Cooperative Jamming for Physical Layer Security Enhancement in Internet of Things

Lin Hu, Hong Wen, *Senior Member, IEEE*, Bin Wu, *Member, IEEE*, Fei Pan, Run-Fa Liao, Huanhuan Song, Jie Tang, and Xiumin Wang

***Abstract*—Internet of Things (IoT) is becoming an emerging paradigm to achieve ubiquitous connectivity, via massive deployment of physical objects, such as sensors, controllers, and actuators. However, concerns on the IoT security are raised due to the wireless broadcasting nature and the energy constraint of the physical objects. In this paper, we study secure downlink transmission from a controller to an actuator, with the help of a cooperative jammer to fight against multiple passive and noncolluding eavesdroppers. In addition to artificial noise aided secrecy beamforming for secure transmission, cooperative jamming (CJ) is explored to further enhance physical layer security. In particular, we provide a secrecy enhancing transmit design to minimize the secrecy outage probability (SOP), subject to a minimum requirement on the secrecy rate. Based on a strict mathematical analysis, we further characterize the impacts of the main channel quality and the minimum secrecy rate on transmit designs. Numerical results confirm that our design can enhance both security (in terms of SOP) and power efficiency as compared with the approach without CJ.**

***Index Terms*—Cooperative jamming (CJ), Internet of Things (IoT), physical layer security (PLS), secrecy outage probability (SOP), secrecy rate.**

I. Introduction

With the advancement of wireless communication and networking techniques, Internet of Things (IoT) is expected to achieve pervasive sensing, intelligent information processing, and efficient resource management in heterogeneous networks [1], [2], e.g., cellular networks, sensor networks, etc. It integrates sensing components measuring information from the physical world, computing and processing systems analyzing the collected sensing information for decision making, and operating and control components performing actuation tasks. In recent years, a wide range of IoT applications have been deployed in areas, such as environment monitoring, security surveillance, spatial crowdsourcing [3], crowd dynamics management [4], and smart cities [5].

Security and privacy protection is a fundamental requirement for IoT applications. In particular, wireless communications in IoT (e.g., uplink communications from sensors to controllers, downlink communications from controllers to actuators, etc.) are highly susceptible to eavesdropping attacks, due to the broadcasting nature of the wireless medium. Traditionally, security issues are addressed by cryptographic encryption methods implemented in upper layers of the network protocol stack. These methods have inherent difficulties and vulnerabilities in secret key distribution and high complexity [6]. Thus, it is a great challenge to implement security in IoT systems with a large number of resource constrained sensors and actuators. Unlike encryption-based security, physical layer security (PLS) [7]–[9] exploits physical properties of wireless channels, e.g., fading, noise, interference, etc. PLS guarantees information-theoretic security regardless of eavesdropper's computing capability. As an alternative or complement to complex cryptographic techniques, PLS is becoming an appealing solution for secure communications in IoT [10].

The pioneering work on PLS can be traced back to wiretap channels in [11], which is then extended to Gaussian degraded wiretap channels in [12], and general nondegraded wiretap channels in [13]. These works demonstrated the existence of coding and signal processing techniques for both reliable and secure communication over wireless channels. Specifically, when the main channel (from source to destination) is better than the eavesdropper channel (from source to eavesdropper), the transmitted secret message can be encoded to achieve a low error probability at the destination, while guaranteeing information-theoretic security against the eavesdropper. Moreover, the secrecy performance is shown to increase with the difference of these two channels. Motivated by these results, PLS techniques are extensively studied to enlarge the signal quality difference at the destination and the eavesdropper [14], with focus on secure multiantenna transmission [15]–[23] and cooperative security [24]–[34].

Multiantenna technique is considered as an efficient and reliable way for improving secrecy, due to the advantage of having spatial degrees of freedom and diversity gains. In particular, when the eavesdropper's instantaneous channel sate

Manuscript received September 2, 2017; revised November 11, 2017; accepted November 15, 2017. Date of publication November 28, 2017; date of current version February 9, 2018. This work was supported in part by the 863 High Technology Plan under Grant 2015AA01A707 and in part by the NSFC (No. 61572114, 61372085, and 61379027). *(Corresponding author: Hong Wen.)*

L. Hu, H. Wen, F. Pan, R.-F. Liao, H. Song, and J. Tang are with the National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: lin.hu.uestc@gmail.com; sunlike@uestc.edu.cn; panfeivivi@hotmail.com; runfa.liao@std.uestc.edu.cn; huanhuansong@126.com; cs.tan@163.com).

B. Wu is with the Tianjin Key Laboratory of Advanced Networking, School of Computer Science and Technology, Tianjin University, Tianjin 300350, China (e-mail: binw@tju.edu.cn).

X. Wang is with the College of Information Engineering, China Jiliang University, Hangzhou 310018, China (e-mail: wxm6341@163.com).

Digital Object Identifier 10.1109/JIOT.2017.2778185

information (CSI) is not available, secrecy beamforming with artificial noise (AN) was proposed in [15], where AN is transmitted on top of the information-bearing signal to deteriorate the eavesdropper channel. Based on this idea, AN assisted transmit designs were studied for both fast and slow fading channels [16]–[23]. For fast fading channels, ergodic secrecy rate is often utilized as the secrecy metric [16], [17]. For slow fading channels, secrecy throughput, secrecy outage probability (SOP), and SOP constrained secrecy rate are often adopted as performance metrics [18]–[23]. Specifically, to minimize SOP, power allocation between information-bearing signal and AN signal was optimized for the single eavesdropper in [19] and [20], and for multiple eavesdroppers in [21]–[23].

To further enhance secrecy of wireless communications, several cooperative security schemes were investigated, such as amplify-and-forward (AF) [27], decode-and-forward (DF) [28], randomize-and-forward [29], and cooperative jamming (CJ) [30]–[32]. In particular, the secrecy rate maximization problem was investigated for single-input single-output [30], single-input multiple-output [31], and multiple-input single-output wiretap channels [32]. It was shown in [32] that, both secrecy rate and secure energy efficiency can be enhanced with CJ scheme, as compared with the approach without CJ. In addition, combinations of CJ and relaying (AF or DF) were studied in [33] and [34].

In this paper, we investigate security enhancement for downlink transmission in IoT networks, where a controller intends to transmit a secret message to an actuator, coexisting with multiple passive eavesdroppers. Besides, there is a friendly cooperative jammer that emits jamming signals to prevent eavesdroppers from retrieving the secret message. We assume that controller and cooperative jammer are equipped with multiple antennas, while the actuator and each eavesdropper are equipped with a single antenna. We consider a slow fading wiretap channel, and assume that eavesdroppers' statistical CSIs are available. In addition to AN assisted multiantenna transmission, a CJ scheme is proposed to further enhance PLS. Specifically, we provide an explicit transmit design to minimize SOP, subject to a minimum secrecy rate constraint. Although the problem is difficult to be solved directly, with a change of variables and a transformation of the objective and constraint functions, we reformulate it as a tractable power allocation problem. Then, we develop an efficient solution to this problem based on convex optimization [35].

Although the optimal power allocation for SOP minimization (SOPM) has been studied in [19]–[23], and the SOP performance has been analyzed in [34], this paper differs from these works in the following aspects.

