized CDI for Alice's secure transmission design. As illustrated in Fig. 1, in this MPOF scheme the CDI feedback link is only active at the nT-th coherence period. Here, T is referred to as the length of feedback interval, and n is a non-negative integer. In particular, at the nT-th coherence period Bob selects the optimal quantized CDI vector from a 2^{B_0}-sized codebook $\mathcal{B}_0 = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_{2^{B_0}}\}$ known a prior at Alice and Bob, yielding

$$\mathbf{c}_n = \underset{\mathbf{b}_i \in \mathcal{B}_0}{\arg\max} |\mathbf{d}_{nT} \mathbf{b}_i^{\dagger}|^2. \tag{4}$$

Then Bob informs Alice of the index of $\mathbf{c}_n$ by using B_0 feedback bits. For the following $T-1$ coherence periods, the CDI

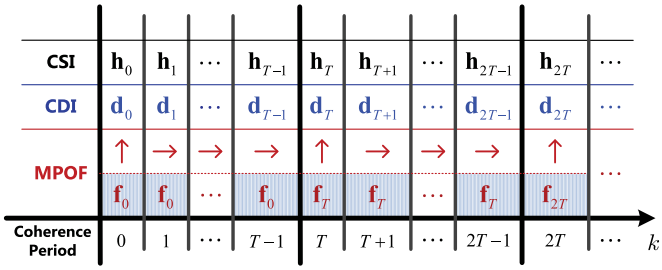

Fig. 1. MPOF scheme: Up arrow (↑) is used to indicate the event that the CDI feedback link is active, while horizontal arrow (→) is used to indicate the event that the CDI feedback link is inactive.

feedback link is inactive, such that the side channel knowledge known at Alice cannot obtain a real-time update. That is, $\mathbf{c}_n$ is the only CDI available at Alice during the periods ranging from $k = nT$ to $k = (n+1)T - 1$, and Alice has to reuse $\mathbf{c}_n$ for data transmission until Bob sends back the index of $\mathbf{c}_{n+1}$ at the $(n+1)T$-th coherence period.

This MPOF scheme is actually an feedback compression scheme, and the average feedback overhead of the MPOF scheme is B_0/T bits/channel use. Here, we clarify that for this MPOF scheme, the T coherence periods in one feedback interval should be regarded as a whole to carry on the analysis. As such, in the following we typically investigate the secure transmission design for the first feedback interval, including the coherence periods ranging from $k = 0$ to $k = T - 1$.

B. Artificial-Noise-Aided Beamforming Scheme

Since we consider the passive eavesdropping scenario, the instantaneous eavesdropper's channel knowledge is unknown to Alice. Under this scenario, the artificial-noise-aided beamforming scheme is often applied for secure communications [19]–[21]. Specifically, at the 0-th coherence period, Alice generates an $M \times M$ precoding matrix as $\mathbf{W}_0 = [\mathbf{f}_0, \mathbf{F}_0]$, where $\mathbf{f}_0 = \mathbf{c}_0^\dagger$, and the columns of $\mathbf{F}_0$ form an orthonormal basis for the null space of $\mathbf{c}_0$.

For the coherence periods ranging from $k = 0$ to $k = T - 1$, the $M \times 1$ transmitted symbol vector $\mathbf{x}_k$ at Alice is designed as $\mathbf{x}_k = \mathbf{f}_0 u_k + \mathbf{F}_0 \mathbf{v}_k$, where u_k is the information-bearing signal, and $\mathbf{v}_k$ is the artificial noise. The variance of u_k is $P_{u,k}$, and the $M-1$ elements of $\mathbf{v}_k$ are i.i.d complex Gaussian random variables with zero mean and variance $P_{v,k}$. By applying this artificial-noise-aided beamforming design, the received symbols at Bob and the j-th Eve in the k-th coherence period become

$$y_k = \sqrt{d_b^{-\alpha}}\mathbf{h}_k\mathbf{f}_0 u_k + \sqrt{d_b^{-\alpha}}\mathbf{h}_k\mathbf{F}_0\mathbf{v}_k + n_k \tag{5}$$

and

$$z_{j,k} = \sqrt{d_j^{-\alpha}}\mathbf{g}_{j,k}\mathbf{f}_0 u_k + \sqrt{d_j^{-\alpha}}\mathbf{g}_{j,k}\mathbf{F}_0\mathbf{v}_k + w_{j,k}, \tag{6}$$

respectively. We consider a power constraint denoted by $P = P_{u,k} + (M-1)P_{v,k}$, and define the power allocation ratio between $P_{u,k}$ and $P_{v,k}$ as $\phi_k = P_{v,k}/P_{u,k}$, such that we have $P_{u,k} = P\varphi_k$ and $P_{v,k} = P\varphi_k\phi_k$, where $\varphi_k = \frac{1}{1+(M-1)\phi_k}$. We clarify that ϕ_k (or φ_k) acts as an important transmission parameter to guarantee good secrecy performance.

III. Virtual Quantization

In this section, we first review the frequently-used design criterion for the optimization of quantization codebook. By combining this criterion with the MPOF scheme, we successfully transform the channel temporal correlation as a virtual reverse feedback link, which enables us to perform the secure transmission design under the MPOF scheme.

A. Quantization Cell Approximation

In the literature, the optimization of quantization codebook $\mathcal{B}$ has been thoroughly studied. Albeit starting from different perspectives, [27] and [28] presented the same criterion for optimal codebook design, i.e., minimizing the maximum correlation between any pair of beamforming vectors. This design problem is actually well known in applied mathematics as the Grassmannian line packing problem [29], [30]. Mathematically, by modeling the codebook $\mathcal{B}$ as a collection of lines in the Euclidean space $\mathbb{C}^M$, the optimal codebook is equivalent to

$$\mathcal{B}_{\text{opt}} = \min_{\mathcal{B}\in\mathbb{C}^{M\times 2^B}} \max_{1\le i<j\le 2^B} D(\mathbf{b}_i, \mathbf{b}_j), \tag{7}$$

where B is the number of quantization bits, $D(\mathbf{b}_i, \mathbf{b}_j) = \cos^2(\theta_{i,j})$, and $\theta_{i,j}$ is the angle between the two lines generated by $\mathbf{b}_i$ and $\mathbf{b}_j$.

However, the design of optimal or near-optimal Grassmannian line packings is usually a challenging problem and can only be numerically determined in general. To further examine the quantization performance, [29], [31] introduced an approximate method to characterize the codebook generated by this criterion. This approximation ideally assumes that each quantization cell can be viewed as a Voronoi region of a spherical cap. In particular, given the designed codebook $\mathcal{B}$, the actual quantization cell

$$\mathcal{R} = \left\{\mathbf{d} : |\mathbf{d}\mathbf{b}_i^\dagger|^2 \ge |\mathbf{d}\mathbf{b}_j^\dagger|, \forall j \ne i\right\} \tag{8}$$

is approximated as

$$\mathcal{R} = \left\{\mathbf{d} : |\mathbf{d}\mathbf{b}_i^\dagger|^2 \ge 1 - \varepsilon\right\}, \tag{9}$$

where $\varepsilon = 2^{-\frac{B}{M-1}}$. The above quantization cell approximation has been widely used as a valid performance indicator for the well-designed codebook.

B. Virtual Quantizer Model

In this work, we also adopt this quantization cell approximation to perform analytical characterization. Specifically, at the 0-th coherence period, Bob performs CDI quantization by selecting the optimal vector from the designated codebook $\mathcal{B}_0$, i.e., $\mathbf{c}_0 = \arg\max_{\mathbf{b}_i\in\mathcal{B}_0} |\mathbf{d}_0\mathbf{b}_i^\dagger|^2$. If we define $\cos^2\theta_0 = |\mathbf{d}_0\mathbf{c}_0^\dagger|^2$, the cumulative distribution function (CDF) of $\cos^2\theta_0$ is approximated as [21, Eq. (6)]

$$F_{\cos^2\theta_0}(x) = \begin{cases} 0, & 0 \le x < 1-\varepsilon_0, \\ 1 - (\frac{1-x}{\varepsilon_0})^{M-1}, & 1-\varepsilon_0 \le x \le 1, \end{cases} \tag{10}$$

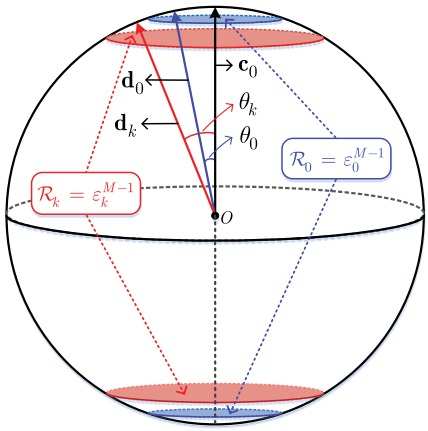

Fig. 2. The illustration of the virtual quantizer's quantization error increasing with the evolution of the main channel.

where $\varepsilon_0 = 2^{-\frac{B_0}{M-1}}$ denotes the maximum quantization error of using codebook $\mathcal{B}_0$.

In the MPOF scheme, $\mathbf{c}_0$ is used to perform data transmission during the T coherence periods of one feedback interval. Since there exists the temporal correlation between $\mathbf{h}_0$ and $\mathbf{h}_k$ $(1 \le k \le T-1)$, we believe that $\mathbf{c}_0$ is not independent of $\mathbf{d}_k$. That is, despite that for the following $T-1$ periods Bob does not perform the real-time quantization, we can still view $\mathbf{c}_0$ as a virtual output of Bob's quantizing $\mathbf{d}_k$ with a reduced-resolution codebook, as shown in Fig. 2. Since the output of this virtual quantizer is restricted to be $\mathbf{c}_0$, this virtual quantization is different from the real-time quantization. Admittedly, when the time-evolution error is large, it is not always the best option to quantize $\mathbf{d}_k$ as $\mathbf{c}_0$. However, since the temporal correlation in the IoT scenarios is typically high, the probability of the output of our virtual quantization being $\mathbf{c}_0$ is actually substantial. Based on this nature, we approximate the CDF of $\cos^2\theta_k = |\mathbf{d}_k\mathbf{c}_0^\dagger|^2$ as the similar form with (10)

$$F_{\cos^2\theta_k}(x) = \begin{cases} 0, & 0 \le x < 1-\varepsilon_k, \\ 1-(\frac{1-x}{\varepsilon_k})^{M-1}, & 1-\varepsilon_k \le x \le 1. \end{cases} \tag{11}$$

Here, the maximum quantization error of this virtual quantizer is facilitated as $\varepsilon_k = 2^{-\frac{B_k}{M-1}}$, where B_k denotes the number of the virtual quantization bits. The following lemma characterizes the mathematical relationship between ε_k and ε_0.