1) Unlike secure transmissions *without* cooperation [19]–[23], we utilize the cooperative transmission to further enhance secrecy performance. Moreover, the work on cooperative security in [34] assumes that each node in the network employs a single antenna. In this paper, we focus on secure transmission with multiple antennas.
2) The analytical approaches in [21] and [22] are based on first-order derivatives, and multiple solutions may exist. In this paper, we show that the objective function in the original SOPM problem can be transformed into a strictly concave function. This guarantees the uniqueness of the optimal solution.
3) We reveal the impacts of the main channel quality and the minimum secrecy rate requirement on the optimal power allocation through strict mathematical proofs, rather than through numerical demonstration as shown in the existing cooperative security schemes.

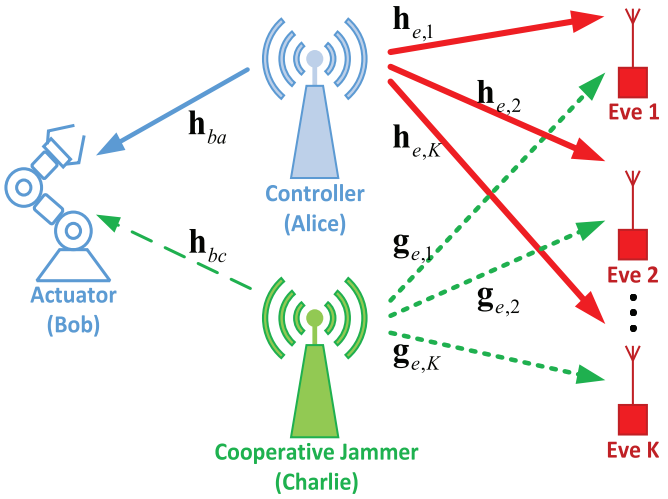


Fig. 1. Model of IoT downlink transmission with PLS.

The rest of this paper is organized as follows. In Section II, we describe system model and problem formulation. Our proposed transmit design for SOPM is presented in Section III. Numerical results are provided in Section IV, and we conclude this paper in Section V.

Notation: Uppercase and lowercase boldface letters denote matrices and column vectors, respectively. Standard lowercase letters denote scalars. null($\mathbf{X}$) is the null space of $\mathbf{X}$, and $\Pi_{\mathbf{X}}^{\perp}$ is the orthogonal complement projector of $\mathbf{X}$. $\mathcal{CN}(\boldsymbol{\mu}, \mathbf{Q})$ denotes the circularly symmetric complex Gaussian distribution with mean $\boldsymbol{\mu}$ and covariance $\mathbf{Q}$. $\Gamma(k, \mu)$ is the gamma distribution with shape k and scale μ. Exp(λ) is the exponential distribution with rate parameter λ. $|\cdot|$ and $\|\cdot\|$ denote the absolute value and ℓ_2 norm, respectively. $\log(\cdot)$ and $\ln(\cdot)$ are the base-2 and natural logarithms, respectively. $\Gamma(\alpha)$ denotes the gamma function [36, 8.310.1]. ${}_1F_1(\alpha; \gamma; z)$ is the degenerate hypergeometric function [36, 9.210.1]. ${}_2F_1(\alpha, \beta; \gamma; z)$ is the Gauss hypergeometric function [36, 9.100]. The symbols $\triangleq$, $\Longrightarrow$, and $\Longleftrightarrow$ denote "defined as," "implies," and the equivalence relation, respectively.

II. System Model and Problem Formulation

We consider secure downlink transmission in IoT networks as shown in Fig. 1, where a controller (Alice) intends to transmit a confidential message to an actuator (Bob), in the presence of multiple passive and noncolluding eavesdroppers (Eves). In addition, a cooperative jammer (Charlie) emits interference signals to confuse Eves. The set of Eves is defined as $\mathcal{K} \triangleq \{1, 2, \ldots, K\}$. We assume that Alice and Charlie are equipped with N_a and N_c antennas, respectively, while Bob

and each Eve are equipped with only a single antenna. All wireless channels are assumed to be independent under slow flat fading conditions. Channels from Alice to Bob and the kth Eve ($k \in \mathcal{K}$) are denoted by $\mathbf{h}_{ba} \in \mathbb{C}^{N_a}$ and $\mathbf{h}_{e,k} \in \mathbb{C}^{N_a}$, respectively, and those from Charlie to Bob and the kth Eve are denoted by $\mathbf{h}_{bc} \in \mathbb{C}^{N_c}$ and $\mathbf{g}_{e,k} \in \mathbb{C}^{N_c}$. We also assume that Bob's perfect CSI and Eves' statistical CSIs are available. Specifically, $\mathbf{h}_{e,k}$ and $\mathbf{g}_{e,k}$ are modeled as random vectors with distributions $\mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_a})$ and $\mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_c})$, respectively.

Given that Alice transmits signal vector $\mathbf{s}_a \in \mathbb{C}^{N_a}$ and Charlie transmits signal vector $\mathbf{s}_c \in \mathbb{C}^{N_c}$, received signals at Bob and the kth Eve ($k \in \mathcal{K}$) can be expressed as

$$y_b = \mathbf{h}_{ba}^H \mathbf{s}_a + \mathbf{h}_{bc}^H \mathbf{s}_c + n_b \tag{1}$$

$$y_{e,k} = \mathbf{h}_{e,k}^H \mathbf{s}_a + \mathbf{g}_{e,k}^H \mathbf{s}_c + n_{e,k} \tag{2}$$

where n_b, $n_{e,k} \sim \mathcal{CN}(0, 1)$ represent additive complex white Gaussian noises at Bob and the kth Eve, respectively. Note that the jamming signal $\mathbf{s}_c$ disrupts secret information receptions at both Bob and Eves. Thus, the secrecy performance is compromised if the transmission of $\mathbf{s}_c$ is not properly designed. To utilize this interference in a positive way, the zero-forcing constraint is imposed at Charlie. In other words, it nulls out the interference toward Bob when emitting jamming signals. Let $\mathbf{T}_c \in \mathbb{C}^{N_c \times (N_c-1)}$ be an orthonormal basis for null($\mathbf{h}_{bc}^H$). Then, we can construct $\mathbf{s}_c$ as

$$\mathbf{s}_c = \sqrt{P_c/(N_c-1)}\mathbf{T}_c \mathbf{z}_c \tag{3}$$

where P_c denotes the transmit power of Charlie; $\mathbf{z}_c \in \mathbb{C}^{N_c-1}$ is a Gaussian noise vector with distribution $\mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_c-1})$. Note that the transmit power of Charlie is equally assigned to N_c-1 entries of $\mathbf{z}_c$, since perfect CSIs of Eves are not available.

For secure transmission from Alice to Bob, AN-assisted secrecy beamforming is developed. Let $[\mathbf{t}_a, \mathbf{T}_a]$ be an orthonormal basis of $\mathbb{C}^{N_a}$, where $\mathbf{t}_a = \mathbf{h}_{ba}/\|\mathbf{h}_{ba}\|$ denotes the secrecy beamforming vector for Alice, and $\mathbf{T}_a$ is utilized for AN generation. Then, we can construct $\mathbf{s}_a$ as

$$\mathbf{s}_a = \sqrt{P_a \phi}\mathbf{t}_a x + \sqrt{P_a(1-\phi)/(N_a-1)}\mathbf{T}_a \mathbf{z}_a \tag{4}$$

where P_a denotes the transmit power of Alice; $\phi \in [0, 1]$ denotes the fraction of P_a allocated to the information-bearing signal; $x \sim \mathcal{CN}(0, 1)$ corresponds to the data symbol for Bob; $\mathbf{z}_a \in \mathbb{C}^{N_a-1}$ is a Gaussian noise vector with distribution $\mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_a-1})$. The first term on the right hand side of (4) represents the information-bearing signal, and the second term represents the AN signal. Note that $\phi = 1$ corresponds to the secrecy beamforming without AN, and $\phi = 0$ means that the secure transmission is suspended. In the latter case, Charlie also stops transmitting jamming signals for power saving.

According to (1)–(4), the signal-to-interference-plus-noise ratios (SINRs) at Bob and the kth Eve ($k \in \mathcal{K}$) are given by

$$\gamma_b(\phi) = P_a \phi \|\mathbf{h}_{ba}\|^2 \tag{5}$$

$$\gamma_{e,k}(\phi) = \frac{P_a \phi |\mathbf{h}_{e,k}^H \mathbf{t}_a|^2}{1 + \frac{P_a(1-\phi)}{N_a-1}\|\mathbf{h}_{e,k}^H \mathbf{T}_a\|^2 + \frac{P_c}{N_c-1}\|\mathbf{g}_{e,k}^H \mathbf{T}_c\|^2}. \tag{6}$$

Hence, capacities of the main channel and the kth eavesdropper channel ($k \in \mathcal{K}$) can be expressed as

$$C_b(\phi) = \log(1 + \gamma_b(\phi)) \qquad C_{e,k}(\phi) = \log(1 + \gamma_{e,k}(\phi)). \tag{7}$$

Utilizing Wyner's wiretap code [11], the secret information is encoded before transmission. Alice determines two rates, i.e., the overall codeword rate R_b and the rate of the secret message R_s (also called the *secrecy rate*). Then, the rate of redundant information $R_e \triangleq R_b - R_s$ can be deliberately added for anti-eavesdropping. In particular, to guarantee the reliable transmission without incurring the capacity outage at Bob, R_b needs to be adjusted to ensure that $R_b \le C_b(\phi)$.

We consider the wiretap scenario in which each Eve independently decodes the secret message based on its own observation. This corresponds to the compound wiretap channel model [37]. As long as at least one of Eves is able to wiretap the secret information, information-theoretic security cannot be guaranteed, and secrecy outage occurs. According to [18], the SOP is given as follows:

$$\begin{aligned}\varepsilon &= \Pr\{\max\nolimits_{k\in\mathcal{K}} C_{e,k}(\phi) > R_e\} \\ &= \Pr\{\max\nolimits_{k\in\mathcal{K}} \gamma_{e,k}(\phi) > 2^{R_b - R_s} - 1\}.\end{aligned} \tag{8}$$

It is observed from (8) that for any fixed $\phi \in (0, 1]$, ε decreases with R_b. Hence, Alice transmits the codeword at the maximum achievable rate, i.e., $R_b = C_b(\phi)$.

Let $R_{\text{th}} > 0$ be a minimum secrecy rate requirement. Then, the secrecy rate constrained SOPM problem is formulated as

$$\begin{aligned}\min\ \ &\varepsilon = \Pr\left\{\max\nolimits_{k\in\mathcal{K}} \gamma_{e,k}(\phi) > 2^{C_b(\phi)-R_s} - 1\right\} \\ \text{s.t.}\ \ &R_{\text{th}} \le R_s \le C_b(\phi);\ 0 < \phi \le 1.\end{aligned} \tag{9}$$

Next, we provide an explicit solution to this problem, by optimizing the secrecy rate and the power allocation ratio.

III. Secrecy Outage Probability Minimization

The SOPM problem (9) is difficult to be solved directly. The main obstacle lies in the probabilistic objective function. In this section, we divide the solution process into two steps. First, problem (9) is transformed into a tractable power allocation problem, by a change of variables and a transformation of the objective and constraint functions. Then, an efficient numerical method is developed to obtain the optimal solution.

A. Reformulation of the SOPM Problem (9)

Taking the objective function in problem (9) into account, it can be shown that ε increases with R_s for any fixed $\phi \in (0, 1]$. Therefore, the optimal secrecy rate (denoted by R_s^*) meets the minimum secrecy rate requirement with equality. In other words, $R_s^* = R_{\text{th}}$ must hold at the minimum SOP. Then, problem (9) can be reformulated as the following power allocation problem:

$$\begin{aligned}\min\ \ &\varepsilon = \Pr\left\{\max\nolimits_{k\in\mathcal{K}} \gamma_{e,k}(\phi) > 2^{C_b(\phi)-R_{\text{th}}} - 1\right\} \\ \text{s.t.}\ \ &R_{\text{th}} \le C_b(\phi);\quad 0 < \phi \le 1.\end{aligned} \tag{10}$$

Note that $C_b(\phi)$ in (7) is a strictly increasing function of ϕ. If $R_{\text{th}} = C_b(1)$, the only feasible solution is $\phi = 1$. In this case, we conclude that $\varepsilon = 1$, leading to an unacceptably high risk of secrecy outage. On the other hand, if $R_{\text{th}} > C_b(1)$, the minimum secrecy rate requirement cannot be guaranteed [i.e., problem (10) is infeasible]. In this case, the wiretap codes cannot be constructed since $C_b(1) - R_s < 0$. In the above

two cases, it is reasonable to suspend the secure transmission from Alice to Bob (i.e., $R_s = 0$ and $\phi = 0$), and thus $\varepsilon = 0$. For power saving, Charlie also suspends jamming signals transmission until the condition $R_{\text{th}} < C_b(1)$ is satisfied.

In the following, we assume that the condition $R_{\text{th}} < C_b(1)$ is satisfied, which is equivalent to

$$R_{\text{th}} < \log\Big(1 + P_a\|\mathbf{h}_{ba}\|^2\Big) \iff \phi_L \triangleq \frac{2^{R_{\text{th}}} - 1}{P_a\|\mathbf{h}_{ba}\|^2} < 1 \quad (11)$$

where ϕ_L is a lower bound on ϕ. Under the above condition, the wiretap codes can be constructed with rates $C_b(\phi)$ and R_s, and $\varepsilon < 1$ can be guaranteed. In addition, it can be shown that the constraint $R_{\text{th}} \le C_b(\phi)$ in problem (10) is equivalent to

$$R_{\text{th}} \le \log\Big(1 + P_a\phi\|\mathbf{h}_{ba}\|^2\Big) \iff \phi \ge \phi_L. \quad (12)$$

Hence, constraints in (10) can be rewritten as $\phi_L \le \phi \le 1$. Note that if $\phi = \phi_L$, we have $C_b(\phi) = R_{\text{th}}$, which immediately implies $\varepsilon = 1$. To prevent this situation, the constraint on ϕ is replaced by $\phi_L < \phi \le 1$, without affecting the optimal solution. Therefore, problem (10) can be recast as

$$\begin{aligned} \min\ \ & \varepsilon = \Pr\Big\{\max\nolimits_{k\in\mathcal{K}}\ \gamma_{e,k}(\phi) > 2^{C_b(\phi)-R_{\text{th}}} - 1\Big\} \\ \text{s.t.}\ \ & \phi \in \mathcal{C} \triangleq \{\phi | \phi_L < \phi \le 1\}. \end{aligned} \quad (13)$$