Lemma 1: The parameter ε_k in (11) is formulated as

$$\varepsilon_k = 1 - \rho^{2k}(1-\varepsilon_0). \tag{12}$$

Proof: The proof is given in Appendix A. ■

Aided by (11), we successfully establish a framework to model the channel temporal correlation as a virtual quantizer. That is, although we adopt the MPOF scheme for CSIT acquisition, we can still think that there always exists a quantizer available at Bob. However, the quantization performance of this virtual quantizer gradually decreases in one feedback interval, indicated by (12). We highlight that this virtual quantizer acts as an important analyzing tool for us to design the secure transmission scheme with feedback compression.

IV. Secure Transmission Design

In this section, we attempt to design an ON-OFF-based secure transmission scheme that applies to the MPOF scheme. Specifically, aided by the statistical characterizations for the received signal-to-interference-plus-noise ratios (SINRs) in the main and eavesdropping channels, we first propose a generalized fixed-rate secure ON-OFF transmission design, and then develop the closed-form expression for the secrecy throughput under our designed secure transmission scheme.

A. Statistical Characterization of the SINRs

In preparation for the secure transmission design, we first focus on characterizing the statistics of the received SINRs at Bob and Eves.

1) The Received SINR at Bob: Based on (5), the actual instantaneous received SINR at Bob during the k-th coherence period is given by

$$\gamma_{b,k} = \frac{P_b\varphi_k|\mathbf{h}_k\mathbf{f}_0|^2}{P_b\varphi_k\phi_k\|\mathbf{h}_k\mathbf{F}_0\|^2+1}, \tag{13}$$

where $P_b = Pd_b^{-\alpha}/\sigma_b^2$. By substituting $|\mathbf{d}_k\mathbf{f}_0|^2 = \cos^2\theta_k$ and $\|\mathbf{d}_k\mathbf{F}_0\|^2 = \sin^2\theta_k$ into (13), we rewrite $\gamma_{b,k}$ as

$$\gamma_{b,k} = \frac{P_b\varphi_k\|\mathbf{h}_k\|^2\cos^2\theta_k}{P_b\varphi_k\phi_k\|\mathbf{h}_k\|^2\sin^2\theta_k+1}. \tag{14}$$

Using the method presented in [21], [31], we derive the CDF of $\gamma_{b,k}$ as

$$F_{\gamma_{b,k}}(x) = \begin{cases} F_1(x), & x \ge \hat{\Psi}_{t,k}, \\ F_2(x), & x < \hat{\Psi}_{t,k}, \end{cases} \tag{15}$$

where

$$F_1(x) = 1 - \beta_k^{M-1}e^{-\frac{x}{P_b\varphi_k}}, \tag{16}$$

and

$$F_2(x) = F_X(\zeta_k) - \beta_k^{M-1}e^{-\frac{x}{P_b\varphi_k}}F_Y(\zeta_k). \tag{17}$$

Here, $\hat{\Psi}_{t,k} = \frac{1-\varepsilon_k}{\varepsilon_k\phi_k}$, $\beta_k = \frac{1}{\varepsilon_k(1+\phi_k x)}$, $\zeta_k = \frac{x/(P_b\varphi_k)}{1-\varepsilon_k-\varepsilon_k\phi_k x}$, $X \sim \mathrm{Gamma}(M-1,1)$, and $Y \sim \mathrm{Gamma}(M-1,\beta_k)$. By taking the second-order derivative, it is easy to find that $F_1(x)$ is a concave function, while $F_2(x)$ is a convex function in the region of $[0,\tilde{\Psi}_{t,k})$ but a concave function in the region of $(\tilde{\Psi}_{t,k},\hat{\Psi}_{t,k})$, where $\tilde{\Psi}_{t,k}$ is the inflection point of $F_2(x)$ and can be numerically determined. These facts can be observed in Fig. 3, which illustrates $F_{\gamma_{b,k}}(x)$ for different values of ϕ_k.

2) The Received SINRs at Eves: Based on (6), the actual instantaneous received SINR at the j-th Eve during the k-th coherence period is expressed by

$$\gamma_{j,k} = \frac{P_e\varphi_k|\mathbf{g}_{j,k}\mathbf{f}_0|^2}{P_e\varphi_k\phi_k\|\mathbf{g}_{j,k}\mathbf{F}_0\|^2+d_j^\alpha}, \tag{18}$$

where $P_e = P/\sigma_e^2$, $|\mathbf{g}_{j,k}\mathbf{f}_0|^2 \sim \mathrm{Exp}(1)$, and $\|\mathbf{g}_{j,k}\mathbf{F}_0\|^2 \sim \mathrm{Gamma}(M-1,1)$. Conditioned on the fixed ϕ_k and $d_j^{-\alpha}$, the

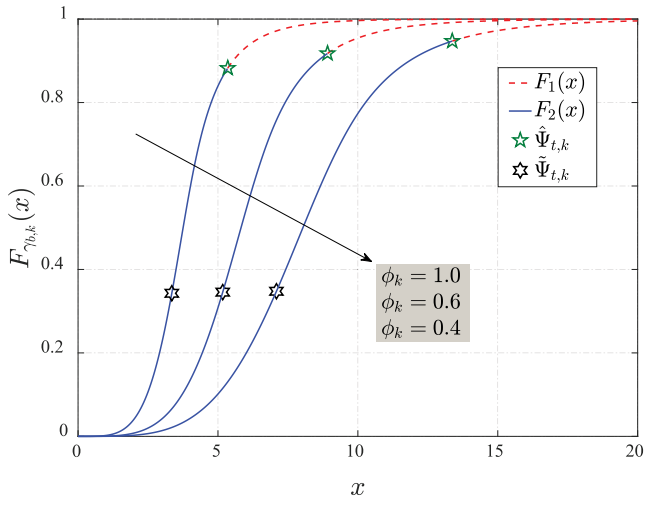

Fig. 3. The CDF of $\gamma_{b,k}$ with $M = 4$, $B_k = 8$, and $P_b = 10$.

CDF of $\gamma_{j,k}$ is derived as

$$F_{\gamma_{j,k}}\left(x|d_j^{-\alpha}\right) = 1 - (1+\phi_k x)^{1-M} e^{-\frac{x d_j^{\alpha}}{P_e \varphi_k}}. \tag{19}$$

Note that the eavesdropper with maximum received SINR has the strongest eavesdropping ability, such that we need to characterize the statistic of $\gamma_{e,k} = \max_{j\in\Phi} \gamma_{j,k}$. In particular, we use the mathematical method proposed in [32] and derive the CDF of $\gamma_{e,k}$ as

$$F_{\gamma_{e,k}}(x) = e^{-\frac{\chi \varphi_k^{\mu}}{x^{\mu}(1+\phi_k x)^{M-1}}}, \tag{20}$$

where $\mu = 2/\alpha$, and $\chi = \lambda\pi\Gamma(\mu+1) P_e^{\mu}$.

B. Wiretap Codes Design

To perform the secure communications, the crucial thing is to determine suitable values for the wiretap code parameters, e.g., the codeword transmission rate R_t and the rate redundancy R_e, respectively [11]. Since the CSIT varies with channel evolution in one feedback interval, we need to construct two code parameter vectors, e.g., $\mathbf{R}_t = [R_{t,1}, R_{t,2}, \ldots, R_{t,T}]$ and $\mathbf{R}_e = [R_{e,1}, R_{e,2}, \ldots, R_{e,T}]$. That is, T sets of code pair $(R_{t,k}, R_{e,k})$ should be designed. We clarify that the T sets of code pair hold constant across the whole transmission and apply to each feedback interval. For the convenience of following derivations, we denote $R_{t,k}$ and $R_{e,k}$ by $R_{t,k} = \log_2(1+\Psi_{t,k})$ and $R_{e,k} = \log_2(1+\Psi_{e,k})$, respectively.

It is worth mentioning that if we focus on one feedback interval, our transmission design looks like an adaptive-rate scheme. However, if we take one feedback interval as a unit and examine this design over the whole transmission process, it is indeed a fixed-rate scheme. Or rather, it is a generalized fixed-rate scheme. We highlight that this generalized fixed-rate design still has the advantage of low complexity and thus suitably applies to the IoT scenarios.

C. Secure ON–OFF Scheme

Under this generalized fixed-rate design, the ON-OFF scheme is a natural choice to perform secure transmission. Therefore, we apply the ON-OFF scheme into our considered scenario by only allowing the message transmission to happen when the legitimate channel capacity exceeds the predetermined codeword transmission rate. In particular, for the k-th coherence period, the transmission probability is facilitated as

$$p_{\mathrm{tm},k} = \Pr\{C_{b,k} \geq R_{t,k}\}, \tag{21}$$

where $C_{b,k} = \log_2(1+\gamma_{b,k})$ is the Bob's channel capacity in the k-th coherence period. Aided by the CDF of $\gamma_{b,k}$ in (15), the transmission probability of the k-th coherence period is derived as

$$p_{\mathrm{tm},k} = \begin{cases} 1 - F_1(\Psi_{t,k}), & \Psi_{t,k} \geq \hat{\Psi}_{t,k}, \\ 1 - F_2(\Psi_{t,k}), & \Psi_{t,k} < \hat{\Psi}_{t,k}. \end{cases} \tag{22}$$

We clarify that in each coherence period Bob needs to convey back an extra bit to identify the ON/OFF state of the transmission. However, compared to the feedback bits for CDI quantization, this 1-bit overhead is so small that it is omitted in this work.