To simplify notations, new variables are defined as follows:

$$X_k \triangleq P_a\phi|\mathbf{h}_{e,k}^H\mathbf{t}_a|^2 \qquad Y_k \triangleq \frac{P_a(1-\phi)}{N_a - 1}\|\mathbf{h}_{e,k}^H\mathbf{T}_a\|^2 \quad (14)$$

$$Z_k \triangleq \frac{P_c}{N_c - 1}\|\mathbf{g}_{e,k}^H\mathbf{T}_c\|^2 \qquad \Upsilon_k \triangleq Y_k + Z_k \quad (15)$$

where $k \in \mathcal{K}$. It can be verified that $X_k \sim \text{Exp}(\lambda)$, $Y_k \sim \Gamma(\alpha_1, \lambda_1)$, and $Z_k \sim \Gamma(\alpha_2, \lambda_2)$, where $\alpha_1 \triangleq N_a - 1$, $\alpha_2 \triangleq N_c - 1$, $\lambda \triangleq 1/(P_a\phi)$, $\lambda_1 \triangleq \alpha_1/(P_a(1-\phi))$, and $\lambda_2 \triangleq \alpha_2/P_c$. According to (14) and (15), the SINR at the kth Eve [see expression (6)] can be rewritten as

$$\gamma_{e,k} = X_k/(1 + \Upsilon_k),\ \ k \in \mathcal{K}. \quad (16)$$

By [38, Ch. 2.7, Th. 2], $\gamma_{e,1}, \gamma_{e,2}, \ldots, \gamma_{e,K}$ are independent and identically distributed random variables. Hence, the objective function in problem (13) is given by

$$\begin{aligned} \varepsilon &= 1 - \Pr\Big\{\max\nolimits_{k\in\mathcal{K}}\ \gamma_{e,k} \le 2^{C_b(\phi)-R_{\text{th}}} - 1\Big\} \\ &= 1 - \Big(\Pr\Big\{\gamma_{e,k} \le 2^{C_b(\phi)-R_{\text{th}}} - 1\Big\}\Big)^K \\ &= 1 - \Big(1 - \bar{F}_{\gamma_{e,k}}\Big(2^{C_b(\phi)-R_{\text{th}}} - 1\Big)\Big)^K \end{aligned} \quad (17)$$

where $\bar{F}_{\gamma_{e,k}}(x) \triangleq \Pr\{\gamma_{e,k} > x\}$ is the complementary cumulative distribution function (CCDF) of $\gamma_{e,k}$. Thus, minimizing ε in (17) is the same as minimizing $\bar{F}_{\gamma_{e,k}}(2^{C_b(\phi)-R_{\text{th}}} - 1)$, which is equivalent to maximizing $-\ln(\bar{F}_{\gamma_{e,k}}(2^{C_b(\phi)-R_{\text{th}}} - 1))$.

To further simplify notations, we define $\mu \triangleq 2^{C_b(\phi)-R_{\text{th}}} - 1$. Consequently, problem (13) can be rewritten as

$$\begin{aligned} \max_{\phi\in\mathcal{C}}\ \ & -\ln\big(\bar{F}_{\gamma_{e,k}}(\mu)\big) \\ \text{s.t.}\ \ & R_{\text{th}} = C_b(\phi) - \log(1+\mu). \end{aligned} \quad (18)$$

To obtain a closed form expression for the objective function in problem (18), we need the following proposition.

Proposition 1: The CCDF of $\gamma_{e,k}$ can be characterized as

$$\bar{F}_{\gamma_{e,k}}(\tau) = \left(\frac{\lambda_1}{\lambda_1 + \lambda\tau}\right)^{\alpha_1}\left(\frac{\lambda_2}{\lambda_2 + \lambda\tau}\right)^{\alpha_2}\frac{1}{e^{\lambda\tau}} \quad (19)$$

where $k \in \mathcal{K}$ and $\tau > 0$.

Proof: Please refer to Appendix A. ■

According to Proposition 1, we can conclude that

$$-\ln\big(\bar{F}_{\gamma_{e,k}}(\mu)\big) = \lambda\mu + \alpha_1\ln\left(1 + \frac{\lambda\mu}{\lambda_1}\right) + \alpha_2\ln\left(1 + \frac{\lambda\mu}{\lambda_2}\right). \quad (20)$$

Making the transformation $w = \mu/\phi$, problem (18) can be reformulated as the following problem:

$$\begin{aligned} \max_{\phi\in\mathcal{C}}\ \ & f = \frac{w}{P_a} + \alpha_1\ln\left(1 + \frac{(1-\phi)w}{\alpha_1}\right) + \alpha_2\ln\left(1 + \frac{w}{d}\right) \\ \text{s.t.}\ \ & R_{\text{th}} = \log(1 + \phi\gamma_B) - \log(1 + \phi w) \end{aligned} \quad (21)$$

where $\gamma_B \triangleq P_a\|\mathbf{h}_{ba}\|^2$ and $d \triangleq P_a\lambda_2$.

Remark 1: The parameter w is determined by the secrecy rate constraint in problem (21). In particular, w can be taken as a function of ϕ, which is expressed as

$$w(\phi) = \frac{1 + \phi\gamma_B - 2^{R_{\text{th}}}}{\phi 2^{R_{\text{th}}}} = \frac{\gamma_B}{2^{R_{\text{th}}}} - \left(\frac{2^{R_{\text{th}}} - 1}{2^{R_{\text{th}}}}\right)\frac{1}{\phi}. \quad (22)$$

Therefore, the objective function f in problem (21) can be considered as a function of ϕ, which is denoted by $f(\phi)$.

Remark 2: The reformulated problem (21) is independent of the number of Eves. Thus, the optimal solution is independent of the number of Eves.

Remark 3: The number of Eves has a great impact on the SOP performance. Let ϕ^* be the optimal solution of (21). The corresponding SOP can be calculated as

$$\varepsilon = 1 - \Big(1 - e^{-f(\phi^*)}\Big)^K. \quad (23)$$

It can be shown from (23) that ε increases with K.

B. Optimization of Power Allocation for Problem (21)

Analyzing function (22), we obtain the following lemma.

Lemma 1: $w(\phi)$ in (22) is a strictly increasing function over $\mathcal{C}$, and is also a strictly concave function over $\mathcal{C}$.

Proof: It can be verified that the inequality $w'(\phi) > 0$ holds for all $\phi \in \mathcal{C}$. In addition, the concavity of $w(\phi)$ can be verified directly by the second order condition [35]. ■

By analyzing the objective function in problem (21) and using Lemma 1, we have the following proposition.

Proposition 2: $f(\phi)$ is a strictly concave function over $\mathcal{C}$.

Proof: The derivative of $f(\phi)$ can be calculated as

$$\begin{aligned} f'(\phi) &= \frac{w'(\phi)}{P_a} + \frac{\alpha_1(1-\phi)w'(\phi) - \alpha_1 w(\phi)}{\alpha_1 + (1-\phi)w(\phi)} + \frac{\alpha_2 w'(\phi)}{w(\phi) + d} \\ &= \underbrace{\left(\frac{1}{P_a} + \frac{\alpha_1}{\frac{\alpha_1}{1-\phi} + w(\phi)} + \frac{\alpha_2}{w(\phi) + d}\right)w'(\phi)}_{\triangleq A(\phi)} \\ &\quad - \underbrace{\frac{\alpha_1}{\frac{\alpha_1}{w(\phi)} + 1 - \phi}}_{\triangleq B(\phi)}. \end{aligned} \quad (24)$$

From Lemma 1, we obtain that $w'(\phi) > 0$ and $w''(\phi) < 0$. It follows that $A(\phi)$ and $B(\phi)$ in (24) are strictly decreasing and increasing functions over $\mathcal{C}$, respectively. Hence, $f'(\phi)$ is a strictly decreasing function, i.e., $f''(\phi) < 0$ for all $\phi \in \mathcal{C}$. This completes the proof of Proposition 2. ■

Corollary 1: If $f'(1) \geq 0$, then $f(\phi)$ is a strictly increasing function over $\mathcal{C}$.

Proof: By Proposition 2, it follows that the inequality $f'(\phi) > f'(1) \geq 0$ holds for all $\phi \in (\phi_L, 1)$. Therefore, the desired result can be established. ■

With the above results, an efficient numerical method for solving problem (21) can be developed, where two different cases are characterized as follows.

1) *Case 1:* $f'(1) \geq 0$. According to Corollary 1, the optimal solution is $\phi^* = 1$ (i.e., Alice performs secrecy beamforming without AN). From (23), the corresponding SOP is given by

$$\varepsilon = 1 - \left(1 - e^{-f(1)}\right)^K. \tag{25}$$

2) *Case 2:* $f'(1) < 0$. Since $w(\phi_L) = 0$, it follows by (24) that:

$$f'(\phi_L) = \left(\frac{1}{P_a} + 1 - \phi_L + \frac{\alpha_2}{d}\right) w'(\phi_L). \tag{26}$$

From Lemma 1, we have $f'(\phi_L) > 0$. Combining this with $f'(1) < 0$ and using Proposition 2, we can conclude that there is an unique optimal solution $\phi^* \in (\phi_L, 1)$ such that

$$f'(\phi^*) = 0 \tag{27}$$

$$w(\phi^*) = \frac{\gamma_B}{2^{R_{\text{th}}}} - \left(\frac{2^{R_{\text{th}}} - 1}{2^{R_{\text{th}}}}\right) \frac{1}{\phi^*}. \tag{28}$$

In this case, secrecy beamforming with AN is performed at Alice. The corresponding SOP can be obtained by (23).

The above results give us some insights as summarized in the following Remark 4.

Remark 4: It is interesting to consider the physical implications of the above two cases [i.e., $f'(1) \geq 0$ and $f'(1) < 0$]. From (24), $f'(1)$ can be expressed as

$$f'(1) = \frac{w'(1)}{P_a} - w(1) + \frac{\alpha_2 w'(1)}{w(1) + d} = \frac{-w^2(1) + bw(1) + c}{w(1) + d} \tag{29}$$

where

$$b = \frac{w'(1)}{P_a} - d = \frac{2^{R_{\text{th}}} - 1}{P_a 2^{R_{\text{th}}}} - \frac{P_a(N_c - 1)}{P_c} \tag{30}$$

$$c = \left(\frac{d}{P_a} + \alpha_2\right) w'(1) = \frac{(N_c - 1)\left(2^{R_{\text{th}}} - 1\right)(1 + P_c)}{P_c 2^{R_{\text{th}}}}. \tag{31}$$

By (22) and Lemma 1, we can conclude that for all $\phi \in \mathcal{C}$

$$w(1) \geq w(\phi) > w(\phi_L) = 0. \tag{32}$$

The denominator of (29) is positive, and hence the sign of $f'(1)$ is determined by the numerator. Consider the function $s(x) = -x^2 + bx + c$ defined over $\mathbb{R}$. According to the quadratic formula, the two roots of the equation $s(x) = 0$ are given by

$$x_1 = \frac{b + \sqrt{b^2 + 4c}}{2} > 0 \quad x_2 = \frac{b - \sqrt{b^2 + 4c}}{2} < 0. \tag{33}$$

Since $f'(1) \geq 0$ is equivalent to $-w^2(1) + bw(1) + c \geq 0$, it follows by (33) that $w(1) \leq x_1$, which is further equivalent to

$$\frac{\gamma_B - 2^{R_{\text{th}}} + 1}{2^{R_{\text{th}}}} = w(1) \leq \frac{b + \sqrt{b^2 + 4c}}{2} \iff \|\mathbf{h}_{ba}\|^2 \leq \rho_{\text{th}} \tag{34}$$

where

$$\rho_{\text{th}} \triangleq \frac{2^{R_{\text{th}}}\left(b + \sqrt{b^2 + 4c}\right)}{2P_a} + 2^{R_{\text{th}}}(b + d) \tag{35}$$

denotes a threshold related to the main channel quality (denoted by $\|\mathbf{h}_{ba}\|^2$). Similarly, we can verify that $f'(1) < 0 \iff \|\mathbf{h}_{ba}\|^2 > \rho_{\text{th}}$. In other words, when the main channel quality is lower than a threshold, i.e., $\|\mathbf{h}_{ba}\|^2 \leq \rho_{\text{th}}$, the optimal solution is $\phi^* = 1$. In this case, it is optimal for Alice to carry out secrecy beamforming with full transmit power. However, when $\|\mathbf{h}_{ba}\|^2 > \rho_{\text{th}}$, the unique optimal solution can be obtained by solving (27) and (28), where $\phi^* \in (\phi_L, 1)$. In this case, secrecy beamforming with AN is performed at Alice.

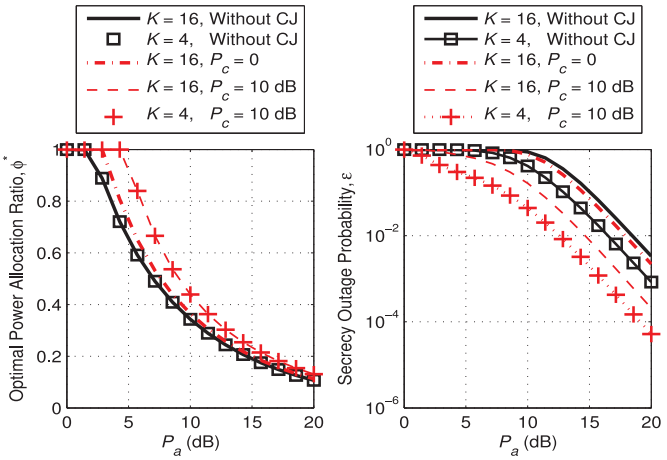


Fig. 2. Optimal power allocation ratio ϕ^* and the corresponding SOP ε.

Furthermore, the following propositions characterize the relationship between the main channel quality and the optimal power allocation ratio, as well as the impact of the minimum secrecy rate requirement on the SOP performance.

Proposition 3: For problem (21), the power allocated to the AN signal increases as the main channel quality improves. The corresponding SOP decreases.

Proof: Please refer to Appendix B. ■

Proposition 4: For problem (21), a higher secrecy rate requirement leads to more power allocated to the information-bearing signal. The corresponding SOP increases.

Proof: Please refer to Appendix C. ■

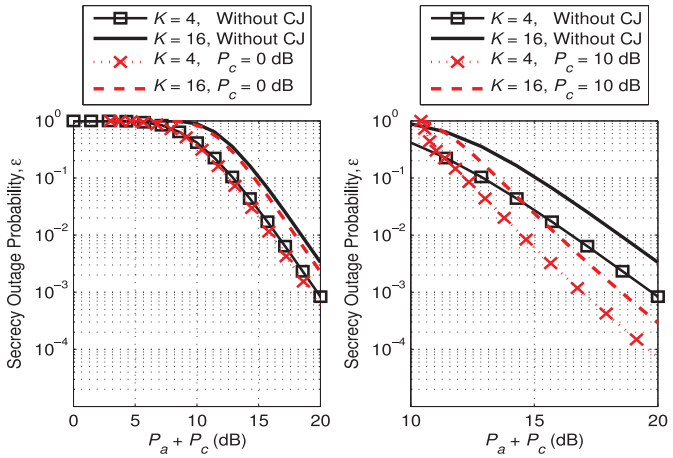


Fig. 3. SOP ε versus the total transmit power $P_a + P_c$.