Since we consider the passive eavesdropping scenario, the perfect secrecy cannot be guaranteed all the time. When the transmission condition is met and yet the designed rate redundancy falls below the channel capacity of the strongest eavesdropper, the leakage of confidential information would occur. This is the so-called secrecy outage event, and the probability of this event, e.g., secrecy outage probability, is a widely used metric to characterize the security level [19], [21]. In this work, we express the secrecy outage probability of the k-th coherence period as

$$p_{\mathrm{so},k} = \Pr\{C_{e,k} \geq R_{e,k} | \text{transmission}\}, \tag{23}$$

where $C_{e,k} = \log_2(1+\gamma_{e,k})$ is the maximum Eve's channel capacity in the k-th coherence period. Due to the fixed-rate design in this work, it is easy to find that the secrecy outage event is actually independent of the transmission condition, such that (23) can be simply rewritten as $p_{\mathrm{so},k} = \Pr\{\gamma_{e,k} \geq \Psi_{e,k}\}$. Aided by the CDF of $\gamma_{e,k}$ in (19), we derive $p_{\mathrm{so},k}$ as

$$p_{\mathrm{so},k} = 1 - F_{\gamma_e}(\Psi_{e,k}) = 1 - e^{-\frac{\chi \varphi_k^{\mu}}{\Psi_{e,k}^{\mu}(1+\phi_k \Psi_{e,k})^{M-1}}}. \tag{24}$$

In the literature works, the secrecy throughput, defined as the average secrecy rate over all the channel realizations, is often taken as the optimization goal to optimize the code parameters, subject to a required secrecy outage probability [33]. For our considered scenario, the secrecy throughput of the k-th coherence period can be written as

$$\eta_k = p_{\mathrm{tm},k}(R_{t,k} - R_{e,k}). \tag{25}$$

However, for the T coherence periods of one feedback interval, different coherence periods have different secrecy throughput performance. As such, the secrecy throughput of our newly designed secure transmission scheme should be redefined by averaging the total secrecy throughput of one feedback interval

over T coherence periods, yielding

$$\eta_{\mathrm{mpof}} = \frac{1}{T}\sum_{k=0}^{T-1}\eta_k = \frac{1}{T}\sum_{k=0}^{T-1} p_{\mathrm{tm},k}(R_{t,k} - R_{e,k}). \tag{26}$$

In the following section, we focus on how to determine optimal T, $\mathbf{\Psi}_t = [\Psi_{t,1}, \Psi_{t,2}, \ldots, \Psi_{t,T}]$, $\mathbf{\Psi}_e = [\Psi_{e,1}, \Psi_{e,2}, \ldots, \Psi_{e,T}]$, and $\boldsymbol{\phi} = [\phi_1, \phi_2, \ldots, \phi_T]$ maximizing the secrecy throughput in (26) subject to a given secrecy outage constraint.

V. Secrecy Throughput Maximization

In this section, we demonstrate that the optimization problem of maximizing the secrecy throughput can be solved via two steps. Specifically, we first fix T and determine the corresponding optimal $\mathbf{\Psi}_t$, $\mathbf{\Psi}_e$, and $\boldsymbol{\phi}$ by designing a BCD algorithm. Then we develop a BCD-based one-dimensional search method to tackle the optimal T.

A. Problem Formulation

Problem 1: The joint optimization of T, $\mathbf{\Psi}_t$, $\mathbf{\Psi}_e$, and $\boldsymbol{\phi}$ maximizing the secrecy throughput under a given secrecy outage constraint can be formulated as

$$\max_{T,\mathbf{\Psi}_t,\mathbf{\Psi}_e,\boldsymbol{\phi}} \ \eta_{\mathrm{mpof}}(T, \mathbf{\Psi}_t, \mathbf{\Psi}_e, \boldsymbol{\phi}), \tag{27a}$$

$$\text{s.t.} \quad \mathbf{p}_{\mathrm{so}} \le \delta \cdot \mathbf{1}, \tag{27b}$$

$$\mathbf{\Psi}_t \ge \mathbf{\Psi}_e, \tag{27c}$$

where $\mathbf{p}_{\mathrm{so}} = [p_{\mathrm{so},1}, p_{\mathrm{so},2}, \ldots, p_{\mathrm{so},T}]$, and δ denotes the required secrecy outage constraint. We clarify that the constraint (27b) results from the secrecy outage requirement, and the constraint (27c) guarantees a positive secrecy rate.

Note that Problem 1 is a typical mixed integer nonlinear programming (MINLP) problem, and few effective algorithms can be used to efficiently solve it. To facilitate an effective method for handling this problem, in this work we carry on the following equivalent transformation

$$\max_{T,\mathbf{\Psi}_t,\mathbf{\Psi}_e,\boldsymbol{\phi}} \eta_{\mathrm{mpof}} \Leftrightarrow \max_{T} \max_{\mathbf{\Psi}_t,\mathbf{\Psi}_e,\boldsymbol{\phi}} \eta_{\mathrm{mpof}}. \tag{28}$$

This transformation implies that we can decompose the entire optimization into two steps: We maximize η_{mpof} by first maximizing over variables $\mathbf{\Psi}_t$, $\mathbf{\Psi}_e$, and $\boldsymbol{\phi}$ subject to a fixed T, and then over the integer variable T. In the following, we perform the optimization procedures step by step.

B. BCD Algorithm Design for Solving the First Problem

In the first step, we aim to address the following problem.

Problem 2: For a fixed T, what are the optimal $\mathbf{\Psi}_t$, $\mathbf{\Psi}_e$, and $\boldsymbol{\phi}$ that maximize η_{mpof} under a given secrecy outage constraint? This problem is formulated as

$$\max_{\mathbf{\Psi}_t,\mathbf{\Psi}_e,\boldsymbol{\phi}} \ \eta_{\mathrm{mpof}}(\mathbf{\Psi}_t, \mathbf{\Psi}_e, \boldsymbol{\phi}), \tag{29a}$$

$$\text{s.t.} \quad \text{(27b) and (27c)}. \tag{29b}$$

Before proceeding to solve Problem 2, we first transform the constraint in (27b) into a more explicit form. In particular, due to the monotonicity of $F_{\gamma_{e,k}}(x)$, we obtain

$$p_{\mathrm{so},k} \le \delta \Leftrightarrow \Psi_{e,k} \ge F^{-1}_{\gamma_{e,k}}(1-\delta), \tag{30}$$

where $F^{-1}_{\gamma_{e,k}}(\cdot)$ denotes the inverse function of $F_{\gamma_{e,k}}(\cdot)$. For ease of notation, we define $\Theta(\phi_k) = F^{-1}_{\gamma_{e,k}}(1-\delta)$.

Since $p_{\mathrm{tm},k}$ is independent of $\Psi_{e,k}$, (26) implies that to maximize η_{mpof}, $\Psi_{e,k}$ should be set to its minimum value, e.g., $\Psi_{e,k} = \Theta(\phi_k)$. Here, we clarify that although $\Theta(\phi_k)$ is an implicit function of ϕ_k, we can still calculate it by numerically searching the unique root of $F_{\gamma_{e,k}}(x) = 1-\delta$ subject to an arbitrary ϕ_k. As such, we simplify Problem 2 as

$$\max_{\mathbf{\Psi}_t,\boldsymbol{\phi}} \quad \eta_{\mathrm{mpof}}\left(\mathbf{\Psi}_t, \boldsymbol{\phi}, \mathbf{\Psi}_e = \Theta(\boldsymbol{\phi})\right), \tag{31a}$$

$$\text{s.t.} \quad \mathbf{\Psi}_t \ge \Theta(\boldsymbol{\phi}). \tag{31b}$$

Although this problem is simplified, it is still non-convex and difficult to address. In the following, we propose an efficient BCD algorithm to solve this joint optimization problem [20]. Specifically, we decouple all the optimization variables into two blocks, e.g., $\{\mathbf{\Psi}_t\}$ and $\{\boldsymbol{\phi}\}$, and alternatively optimize one block of variables by fixing the other block of variables at their values from the last iteration. Each iteration of the proposed algorithm involves solving two subproblems as follows.

1) Subproblem 1: In each iteration procedure, we first intend to optimize $\mathbf{\Psi}_t$ subject to $\boldsymbol{\phi}$ by considering the following problem

$$\max_{\mathbf{\Psi}_t} \ \eta_{\mathrm{mpof}}(\mathbf{\Psi}_t, \boldsymbol{\phi}). \tag{32}$$

By observing the expression for η_{mpof} in (26), we find that the maximization of η_{mpof} can be facilitated by respectively maximizing its general term, e.g., η_k. Moreover, in the term of η_k, $\Psi_{t,k}$ is merely coupled with ϕ_k, which implies that we only need to characterize the maximization of η_k to determine the optimal $\Psi_{t,k}$ with a fixed ϕ_k.

Note that (27c) leads to a natural constraint on $\Psi_{t,k}$, e.g., $\Psi_{t,k} \ge \Theta(\phi_k)$. In this subsection, we focus on the most complex case, e.g., $\Theta(\phi_k) < \tilde{\Psi}_{t,k}$, and discuss how to find the optimal $\Psi_{t,k}$ by dividing the feasible region of $\Psi_{t,k}$ into three parts, e.g., $[\Theta(\phi_k), \tilde{\Psi}_{t,k}]$, $[\tilde{\Psi}_{t,k}, \hat{\Psi}_{t,k}]$, and $[\hat{\Psi}_{t,k}, \in \infty)$. It is worth mentioning that other cases are simpler than this, and they can also be solved using the method presented below.

Considering the first region, e.g., $[\Theta(\phi_k), \tilde{\Psi}_{t,k}]$, the expression for η_k can be formulated as

$$\eta_k = \frac{1 - F_2(\Psi_{t,k})}{\ln 2} \ln\left(\frac{1+\Psi_{t,k}}{1+\Theta(\phi_k)}\right). \tag{33}$$

By taking the first-order derivative of η_k in (33) on $\Psi_{t,k}$, we formulate $A(\Psi_{t,k}) = \partial\eta_k / \partial\Psi_{t,k}$ as

$$A(\Psi_{t,k}) = -\frac{f_2(\Psi_{t,k})}{\ln 2}\ln\left(\frac{1+\Psi_{t,k}}{1+\Theta(\phi_k)}\right) + \frac{1 - F_2(\Psi_{t,k})}{\ln 2 \cdot (1+\Psi_{t,k})}, \tag{34}$$

where $f_2(\cdot)$ is the derivative function of $F_2(\cdot)$. Since $F_2(\cdot)$ is a convex function in the region of $[0, \tilde{\Psi}_{t,k}]$, we state that $f_2(\cdot)$ is an increasing function of $\Psi_{t,k}$. As such, the first term in the right-hand side (RHS) of (34) is a decreasing function of $\Psi_{t,k}$.