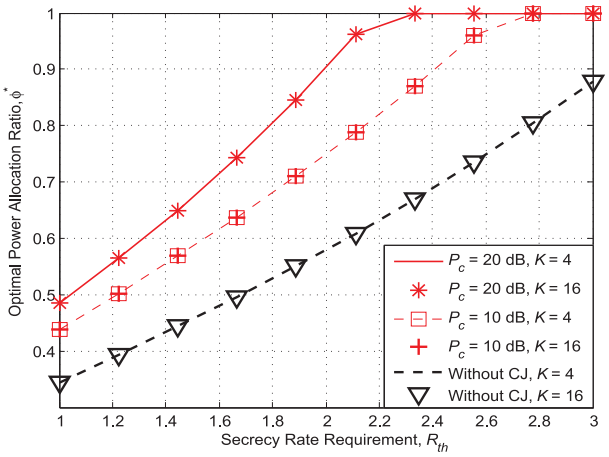


Fig. 6. Optimal power allocation ratio ϕ^* versus R_{th}, with $P_a = 10$ dB.

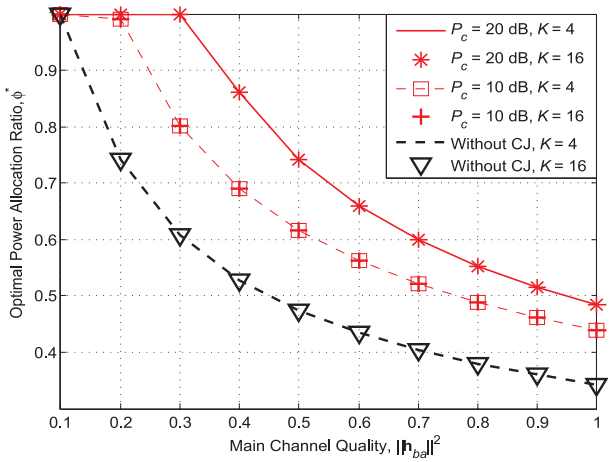


Fig. 4. Optimal power allocation ratio ϕ^* versus $\|\mathbf{h}_{ba}\|^2$, with $P_a = 10$ dB.

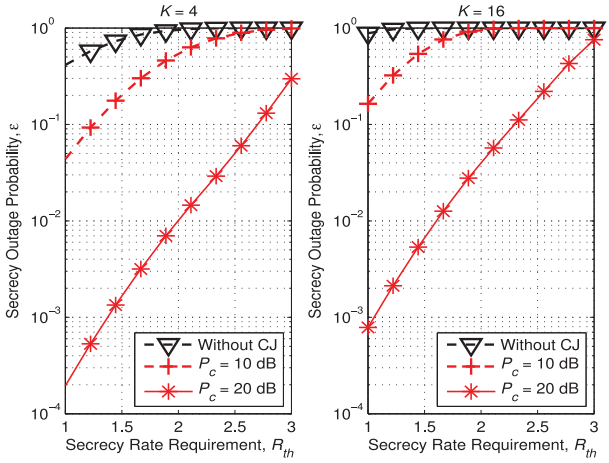


Fig. 7. SOP ε versus R_{th}, with $P_a = 10$ dB.

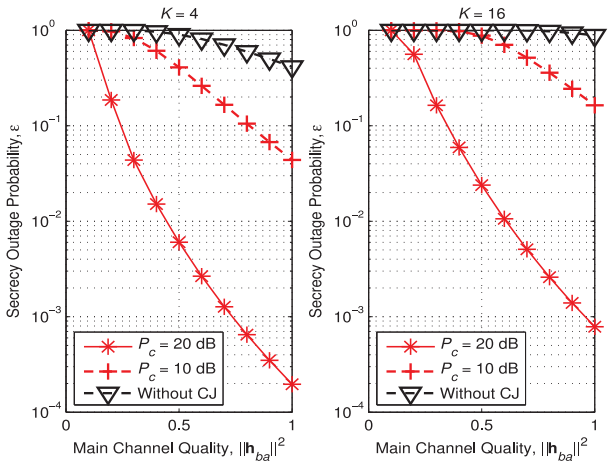


Fig. 5. SOP ε versus $\|\mathbf{h}_{ba}\|^2$, with $P_a = 10$ dB.

IV. Numerical Results

In this section, we verify the performance of the proposed CJ scheme. System parameters are set as $N_a = N_b = 4$. The secrecy rate is measured by bits per channel use (bpcu). Unless otherwise specified, we set $\|\mathbf{h}_{ba}\|^2 = 1$ and $R_{\text{th}} = 1$ bpcu.

Fig. 2 shows the optimal power allocation ratio ϕ^* versus P_a and the corresponding SOP ε versus P_a. It can be shown that ϕ^* in the proposed CJ scheme is higher than that without CJ. For the CJ scheme, ϕ^* decreases with P_a, and increases with P_c. Besides, ϕ^* is independent of the number of Eves K, which is consistent with Remark 2. However, the SOP performance is degraded as K increases. In addition, we observe that the SOP performance is enhanced with CJ scheme. This is mainly due to the jamming signal transmitted by Charlie, which causes significant performance degradation at Eves. Another reason is that the CJ scheme consumes more power than the approach without CJ. However, as shown in Fig. 3, a lower SOP can be achieved by the CJ scheme in a wide range of total transmit power. This reveals that the CJ scheme is more efficient in power resource utilization.

Figs. 4 and 5 present the impact of the main channel quality $\|\mathbf{h}_{ba}\|^2$ on ϕ^* and ε. It can be observed from Fig. 4 that when the main channel quality improves, more power should be allocated to the AN signal. The corresponding SOP decreases as $\|\mathbf{h}_{ba}\|^2$ increases, as shown in Fig. 5. These observations are consistent with Proposition 3. Fig. 4 also shows that more power should be allocated to the information-bearing signal when P_c increases.

Figs. 6 and 7 show the impact of the secrecy rate requirement R_{th} on ϕ^* and ε. Note that to minimize the SOP, Alice selects the secrecy rate as $R_s = R_{\text{th}}$ (see Section III-A for details). From Fig. 6, we observe that ϕ^* increases with R_{th}. The corresponding SOP also increases with R_{th}, as shown in Fig. 7. These observations are consistent with Proposition 4.

V. Conclusion

We investigated secure downlink transmission in IoT networks, and proposed a CJ scheme to enhance PLS. Specifically, we provided an explicit transmit design for minimizing the SOP, subject to a minimum secrecy rate constraint. Moreover, we characterized the impacts of specific parameters on the optimal power allocation between information-bearing signal and AN signal. Based on our in-depth theoretical analysis, we concluded that more power should be allocated to the AN signal when the main channel quality improves, and to the information-bearing signal when the secrecy rate increases. Numerical results confirmed that the SOP performance and power efficiency can be enhanced with the proposed CJ scheme, as compared with the approach without CJ.