Aided by the monotonicity of the second term in the RHS of (34), we find that $A(\Psi_{t,k})$ is a decreasing function of $\Psi_{t,k}$ in the region of $[0, \tilde{\Psi}_{t,k}]$.

Note that $A(0) > 0$, but $A(\tilde{\Psi}_{t,k})$ varies. Under the case with $A(\tilde{\Psi}_{t,k}) \geq 0$, $A(\Psi_{t,k}) \geq 0$ always holds true, indicating that η_k monotonically increases with $\Psi_{t,k}$, and thus the maximum is achieved at $\Psi_{t,k} = \tilde{\Psi}_{t,k}$. Under the case with $A(\tilde{\Psi}_{t,k}) < 0$, $A(\Psi_{t,k})$ is first positive then negative, indicating that η_k first increases then decreases with $\Psi_{t,k}$, and thus the maximum is achieved at the unique root of $A(\Psi_{t,k}) = 0$. As such, in the region of $[0, \tilde{\Psi}_{t,k}]$, the optimal $\Psi_{t,k}$ maximizing η_k can be expressed by

$$\Psi_{t,k,1}^{\mathrm{opt}} = \begin{cases} \tilde{\Psi}_{t,k}, & A(\tilde{\Psi}_{t,k}) \geq 0, \\ \Psi_{t,k}^{\star}, & A(\tilde{\Psi}_{t,k}) < 0, \end{cases} \tag{35}$$

where $\Psi_{t,k}^{\star}$ satisfies $A(\Psi_{t,k}^{\star}) = 0$, and can be calculated by using the bisection method.

Considering the second region, e.g., $[\tilde{\Psi}_{t,k}, \hat{\Psi}_{t,k}]$, the expressions for η_k and $\partial\eta_k/\partial\Psi_{t,k}$ can also be formulated as (33) and (34), respectively. However, since $F_2(\cdot)$ becomes a concave function in the region of $[\tilde{\Psi}_{t,k}, \hat{\Psi}_{t,k}]$, the monotonicity of $A(\Psi_{t,k})$ is no longer easy to judge. In addition, the complicated expression for $A(\Psi_{t,k})$ makes it impossible to mathematically characterize its monotonicity. Fortunately, since the size of the second region is small, we can directly adopt the one-dimensional search method to determine the optimal $\Psi_{t,k}$ maximizing η_k, which is referred to as $\Psi_{t,k,2}^{\mathrm{opt}}$.

Considering the third region, e.g., $[\hat{\Psi}_{t,k}, \in \infty)$, the expression for η_k can be formulated as

$$\eta_k = \frac{1 - F_1(\Psi_{t,k})}{\ln 2} \ln\left(\frac{1 + \Psi_{t,k}}{1 + \Theta(\phi_k)}\right). \tag{36}$$

By taking the first-order derivative of η_k in (36) on $\Psi_{t,k}$, we formulate $B(\Psi_{t,k}) = \partial\eta_k/\partial\Psi_{t,k}$ as

$$B(\Psi_{t,k}) = -\frac{f_1(\Psi_{t,k})}{\ln 2} \ln\left(\frac{1 + \Psi_{t,k}}{1 + \Theta(\phi_k)}\right) + \frac{1 - F_1(\Psi_{t,k})}{\ln 2 \cdot (1 + \Psi_{t,k})}, \tag{37}$$

where $f_1(\cdot)$ is the derivative function of $F_1(\cdot)$. Aided by the expression for $F_1(\cdot)$ in (16), we can further derive (37) as

$$B(\Psi_{t,k}) = \frac{\varepsilon_k^{1-M} e^{-\frac{\Psi_{t,k}}{P_b \varphi_k}} H(\Psi_{t,k})}{\ln 2 \cdot (1 + \phi_k \Psi_{t,k})^M}, \tag{38}$$

where $H(\Psi_{t,k})$ is expressed by

$$H(\Psi_{t,k}) = \frac{1 + \phi_k \Psi_{t,k}}{1 + \Psi_{t,k}} - \frac{1 + \phi_k \Psi_{t,k}}{P_b \varphi_k} \ln\left(\frac{1 + \Psi_{t,k}}{1 + \Theta(\phi_k)}\right) - (M - 1)\, \phi_k \ln\left(\frac{1 + \Psi_{t,k}}{1 + \Theta(\phi_k)}\right). \tag{39}$$

Since the sign of $B(\Psi_{t,k})$ follows that of $H(\Psi_{t,k})$, the monotonicity of η_k can be examined by analyzing the sign of $H(\Psi_{t,k})$. Aided by (39), it is not hard to find that when $\phi_k \leq 1$ holds true,[1] $H(\Psi_{t,k})$ is a decreasing function of $\Psi_{t,k}$.

Note that $H(\in \infty) < 0$, but $H(\hat{\Psi}_{t,k})$ varies. If $H(\hat{\Psi}_{t,k}) \leq 0$, $H(\Psi_{t,k}) \leq 0$ always holds true, i.e., η_k monotonically decreases with $\Psi_{t,k}$, such that the maximum is achieved at $\Psi_{t,k} = \hat{\Psi}_{t,k}$. However, if $H(\hat{\Psi}_{t,k}) > 0$, $H(\Psi_{t,k})$ is first positive then negative. That is, η_k first increases then decreases with $\Psi_{t,k}$, and the maximum is achieved at the unique root of $H(\Psi_{t,k}) = 0$. As such, in the region of $[\hat{\Psi}_{t,k}, \in \infty)$, the optimal $\Psi_{t,k}$ maximizing η_k can be expressed by

$$\Psi_{t,k,3}^{\mathrm{opt}} = \begin{cases} \hat{\Psi}_{t,k}, & H(\hat{\Psi}_{t,k}) \leq 0, \\ \Psi_{t,k}^{*}, & H(\hat{\Psi}_{t,k}) > 0, \end{cases} \tag{40}$$

where $\Psi_{t,k}^{*}$ satisfies $H(\Psi_{t,k}^{*}) = 0$, and can be calculated by using the bisection method. In terms of the search bound, e.g., $[a, b]$, we use $a = \hat{\Psi}_{t,k}$ and preassign the right bound as $b = a + 10$. Then we check if $H(a)H(b) < 0$ holds true. If not, we double the value of b until $H(a)H(b) < 0$ is satisfied.

Based on the above analysis, the optimal $\Psi_{t,k}$ maximizing η_k with a fixed ϕ_k is given by

$$\Psi_{t,k}^{\mathrm{opt}} = \underset{\Psi_{t,k} \in \{\Psi_{t,k,1}^{\mathrm{opt}}, \Psi_{t,k,2}^{\mathrm{opt}}, \Psi_{t,k,3}^{\mathrm{opt}}\}}{\arg\max} \eta_k(\Psi_{t,k}). \tag{41}$$

Aided by (41), we clarify that the optimal $\boldsymbol{\Psi}_t$ subject to a fixed $\boldsymbol{\phi}$ can be determined.

2) Subproblem 2: In each iteration procedure, we then intend to optimize $\boldsymbol{\phi}$ subject to $\boldsymbol{\Psi}_t$ by considering the following problem

$$\max_{\boldsymbol{\phi}} \ \eta_{\mathrm{mpof}}(\boldsymbol{\Psi}_t, \boldsymbol{\phi}). \tag{42}$$

Similarly, we characterize the optimal ϕ_k with a fixed $\Psi_{t,k}$ by maximizing η_k. To clarify, we temporarily put the constraint $\phi_k \leq 1$ aside to ease the difficulty of finding solution, but this relaxation does not mean that we ignore this constraint. Instead, we add this constraint on the final solution, such that $\phi_k \leq 1$ still holds true.

To guarantee (27c) holds true, ϕ_k should be restricted to be larger than ϕ_k°, where ϕ_k° is the solution of $\Theta(\phi_k) = \Psi_{t,k}$. In this subsection, we also focus on the most complex case, e.g., $\phi_k^{\circ} < \phi_k^{*}$, where $\phi_k^{*} = (\varepsilon_k^{-1} - 1)/\Psi_{t,k}$. In the following, we discuss how to find the optimal ϕ_k by dividing its feasible region into two parts, e.g., $[\phi_k^{\circ}, \phi_k^{*}]$ and $[\phi_k^{*}, \in \infty)$.

For the first region, e.g., $[\phi_k^{\circ}, \phi_k^{*}]$, $\Psi_{t,k} < \hat{\Psi}_{t,k}$ holds true. Under this case, the expression for η_k can be formulated as (33), which enables us to derive $C(\phi_k) = \partial\eta_k/\partial\phi_k$ as

$$C(\phi_k) = -f_X\left(\zeta_k\right) \zeta_k^{'}(\phi_k) - \beta_k^{M-1} e^{-\frac{x}{P_b \zeta_k}} g(\phi_k), \tag{43}$$

where

$$\zeta_k^{'}(\phi_k) = \frac{\Psi_{t,k}}{P_b} \frac{(M-1)(1-\varepsilon_k) + \varepsilon_k \Psi_{t,k}}{\left(1 - \varepsilon_k - \varepsilon_k \phi_k \Psi_{t,k}\right)^2}, \tag{44}$$

[1]We clarify that $\phi_k \leq 1$ guarantees $P_{v,k} \leq P_{u,k}$, thus limiting the artificial noise leaked into the main channel in a certain range. That is, $\phi_k \leq 1$ is a natural and reasonable choice to design the secure transmission scheme.

and

$$g(\phi_k) = \left(\frac{(M-1)\,\phi_k}{1+\phi_k \Psi_{t,k}} + \frac{1}{P_b \zeta_k} \right) F_Y\left(\zeta_k\right) - f_Y\left(\zeta_k\right) \zeta_k^{'}(\phi_k). \tag{45}$$

Although we can obtain the closed-form expression of $C(\phi_k)$, it is difficult to further characterize its monotonicity due to the complicated expression of $g(\phi_k)$. Fortunately, we observe that the size of the first region is small, and thus using the one-dimensional search method to find the optimal ϕ_k is acceptable. We refer to the optimal ϕ_k in the first region as $\phi_{k,1}^{\mathrm{opt}}$.