Appendix A
Proof of Proposition 1

Proof: According to [36, 3.383.1] and [38], the probability density function of Υ_k, $k \in \mathcal{K}$, can be calculated as follows:

$$\begin{aligned} f_{\Upsilon_k}(\upsilon) &= \int_{-\infty}^{\infty} f_{Y_k}(\upsilon - z) f_{Z_k}(z) dz \\ &= \frac{\lambda_1^{\alpha_1}\lambda_2^{\alpha_2} e^{-\lambda_1 \upsilon}}{\Gamma(\alpha_1)\Gamma(\alpha_2)} \int_0^{\upsilon} z^{\alpha_2 - 1} (\upsilon - z)^{\alpha_1 - 1} e^{(\lambda_1 - \lambda_2) z} dz \\ &= \frac{\lambda_1^{\alpha_1}\lambda_2^{\alpha_2} \upsilon^{\alpha_1+\alpha_2-1}}{e^{\lambda_1 \upsilon}\Gamma(\alpha_1+\alpha_2)} {}_1F_1(\alpha_2; \alpha_1+\alpha_2; (\lambda_1-\lambda_2)\upsilon) \end{aligned} \quad (36)$$

where $\upsilon > 0$, and the last equality follows from the fact that $\alpha_1 > 0$ and $\alpha_2 > 0$.

From (36), the CCDF of $\gamma_{e,k}$, $k \in \mathcal{K}$, can be calculated as

$$\begin{aligned} \bar{F}_{\gamma_{e,k}}(\tau) &= \Pr(\gamma_{e,k} > \tau) \\ &= \Pr(X_k > \tau + \tau \Upsilon_k) \\ &= \int_0^{\infty} \left(\int_{\tau+\tau\upsilon}^{\infty} \lambda e^{-\lambda x} dx \right) f_{\Upsilon_k}(\upsilon) d\upsilon \\ &= \frac{\lambda_1^{\alpha_1}\lambda_2^{\alpha_2} e^{-\lambda\tau}}{\Gamma(\alpha_1+\alpha_2)} \int_0^{\infty} \frac{\upsilon^{\alpha_1+\alpha_2-1}}{e^{(\lambda_1+\lambda\tau)\upsilon}} \\ &\quad \times {}_1F_1(\alpha_2; \alpha_1+\alpha_2; (\lambda_1-\lambda_2)\upsilon) d\upsilon \end{aligned} \quad (37)$$

where $\tau > 0$. According to (37), we can obtain a closed form expression for $\bar{F}_{\gamma_{e,k}}(\tau)$. Three cases are considered as follows.

1) If $\lambda_1 = \lambda_2$, we have

$$\begin{aligned} \bar{F}_{\gamma_{e,k}}(\tau) &= \frac{\lambda_1^{\alpha_1+\alpha_2} e^{-\lambda\tau}}{\Gamma(\alpha_1+\alpha_2)} \int_0^{\infty} \frac{\upsilon^{\alpha_1+\alpha_2-1}}{e^{(\lambda_1+\lambda\tau)\upsilon}} d\upsilon \\ &= \frac{\lambda_1^{\alpha_1+\alpha_2} e^{-\lambda\tau}}{(\lambda_1+\lambda\tau)^{\alpha_1+\alpha_2}}. \end{aligned} \quad (38)$$

2) If $\lambda_1 > \lambda_2$, we obtain that

$$\lambda_1 + \lambda\tau > \lambda_1 - \lambda_2 > 0 \implies |\lambda_1 + \lambda\tau| > |\lambda_1 - \lambda_2|. \quad (39)$$

Hence by [36, 7.621.4], we have

$$\begin{aligned} \bar{F}_{\gamma_{e,k}}(\tau) &= \frac{\lambda_1^{\alpha_1}\lambda_2^{\alpha_2} e^{-\lambda\tau}}{(\lambda_1+\lambda\tau)^{\alpha_1+\alpha_2}} {}_2F_1\left(\alpha_2, \alpha_1+\alpha_2; \alpha_1 + \alpha_2; \frac{\lambda_1-\lambda_2}{\lambda_1+\lambda\tau}\right) \\ &= \left(\frac{\lambda_1}{\lambda_1+\lambda\tau}\right)^{\alpha_1} \left(\frac{\lambda_2}{\lambda_2+\lambda\tau}\right)^{\alpha_2} \frac{1}{e^{\lambda\tau}}. \end{aligned} \quad (40)$$

3) If $\lambda_1 < \lambda_2$, we can conclude that

$$\lambda_2 + \lambda\tau > \lambda_2 - \lambda_1 > 0 \implies |\lambda_2 + \lambda\tau| > |\lambda_2 - \lambda_1|. \quad (41)$$

Therefore, by [36, 7.621.4], it follows that:

$$\begin{aligned} \bar{F}_{\gamma_{e,k}}(\tau) &= \frac{\lambda_1^{\alpha_1}\lambda_2^{\alpha_2} e^{-\lambda\tau}}{\Gamma(\alpha_1+\alpha_2)} \int_0^{\infty} \frac{e^{(\lambda_1-\lambda_2)\upsilon}}{e^{(\lambda_1+\lambda\tau)\upsilon}} \upsilon^{\alpha_1+\alpha_2-1} \\ &\quad \times {}_1F_1(\alpha_1; \alpha_1+\alpha_2; (\lambda_2-\lambda_1)\upsilon) d\upsilon \\ &= \frac{\lambda_1^{\alpha_1}\lambda_2^{\alpha_2} e^{-\lambda\tau}}{(\lambda_2+\lambda\tau)^{\alpha_1+\alpha_2}} {}_2F_1\left(\alpha_1, \alpha_1+\alpha_2; \alpha_1 + \alpha_2; \frac{\lambda_2-\lambda_1}{\lambda_2+\lambda\tau}\right) \\ &= \left(\frac{\lambda_1}{\lambda_1+\lambda\tau}\right)^{\alpha_1} \left(\frac{\lambda_2}{\lambda_2+\lambda\tau}\right)^{\alpha_2} \frac{1}{e^{\lambda\tau}}. \end{aligned} \quad (42)$$

Finally, combining (38), (40), and (42), we conclude that

$$\bar{F}_{\gamma_{e,k}}(\tau) = \left(\frac{\lambda_1}{\lambda_1+\lambda\tau}\right)^{\alpha_1} \left(\frac{\lambda_2}{\lambda_2+\lambda\tau}\right)^{\alpha_2} \frac{1}{e^{\lambda\tau}}. \quad (43)$$

This completes the proof of Proposition 1. ■

Appendix B
Proof of Proposition 3

Proof: Let $\|\mathbf{h}_{ba}^{(i)}\|^2$ denote the main channel quality, and assume that the optimal solution to problem (21) is ϕ_i^*, where $i \in \{1, 2\}$. In order to simplify notations, we define the following vectors:

$$\mathbf{x}_i = \left(\left\|\mathbf{h}_{ba}^{(i)}\right\|, \phi_i\right) \quad \mathbf{x}_i^* = \left(\left\|\mathbf{h}_{ba}^{(i)}\right\|, \phi_i^*\right), \quad i \in \{1, 2\}. \quad (44)$$

Then, the optimal value of problem (21) can be rewritten as

$$\begin{aligned} f(\mathbf{x}_i^*) &= \frac{w(\mathbf{x}_i^*)}{P_a} + \alpha_1 \ln\left(1 + \frac{(1-\phi_i^*)w(\mathbf{x}_i^*)}{\alpha_1}\right) \\ &\quad + \alpha_2 \ln\left(1 + \frac{w(\mathbf{x}_i^*)}{d}\right), \quad i \in \{1, 2\} \end{aligned} \quad (45)$$

where $w(\mathbf{x}_i^*)$ satisfies the following secrecy rate constraint:

$$R_{\text{th}} = \log\left(1 + \phi_i^* P_a \left\|\mathbf{h}_{ba}^{(i)}\right\|^2\right) - \log\left(1 + \phi_i^* w(\mathbf{x}_i^*)\right). \quad (46)$$

Therefore, according to (23), the corresponding SOP can be calculated as

$$\varepsilon(\mathbf{x}_i^*) = 1 - \left(1 - e^{-f(\mathbf{x}_i^*)}\right)^K \quad i \in \{1, 2\}. \quad (47)$$

Without loss of generality, we assume that $\|\mathbf{h}_{ba}^{(1)}\|^2 < \|\mathbf{h}_{ba}^{(2)}\|^2$. In the following, we prove that $\phi_1^* \geq \phi_2^*$ and $\varepsilon(\mathbf{x}_1^*) > \varepsilon(\mathbf{x}_2^*)$.