For the second region, e.g., $[\phi_k^*, \in \infty)$, $\Psi_{t,k} \geq \hat{\Psi}_{t,k}$ holds true, and η_k can be formulated as (36). By taking the first-order derivative of η_k on ϕ_k, we derive $G(\phi_k) = \partial \eta_k / \partial \phi_k$ as

$$G(\phi_k) = \frac{\varepsilon_k^{1-M} e^{-\frac{\Psi_{t,k}}{P_b \varphi_k}} J(\phi_k)}{\ln 2 \cdot \phi_k (1+\phi_k \Psi_{t,k})^{M-1}}, \tag{46}$$

where $J(\phi_k)$ is expressed by

$$\begin{aligned} J(\phi_k) = & -\frac{\Theta^{'}(\phi_k)\phi_k}{1+\Theta(\phi_k)} - \frac{(M-1)\,\phi_k \Psi_{t,k}}{1+\phi_k \Psi_{t,k}} \ln\left(\frac{1+\Psi_{t,k}}{1+\Theta(\phi_k)}\right) \\ & - \frac{(M-1)\,\phi_k \Psi_{t,k}}{P_b} \ln\left(\frac{1+\Psi_{t,k}}{1+\Theta(\phi_k)}\right). \end{aligned} \tag{47}$$

To examine the monotonicity of $J(\phi_k)$, we provide the monotonicity and concavity of $\Theta(\phi_k)$ in the following lemma.

Lemma 2: $\Theta(\phi_k)$ is a monotonically decreasing function and also is a convex function of ϕ_k.

Proof: The proof is given in Appendix B. ■

Aided by Lemma 2, it is easy to find that all the three terms in the RHS of (47) are decreasing functions of ϕ_k. Therefore, we conclude that $J(\phi_k)$ is a decreasing function of ϕ_k. Note that $J(\in \infty) \leq 0$, but $J(\phi_k^*)$ varies. If $J(\phi_k^*) \leq 0$, $J(\phi_k) \leq 0$ always holds true, i.e., η_k monotonically decreases with ϕ_k, such that the maximum is achieved at $\phi_k = \phi_k^*$. However, if $J(\phi_k^*) > 0$, $J(\phi_k)$ is first positive then negative. That is, η_k first increases then decreases with ϕ_k, and the maximum is achieved at the unique root of $J(\phi_k) = 0$. As such, in the region of $[\phi_k^*, \in \infty)$, the optimal ϕ_k maximizing η_k can be expressed by

$$\phi_{k,2}^{\mathrm{opt}} = \begin{cases} \phi_k^*, & J(\phi_k^*) \leq 0, \\ \phi_k^\star, & J(\phi_k^*) > 0, \end{cases} \tag{48}$$

where $\phi_k^\star$ satisfies $J(\phi_k^\star) = 0$. Also, the explicit expression for $\phi_k^\star$ is difficult to derive, and we still adopt the bisection method to calculate it.

Based on the aforementioned discussions and the constraint $\phi_k \leq 1$, we state that the optimal ϕ_k maximizing η_k for a fixed $\Psi_{t,k}$ is given by

$$\phi_k^{\mathrm{opt}} = \underset{\phi_k \in \{\phi_{k,1}^{\mathrm{opt}}, \phi_{k,2}^{\mathrm{opt}}, 1\}}{\arg\max} \eta_k(\phi_k). \tag{49}$$

Aided by (49), we state that the optimal $\boldsymbol{\phi}$ subject to a fixed $\boldsymbol{\Psi}_t$ can be determined.

Based on the above analysis to the two subproblems, a BCD algorithm can be developed to iteratively optimize $\boldsymbol{\Psi}_t$ and $\boldsymbol{\phi}$, which is summarized in Algorithm 1. In regards to the convergence of this algorithm for solving Problem 2, we present the following proposition.

Algorithm 1: Proposed BCD Algorithm for Solving the Problem in Problem 2.

1: For a fixed T, calculate $\{\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{T-1}\}$ using (12).
2: Initialize $n = 1$, $\boldsymbol{\phi}[1]$ and $\boldsymbol{\Psi}_t[1]$.
3: Set the tolerance of accuracy $\epsilon > 0$.
4: Calculate $\eta_{\mathrm{mpof}}(\boldsymbol{\Psi}_t[1], \boldsymbol{\phi}[1])$ according to (26).
5: **repeat**
6: $\quad n = n + 1$.
7: $\quad$ Given $\boldsymbol{\phi}[n-1]$, obtain $\boldsymbol{\Psi}_t[n]$ according to (41).
8: $\quad$ Given $\boldsymbol{\Psi}_t[n]$, obtain $\boldsymbol{\phi}[n]$ according to (49).
9: **until** The difference of the objective function in (31a) in successive iterations is smaller than ϵ.
10: Output $\boldsymbol{\Psi}_t[n]$, $\boldsymbol{\phi}[n]$, and $\boldsymbol{\Psi}_e[n] = \Theta(\boldsymbol{\phi}[n])$.

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

Proof: The proof is given in Appendix C. ■

C. One-Dimensional Search for Finding the Optimal T

In this subsection, we concentrate on the second problem, e.g., searching the optimal T maximizing η_{mpof} over its feasible region. We first show that subject to the feedback constraint of each coherent period, e.g., B_c, the feasible region of T can be determined in the following theorem.

Theorem 1: When we perform secure transmission under our proposed MPOF scheme, the maximum length of feedback interval is expressed by $T_{\max} = m^* - 1$, where m^* is the minimum integer satisfying

$$1 - \rho^{2(m-1)} \left(1 - \varepsilon_c^m\right) > \varepsilon_{\max},\ m \in N, \tag{50}$$

where $\varepsilon_c = 2^{-\frac{B_c}{M-1}}$, $\varepsilon_{\max} = 2^{-\frac{B_{\min}}{M-1}}$ denotes the maximum allowable quantization error, and N denotes the set of positive integers. Here, $B_{\min}$ denotes the number of the minimum required feedback bits.

Proof: Using the MPOF scheme, all the feedback resources of T coherence periods should be assigned to B_0, e.g., $B_0 = B_c T$. Since ε_k gradually increases in one feedback interval, we only need to examine the final coherence period and ensure that $\varepsilon_{T-1} < \varepsilon_{\max}$ always holds true.[2] Aided by (12), ε_{T-1} can be written as

$$\varepsilon_{T-1} = 1 - \rho^{2(T-1)} \left(1 - \varepsilon_c^T\right). \tag{51}$$

To find the mathematical relationship between ε_{T-1} with T, we define $h(t) = 1 - \rho^{2(t-1)} \left(1 - \varepsilon_c^t\right)$, where $t \in [1, \in \infty)$. As such, ε_{T-1} can be analyzed via examining the monotonicity of $h(t)$. Specifically, we take the first derivative of $h(t)$, yielding

$$h^{'}(t) = \rho^{2(t-1)} \left(\varepsilon_c^t \ln\left(\rho^2 \varepsilon_c\right) - \ln \rho^2\right). \tag{52}$$

Aided by (52), we present the following discussions.

[2] A higher quantization error would cause serious noise leakage problem, significantly degrading the secrecy performance.

- *Case 1*: $\varepsilon_c \ln\left(\rho^2\varepsilon_c\right) \geq \ln\rho^2$. Under this case, $h^{'}(t) \geq 0$ always holds true for $t \geq 1$, and thus $h(t)$ is an increasing function in the feasible region of $t \in [1, \in \infty)$.
- *Case 2*: $\varepsilon_c \ln\left(\rho^2\varepsilon_c\right) < \ln\rho^2$. Under this case, $h^{'}(t)$ is first negative then positive, indicating that $h(t)$ first decreases then increases as t increases from 1 to ∞.

Given $h(1) = \varepsilon_c < \varepsilon_{\max}$ and $h(\in \infty) = 1 > \varepsilon_{\max}$, we state that in either case there is only one solution satisfying $h(t) = \varepsilon_{\max}$. Thus, the maximum length of feedback interval (e.g., $T_{\max}$) can be determined by finding the minimum positive integer m satisfying $h(m) > \varepsilon_{\max}$, which can be formulated as

$$m^* = \underset{m}{\operatorname{argmin}}\ h(m) - \varepsilon_{\max},\ \text{s.t. } h(m) > \varepsilon_{\max}. \tag{53}$$

Then we have $T_{\max} = m^* - 1$ and complete our proof. ■

Aided by Theorem 1, the optimization problem in the second step can be formulated as follows.

Problem 3: Given the feedback constraint of each coherence period, e.g., B_c, what is the optimal T that maximizes η_{mpof} under a given secrecy outage constraint? This problem is mathematically expressed as

$$\max_{T} \quad \eta_{\text{mpof}}(T, \boldsymbol{\Psi}_t^{\text{opt}}, \boldsymbol{\Psi}_e^{\text{opt}}, \boldsymbol{\phi}^{\text{opt}}), \tag{54a}$$

$$\text{s.t.} \quad 1 \leq T \leq T_{\max}, T \in N. \tag{54b}$$

In (54a), $\boldsymbol{\Psi}_t^{\text{opt}}$, $\boldsymbol{\Psi}_e^{\text{opt}}$, and $\boldsymbol{\phi}^{\text{opt}}$ can be obtained via solving Problem 2. However, since $\boldsymbol{\Psi}_t^{\text{opt}}$, $\boldsymbol{\Psi}_e^{\text{opt}}$, and $\boldsymbol{\phi}^{\text{opt}}$ vary with T and are not explicit functions of T, we clarify that Problem 3 is a typical non-linear integer problem and difficult to handle. Fortunately, we find that (54a) is merely a one-dimensional optimization problem, and its search space is quite limited. Motived by this, we can directly apply the one-dimensional search method to solve this problem.

VI. Numerical Results

In this section, we present numerical results to corroborate the aforementioned theoretical analysis. We first provide the validity of our proposed virtual quantizer model in Section III by using Monte Carlo simulations. Then we examine the secrecy throughput performance of our new secure transmission design under the MPOF scheme, based on which we finally characterize the performance advantage of our proposed scheme over the conventional scheme.

A. Verification of the Virtual Quantizer Model

Note that in Section III, we establish a virtual quantizer to transform the channel temporal correlation, which enables us to further perform the secure transmission design under our proposed MPOF scheme. Since this virtual quantizer occupies such a significant position, we firstly verify its correctness by providing Figs. 4 and 5. To clarify, in the simulation process we directly use the codebook examples listed in [34]. For the Monte Carlo simulations, we obtain the numerical results by averaging over 10^6 channel trials.

Fig. 4 plots the probability of $\cos^2\theta_k$ less than $1-\varepsilon_k$ versus ρ for different values of k, along which the Monte Carlo

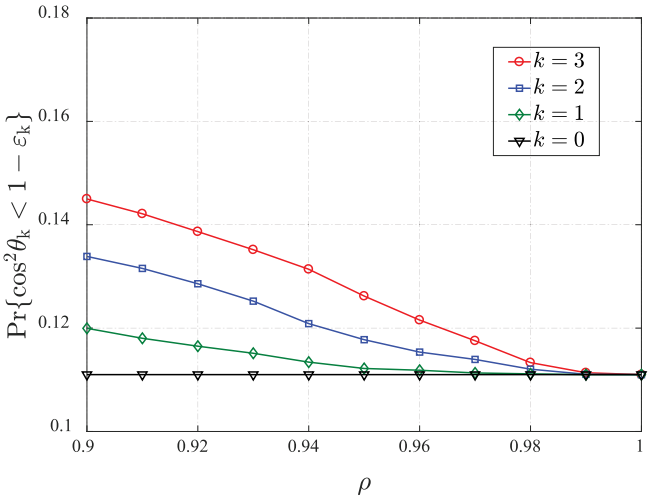

Fig. 4. The probability of $\cos^2\theta_k$ less than $1-\varepsilon_k$ versus ρ with $M=4$ and $B_0=6$.

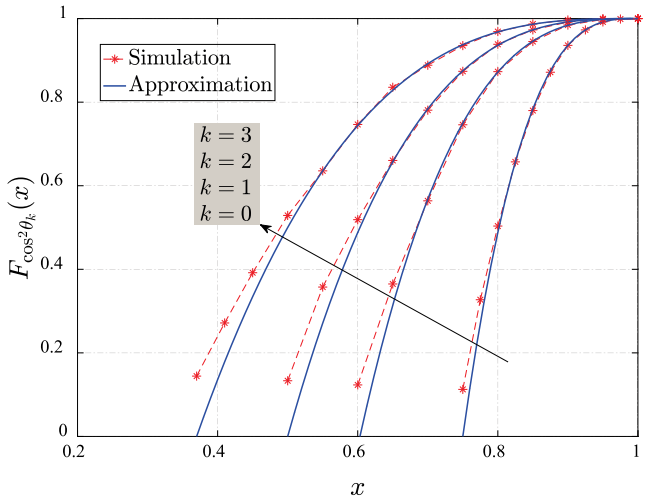

Fig. 5. The CDF of $\cos^2\theta_k$ with $M=4$, $\rho=0.9$, and $B_0=6$.

simulations, marked by '$*$', are also provided. For a simple notation, we define $p_k = \Pr\{\cos^2\theta_k < 1-\varepsilon_k\}$. Note that an ideal codebook is the one with $p_0 = 0$. In this case, the actual CDF of $\cos^2\theta_0$ coincides with (10). However, designing an ideal codebook is practically unreachable [29], [31], and only a suboptimal codebook with $p_0 > 0$ can be numerically obtained. This helps explain why we observe from this figure that $p_0 = 0.11$. This observation highlights that even though the real-time quantization is available, the widely-used CDF of $\cos^2\theta_0$ in (10) is actually an approximated expression. We also observe that for a fixed ρ, p_k would increase as k increases. This is not surprising since the virtual quantizer's performance degrades with channel evolution. However, it is a fortune that p_k merely has a minor increase when ρ is high. That is, p_k is still in a reasonable scope relative to p_0. This observation makes it possible to approximate the CDF of $\cos^2\theta_k$ as (11), which has the similar form with (10).

Fig. 5 plots the CDF of $\cos^2\theta_k$ for different values of k. In this figure, we depict the theoretic curves by using the approximate

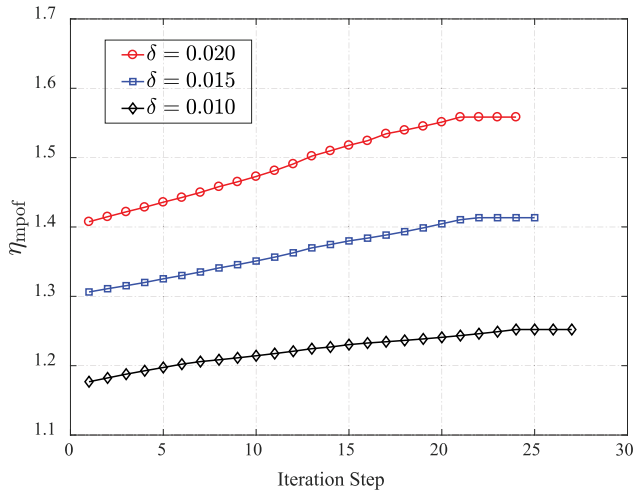

Fig. 6. The convergence rate of the BCD algorithm with $M = 4$, $\alpha = 4$, $P_b = 20\,\mathrm{dB}$, $P_e = 0\,\mathrm{dB}$, $\rho = 0.9$, $B_c = 6$, and $B_{\min} = 2$.

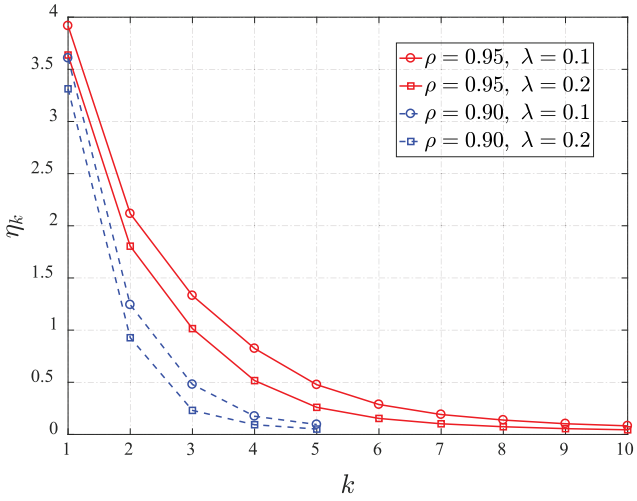

Fig. 7. The secrecy throughput of different coherence periods with $M = 4$, $\alpha = 4$, $P_b = 20\,\mathrm{dB}$, $P_e = 0\,\mathrm{dB}$, $B_c = 6$, $B_{\min} = 2$, and $\delta = 0.01$.

expression in (11), and provide some Monte Carlo simulations for verification. We observe from this figure that when x is relatively large, the difference between the approximate result and the numerical result is extremely minor. This verification demonstrates that the expression for the CDF of $\cos^2\theta_k$ in (11) is a good approximation. Thus, it can be used for performance characterization when we analyze the virtual quantizer of the k-th coherence period. Since the theoretical analysis for our secure transmission design builds on (11), we highlight that this figure ensures the preciseness of our theoretical analysis.

B. Secrecy Throughput Under the MPOF Scheme

We next focus on illustrating the secrecy throughput of our proposed transmission scheme. We first examine the convergence of our designed BCD algorithm in Fig. 6. Then we set $T = T_{\max}$ and individually illustrate the secrecy throughput of different coherence periods in Fig. 7. Finally, we depict the secrecy throughput under the MPOF scheme in Fig. 8.

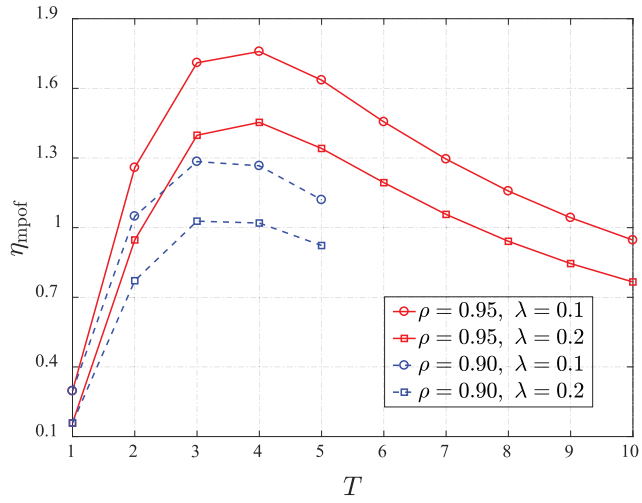

Fig. 8. The secrecy throughput under the MPOF scheme with $M = 4$, $\alpha = 4$, $P_b = 20\,\mathrm{dB}$, $P_e = 0\,\mathrm{dB}$, $B_c = 6$, $B_{\min} = 2$, and $\delta = 0.01$.

Fig. 6 plots the convergence rate of our designed BCD algorithm for different values of δ. We first observe that the number of the required iteration steps is generally small, e.g., less than 30. We also observe that the number of the required iteration steps is influenced by δ. Intuitively, a higher number of iteration steps are required when the secrecy outage constraint becomes stricter. For example, 24 iteration steps are needed when $\delta = 0.02$, while 27 iteration steps are needed when $\delta = 0.01$. This figure indicates that our BCD algorithm converges fast, and highlights its efficiency and practicality for determining the appropriate system parameters.

Fig. 7 plots the secrecy throughput of different coherence periods in one feedback interval. In this figure, we directly set $T = T_{\max}$ and individually illustrate the secrecy throughput of the k-th coherence period, e.g., η_k. We first observe that for the fixed ρ and λ, η_k decreases as k increases. This is due to the fact the CSIT becomes less accurate with channel evolution, leading to the reduction of the transmission probability. Moreover, this figure demonstrates that η_k decreases when λ increases. This is because the eavesdropping ability grows with λ, degrading the secrecy performance.

Fig. 8 plots the secrecy throughput under the MPOF scheme versus T. The curves for η_{mpof} are generated by applying the BCD algorithm. We first observe that η_{mpof} first increases then decreases as T increases from 1 to $T_{\max}$. This observation indicates that there exists an optimal T (e.g., T_{opt}) maximizing the secrecy throughput under the MPOF scheme. Even though the theoretical solution for T_{opt} is difficult to find, we state that it can be easily determined by employing a simple one-dimensional search. We also observe that the maximum η_{mpof} increases as ρ increases. This demonstrates that under a certain feedback rate constraint, a higher channel temporal correlation can support a larger secrecy throughput.

C. Performance Comparison

In this subsection, we show the secrecy performance advantage resulted from the MPOF scheme by comparing it with the

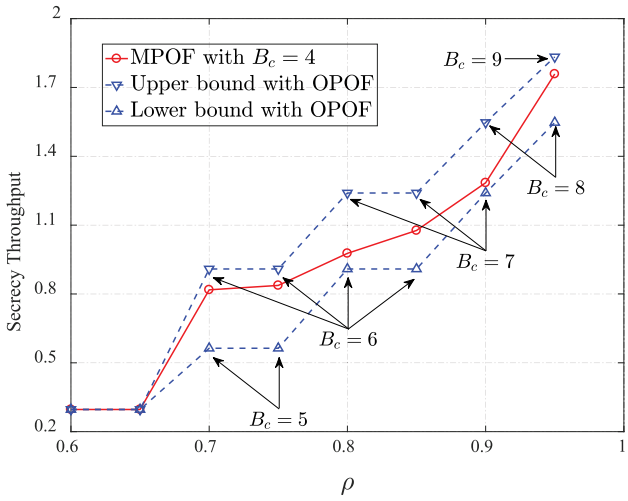

Fig. 9. The advantage of the MPOF scheme on reducing feedback resources with $M = 4$, $\alpha = 4$, $P_b = 20\,\text{dB}$, $P_e = 0\,\text{dB}$, $\delta = 0.01$, and $\lambda = 0.1$.

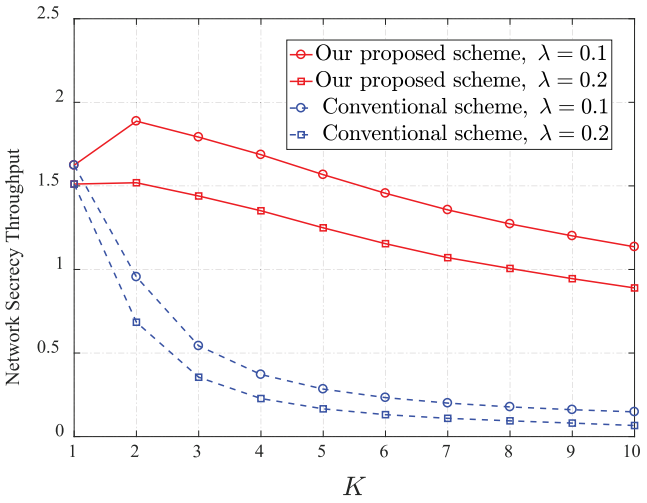

Fig. 10. The advantage of the MPOF scheme on improving network secrecy throughput with $M = 16$, $\alpha = 4$, $P_b = 20\,\text{dB}$, $P_e = 0\,\text{dB}$, $B_{\text{total}} = 40$, $\rho = 0.9$, $\delta = 0.01$, and $\lambda = 0.1$.

conventional one-period one-feedback (OPOF) scheme. Specifically, we show the benefits of the MPOF scheme on saving feedback resources and improving the secrecy throughput in Figs. 9 and 10, respectively.

Fig. 9 shows the advantage of the MPOF scheme over the conventional OPOF scheme in terms of saving feedback resources for secure transmission. To identify this advantage of the MPOF scheme, in this figure we mark the specific number of feedback bits the OPOF scheme needs when it achieves the secrecy throughput performance close to the MPOF scheme. We observe from this figure that compared to the OPOF scheme, the MPOF scheme has a significant increase in feedback bits reduction. Furthermore, this increase becomes more profound as ρ increases, i.e., a higher ρ means saving more feedback bits. In particular, under the given parameters of this figure, we find that $\rho = 0.90$ equivalently saves 3 bits, and $\rho = 0.95$ equivalently saves 5 bits. This figure highlights that the MPOF scheme is capable of exploiting the benefits of channel temporal correlation for the secure transmission with reduced feedback bits.

Fig. 10 focuses on a practical IoT scenario and shows the advantage of the MPOF scheme over the conventional OPOF scheme in terms of improving the network secrecy throughput. To be specific, we consider the homogeneous IoT downlink network, where the central controller exploits the zero-forcing beamforming to simultaneously serve K legitimate users, and uses the remaining $M - K$ spatial dimensions to send AN for confusing eavesdroppers. We observe from this figure that compared to the conventional scheme, our proposed scheme achieves a significant increase in the network secrecy throughput when $K \geq 2$. Due to this advantage, it is safe to conclude that the MPOF scheme is well suited for IoT networks where the high channel temporal correlation is quite common but the feedback resources are extremely limited.

VII. Conclusion

In this work, we concentrated on implementing physical layer security to safeguard the downlink transmission of the IoT applications. In particular, we designed a secure ON-OFF transmission scheme with low complexity and small requirements on the feedback overhead. The key innovation of this design is a novel feedback scheme, which is able to integrate the feedback resources of multiple coherence periods for CSIT acquisition. Based on this feedback scheme, we developed an ON-OFF-based secure transmission design and then proposed a BCD-based one-dimensional search method to maximize the secrecy throughput. Numerical results showed that our secure transmission design would significantly improve the secrecy throughput or reduce the feedback overhead, by utilizing the channel temporal correlation existing in the IoT scenarios.

Appendix A
Proof of Lemma 1

Aided by (3), we establish the general relationship between $\mathbf{h}_k$ and $\mathbf{h}_0$ as $\mathbf{h}_k = \rho^k \mathbf{h}_0 + \sqrt{1-\rho^{2k}}\mathbf{e}$, where $\mathbf{e} \in \mathbb{C}^{1\times M}$ has i.i.d complex Gaussian random entires with zero mean and unit variance. As such, $\mathbb{E}\{|\mathbf{h}_k \mathbf{c}_0^\dagger|^2\}$ is formulated as

$$\begin{aligned}\mathbb{E}\left\{|\mathbf{h}_k \mathbf{c}_0^\dagger|^2\right\} &= \mathbb{E}\left\{|(\rho^k \mathbf{h}_0 + \sqrt{1-\rho^{2k}}\mathbf{e})\mathbf{c}_0^\dagger|^2\right\} \\ &= \rho^{2k}\mathbb{E}\left\{|\mathbf{h}_0 \mathbf{c}_0^\dagger|^2\right\} + \left(1-\rho^{2k}\right)\mathbb{E}\left\{|\mathbf{e}\mathbf{c}_0^\dagger|^2\right\}, \end{aligned} \tag{55}$$

It follows that $\mathbf{h}_0$ and $\mathbf{e}$ are independent and have zero mean, thus the expectations for all cross-terms, e.g., $\mathbb{E}\{\mathbf{c}_0\mathbf{h}_0^\dagger\mathbf{e}\mathbf{c}_0^\dagger\}$ and $\mathbb{E}\{\mathbf{c}_0\mathbf{e}^\dagger\mathbf{h}_0\mathbf{c}_0^\dagger\}$, become zero [26].

Since $\mathbf{e}$ is independent of the unit-norm vector $\mathbf{c}_0$, we have $\mathbf{e}\mathbf{c}_0^\dagger \sim \mathcal{CN}(0,1)$, such that $\mathbb{E}\{|\mathbf{e}\mathbf{c}_0^\dagger|^2\} = 1$. Moreover, using the independence between the direction knowledge and the amplitude knowledge [35], we have

$$\mathbb{E}\left\{|\mathbf{h}_0 \mathbf{c}_0^\dagger|^2\right\} = \mathbb{E}\{\|\mathbf{h}_0\|^2\}\mathbb{E}\left\{\cos^2\theta_0\right\} \tag{56}$$

and

$$\mathbb{E}\left\{|\mathbf{h}_k\mathbf{c}_0^{\dagger}|^2\right\} = \mathbb{E}\left\{\|\mathbf{h}_k\|^2\right\}\mathbb{E}\left\{\cos^2\theta_k\right\}, \tag{57}$$

where the amplitudes satisfy

$$\mathbb{E}\{\|\mathbf{h}_0\|^2\} = \mathbb{E}\{\|\mathbf{h}_k\|^2\} = M. \tag{58}$$

By substituting (56), (57) and (58) into (55), we derive $\mathbb{E}\left\{\cos^2\theta_k\right\}$ as

$$\mathbb{E}\left\{\cos^2\theta_k\right\} = \rho^{2k}\mathbb{E}\left\{\cos^2\theta_0\right\} + \frac{1-\rho^{2k}}{M}. \tag{59}$$

On the other hand, aided by the CDF of $\cos^2\theta_0$ and $\cos^2\theta_k$ in (10) and (11), we derive $\mathbb{E}\left\{\cos^2\theta_0\right\}$ and $\mathbb{E}\left\{\cos^2\theta_k\right\}$ as

$$\mathbb{E}\left\{\cos^2\theta_0\right\} = 1 - \left(1 - M^{-1}\right)\varepsilon_0, \tag{60}$$

and

$$\mathbb{E}\left\{\cos^2\theta_k\right\} = 1 - \left(1 - M^{-1}\right)\varepsilon_k, \tag{61}$$

respectively. By substituting (60) into (59), we can formulate $\mathbb{E}\left\{\cos^2\theta_k\right\}$ as another form, given by

$$\begin{aligned}
&\mathbb{E}\left\{\cos^2\theta_k\right\} \\
&= \rho^{2k}\left(1 - \left(1 - M^{-1}\right)\varepsilon_0\right) + (1-\rho^{2k})M^{-1} \\
&= \rho^{2k}\left(1 - M^{-1} - \left(1 - M^{-1}\right)\varepsilon_0\right) + M^{-1} \\
&= \rho^{2k}\left(1 - M^{-1}\right)(1-\varepsilon_0) - \left(1 - M^{-1}\right) + 1 \\
&= 1 - \left(1 - M^{-1}\right)\left(1 - \rho^{2k}\left(1-\varepsilon_0\right)\right).
\end{aligned} \tag{62}$$

Comparing (62) with (61), we conclude that ε_k can be formulated as (12) in Lemma 1.

Appendix B
Proof of Lemma 2

For simplicity of the notations, we omit ϕ_k from $\Theta(\phi_k)$ in the following proof. Note that the definition of Θ produces that $F_{\gamma_{e,k}}(\Theta) = 1 - \delta$, which yields

$$\Omega(\Theta, \phi_k) + C = 0 \tag{63}$$

where

$$\Omega(\Theta, \phi_k) = (1 + \phi_k\Theta)^{M-1}(\Theta + (M-1)\,\phi_k\Theta)^{\mu}, \tag{64}$$

and $C = \chi/\ln(1-\delta)$. Using the derivative rule for implicit functions, we first derive the first-order derivative of Θ on ϕ_k as

$$\Theta' = \frac{d\Theta}{d\phi_k} = -\frac{\partial\Omega/\partial\phi_k}{\partial\Omega/\partial\Theta} = K(\Theta, \phi_k) + L(\Theta, \phi_k), \tag{65}$$

where $K(\Theta, \phi_k)$ and $L(\Theta, \phi_k)$ are respectively expressed as

$$K(\Theta, \phi_k) = -\frac{(M-1)\,\Theta}{1 + (M-1)\,\phi_k} \tag{66}$$

and

$$L(\Theta, \phi_k) = -\frac{(M-1)\,\Theta^2}{(1 + (M-1)\,\phi_k)\,(\mu + (M-1+\mu)\,\Theta\phi_k)}. \tag{67}$$

Obviously, $\frac{d\Theta}{d\phi_k} < 0$ always holds, i.e., Θ is a decreasing function of ϕ_k. Based on this result, we further find that $K(\Theta, \phi_k)$ is an increasing function of ϕ_k, e.g., $dK(\Theta, \phi_k)/d\phi_k > 0$. To characterize the concavity of Θ on ϕ_k, we next investigate the monotonicity of $L(\Theta, \phi_k)$ on ϕ_k. Specifically, we define $\Xi = \Theta\phi_k$, and re-express (63) as

$$\Omega(\Xi, \phi_k) + C = 0 \tag{68}$$

where $\Omega(\Xi, \phi_k) = \Xi^{\mu}(1+\Xi)^{M-1}(M - 1 + \phi_k^{-1})^{\mu}$. Using the same method as in (65), it is not hard to find that Ξ is an increasing function of ϕ_k. Based on a simple monotonicity analysis, we state that $L(\Theta, \phi_k)$ is also an increasing function of ϕ_k, e.g., $dL(\Theta, \phi_k)/d\phi_k > 0$. As such, we have

$$\Theta'' = \frac{d}{d\phi_k}\left(\frac{d\Theta}{d\phi_k}\right) = \frac{dK(\Theta, \phi_k)}{d\phi_k} + \frac{dL(\Theta, \phi_k)}{d\phi_k} > 0, \tag{69}$$

and conclude that Θ is a decreasing and convex function of ϕ_k in Lemma 2.

Appendix C
Proof of Proposition 1

By observing (31a) and (31b), it is not hard to find that the objective function is continuously differentiable, and the feasible set is closed, nonempty and convex. Since $\eta_{\mathrm{mpof}}(\boldsymbol{\Psi}_t, \boldsymbol{\phi})$ is a bounded function, by using Bolzano-Weierstrass theorem, we know that the optimization variables (e.g., $\boldsymbol{\Psi}_t$ and $\boldsymbol{\phi}$) must have limit points, as long as $\eta_{\mathrm{mpof}}(\boldsymbol{\Psi}_t, \boldsymbol{\phi})$ is a monotonically nondecreasing function. Mathematically, we should prove the following relationship

$$\eta_{\mathrm{mpof}}(\boldsymbol{\Psi}_t[n], \boldsymbol{\phi}[n]) \geq \eta_{\mathrm{mpof}}(\boldsymbol{\Psi}_t[n-1], \boldsymbol{\phi}[n-1]). \tag{70}$$

We find that (70) is easy to prove in accordance with the properties of the saddle points, yielding

$$\begin{aligned}
\eta_{\mathrm{mpof}}(\boldsymbol{\Psi}_t[n], \boldsymbol{\phi}[n]) &\geq \eta_{\mathrm{mpof}}(\boldsymbol{\Psi}_t[n], \boldsymbol{\phi}[n-1]) \\
&\geq \eta_{\mathrm{mpof}}(\boldsymbol{\Psi}_t[n-1], \boldsymbol{\phi}[n-1]).
\end{aligned} \tag{71}$$

By invoking ([36], Corollary 2), we state that every limit point obtained by Algorithm 1 is a stationary point of Problem 2.

References

[1] J. G. Andrews *et al.*, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, Jun. 2014.

[2] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Commun. Surv. Tuts.*, vol. 18, no. 3, pp. 1617–1655, Third Quarter 2016.

[3] M. R. Palattella *et al.*, "Internet of Things in the 5G era: Enablers, architecture, and business models," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 1045–1072, Mar. 2016.

[4] S.-C. Lin and K.-C. Chen, "Improving spectrum efficiency via in-network computations in cognitive radio sensor networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1222–1234, Mar. 2014.

[5] I. F. Akyildiz, S. Nie, S.-C. Lin, and M. Chandrasekaran, "5G roadmap: 10 key enabling technologies," *Comput. Netw.*, vol. 106, pp. 17–48, Sep. 2016.

[6] A. A. Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surv. Tuts.*, vol. 17, no. 4, pp. 2347–2376, Fourth Quarter 2015.

[7] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Commun. Surv. Tuts.*, vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 2015.

[8] W. Trappe, "The challenges facing physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, Jun. 2015.
[9] 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.
[10] 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.
[11] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[12] A. Khisti and G. Wornell, "Secure transmission with multiple antennas—I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.
[13] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.
[14] D. Lun, H. Zhu, 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.
[15] Z. Gan, C. Li-Chia, and W. Kai-Kit, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.
[16] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[17] S. Liu, Y. Hong, and E. Viterbo, "Artificial noise revisited," *IEEE Trans. Inf. Theory*, vol. 61, no. 7, pp. 3901–3911, Jul. 2015.
[18] S. C. Lin, T. H. Chang, Y. L. Liang, Y. W. P. Hong, and C. Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise: The noise leakage problem," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 901–915, Mar. 2011.
[19] 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.
[20] H. Wang, C. Wang, and W. Ng, "Artificial noise assisted secure transmission under training and feedback," *IEEE Trans. Signal Process.*, vol. 63, no. 23, pp. 6285–6298, Dec. 2015.
[21] 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.
[22] B. C. Banister and J. R. Zeidler, "Feedback assisted transmission subspace tracking for MIMO systems," *IEEE J. Sel. Areas Commun.*, vol. 21, no. 3, pp. 452–463, Mar. 2003.
[23] K. Huang, R. W. Heath, and J. G. Andrews, "Limited feedback beamforming over temporally correlated channels," *IEEE Trans. Signal Process.*, vol. 57, no. 5, pp. 1959–1975, May 2009.
[24] K. Huang, V. K. N. lau, and D. Kim, "Event-driven optimal feedback control for multiantenna beamforming," *IEEE Trans. Signal Process.*, vol. 58, no. 6, pp. 3298–3312, Jun. 2010.
[25] C. C. Tan and N. C. Beaulieu, "On first-order Markov modeling for the Rayleigh fading channel," *IEEE Trans. Commun.*, vol. 48, no. 12, pp. 2032–2040, Dec. 2000.
[26] T. Kim, D. J. Love, and B. Clerckx, "Does frequent low resolution feedback outperform infrequent high resolution feedback for multiple antenna beamforming systems," *IEEE Trans. Signal Process.*, vol. 59, no. 4, pp. 1654–1669, Apr. 2011.
[27] 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.
[28] 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.
[29] S. Zhou, Z. Wang, and G. B. Giannakis, "Quantifying the power loss when transmit beamforming relies on finite-rate feedback,"*IEEE Trans. Wireless Commun.*, vol. 4, no. 4, pp. 1948–1957, Jul. 2005.
[30] D. J. Love, R. W. Heath Jr, V. K. N. Lau, D. Gesbert, B. D. Rao, and M. Andrews, "An overview of limited feedback in wireless communication systems," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 8, pp. 2735–2747, Oct. 2008.
[31] T. Yoo, N. Jindal, and A. Goldsmith, "Multi-antenna downlink channels with limited feedback and user selection," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 7, pp. 1478–1491, Sep. 2007.
[32] 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.
[33] H. Wang and X. Xia, "Enhancing wireless secrecy via cooperation: Signal design and optimization," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 47–53, Dec. 2015.
[34] A. Medra and T. N. Davidson, "Optimization of training and feedback overhead for beamforming over block fading channels," *IEEE Trans. Signal Process.*, vol. 62, no. 5, pp. 1305–1318, Mar. 2014.
[35] W. Spantipach and M. L. Honig, "Flexible codebook design for limited feedback systems via sequential smooth optimization on the Grassmannian manifold," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6103–6115, Dec. 2010.
[36] 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 in 2012 from the PLA Army Engineering University, Nanjing, China, where he has been working toward the Ph.D. degree in communications and information system at the College of Communications Engineering, since 2014. His current research interests include physical layer security and Internet of Things (with a particular emphasis on designing secure transmission schemes in the Internet of Things).

Yueming Cai (M'05–SM'12) received the B.S. degree in physics from Xiamen University, Xiamen, China in 1982, and the M.S. degree in microelectronics engineering and the Ph.D. degree in communications and information systems from Southeast University, Nanjing, China, in 1988 and 1996, respectively. His current research interests include multiple-input multiple-output systems, cooperative communications, device-to-device communications, and physical layer security.

Nan Yang (S'09–M'11) received the B.S. degree in electronics from China Agricultural University, Beijing, China, in 2005, and the M.S. and Ph.D. degrees in electronic engineering from the Beijing Institute of Technology, Beijing, in 2007 and 2011, respectively. Since July 2014, he has been with the Research School of Engineering, Australian National University, Canberra, ACT, Australia, where he is currently a Future Engineering Research Leadership Fellow and a Senior Lecturer. Prior to this, he was a Postdoctoral Research Fellow with 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. His general research interests include communications theory and signal processing, with specific interests in massive multiantenna systems, millimeter-wave communications, ultrareliable low-latency communications, cyber-physical security, and molecular communications. He was a recipient of 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 was 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, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and the *Transactions on Emerging Telecommunications Technologies*.