First, from (22), $w(\mathbf{x}_i)$ and the derivative of $w(\mathbf{x}_i)$ with respect to ϕ_i can be expressed as

$$w(\mathbf{x}_i) = \frac{P_a \left\| \mathbf{h}_{ba}^{(i)} \right\|^2}{2^{R_{\text{th}}}} - \left(\frac{2^{R_{\text{th}}} - 1}{2^{R_{\text{th}}}} \right) \frac{1}{\phi_i} \tag{48}$$

$$w'(\mathbf{x}_i) = \frac{2^{R_{\text{th}}} - 1}{2^{R_{\text{th}}}} \frac{1}{\phi_i^2}. \tag{49}$$

Then, from (24), the derivative of $f(\mathbf{x}_i)$ with respect to ϕ_i is given by

$$\begin{aligned} f'(\mathbf{x}_i) &= \frac{w'(\mathbf{x}_i)}{P_a} + \frac{\alpha_1(1-\phi_i)w'(\mathbf{x}_i) - \alpha_1 w(\mathbf{x}_i)}{\alpha_1 + (1-\phi_i)w(\mathbf{x}_i)} + \frac{\alpha_2 w'(\mathbf{x}_i)}{w(\mathbf{x}_i) + d} \\ &= w'(\mathbf{x}_i) \left(\frac{1}{P_a} + \frac{\alpha_1}{\frac{\alpha_1}{1-\phi_i} + w(\mathbf{x}_i)} + \frac{\alpha_2}{w(\mathbf{x}_i) + d} \right) \\ &\quad - \frac{\alpha_1}{\frac{\alpha_1}{w(\mathbf{x}_i)} + (1-\phi_i)}. \end{aligned} \tag{50}$$

In particular, two cases are considered to complete the proof.

1) *Case 1:* $\|\mathbf{h}_{ba}^{(1)}\|^2 \le \rho_{\text{th}}$. According to Remark 4, we can conclude that $f'(\mathbf{x}_1^*) \ge 0$ and $\phi_1^* = 1$. Next, two different situations can be considered as follows.
   a) $\|\mathbf{h}_{ba}^{(1)}\|^2 < \|\mathbf{h}_{ba}^{(2)}\|^2 \le \rho_{\text{th}}$. From Remark 4, we obtain that $\phi_1^* = \phi_2^* = 1$, and thus by (48), $w(\mathbf{x}_2^*) > w(\mathbf{x}_1^*)$. Then from (45) we have $f(\mathbf{x}_2^*) > f(\mathbf{x}_1^*)$. Therefore, from (47), we can conclude that $\varepsilon(\mathbf{x}_2^*) < \varepsilon(\mathbf{x}_1^*)$.
   b) $\|\mathbf{h}_{ba}^{(1)}\|^2 \le \rho_{\text{th}} < \|\mathbf{h}_{ba}^{(2)}\|^2$. From Remark 4, we have $\phi_L^{(2)} < \phi_2^* < \phi_1^* = 1$ and $f'(\mathbf{x}_2^*) = 0$, where $\phi_L^{(2)} = (2^{R_{\text{th}}} - 1)/(P_a \|\mathbf{h}_{ba}^{(2)}\|^2)$. Then, from (49), we get $w'(\mathbf{x}_1^*) < w'(\mathbf{x}_2^*)$. To prove $w(\mathbf{x}_2^*) > w(\mathbf{x}_1^*)$, we assume in contradiction that $w(\mathbf{x}_2^*) \le w(\mathbf{x}_1^*)$. Since $f'(\mathbf{x}_1^*) \ge f'(\mathbf{x}_2^*) = 0$, it follows by (49) and (50) that:

$$\frac{w(\mathbf{x}_2^*)}{1 + \frac{(1-\phi_2^*)w(\mathbf{x}_2^*)}{\alpha_1}} > w(\mathbf{x}_1^*) \implies \phi_2^* > 1 \tag{51}$$

   which is a contradiction to the fact that $\phi_2^* < 1$. We thus conclude that $w(\mathbf{x}_2^*) > w(\mathbf{x}_1^*)$. Then, from (45) we have $f(\mathbf{x}_2^*) > f(\mathbf{x}_1^*)$. Therefore, from (47), we get $\varepsilon(\mathbf{x}_2^*) < \varepsilon(\mathbf{x}_1^*)$.
2) *Case 2:* $\|\mathbf{h}_{ba}^{(1)}\|^2 > \rho_{\text{th}}$. Since $\|\mathbf{h}_{ba}^{(2)}\|^2 > \|\mathbf{h}_{ba}^{(1)}\|^2 > \rho_{\text{th}}$, it follows by Remark 4 that $f'(\mathbf{x}_1^*) = f'(\mathbf{x}_2^*) = 0$, $\phi_1^* < 1$, and $\phi_2^* < 1$. To prove $\phi_2^* < \phi_1^*$, suppose in contradiction that $\phi_2^* \ge \phi_1^*$. Then, from (48), we obtain $w(\mathbf{x}_2^*) > w(\mathbf{x}_1^*)$ and $w'(\mathbf{x}_2) \le w'(\mathbf{x}_1)$. Hence, from (49) and (50), we have $f'(\mathbf{x}_2^*) < f'(\mathbf{x}_1^*)$, contradicting that $f'(\mathbf{x}_1^*) = f'(\mathbf{x}_2^*) = 0$. We thus conclude that $\phi_2^* < \phi_1^*$ and $w'(\mathbf{x}_2) > w'(\mathbf{x}_1)$. To prove $w(\mathbf{x}_2^*) > w(\mathbf{x}_1^*)$, we assume in contradiction that $w(\mathbf{x}_2^*) \le w(\mathbf{x}_1^*)$. Then, from (49) and (50), we obtain that $f'(\mathbf{x}_2^*) > f'(\mathbf{x}_1^*)$, which is a contradiction to $f'(\mathbf{x}_1^*) = f'(\mathbf{x}_2^*) = 0$. We thus have $w(\mathbf{x}_2^*) > w(\mathbf{x}_1^*)$. Then by (45), we can conclude that $f(\mathbf{x}_2^*) > f(\mathbf{x}_1^*)$, and hence by (47), we get $\varepsilon(\mathbf{x}_2^*) < \varepsilon(\mathbf{x}_1^*)$.

Hence, we conclude that if $\|\mathbf{h}_{ba}^{(1)}\|^2 < \|\mathbf{h}_{ba}^{(2)}\|^2$, then $\phi_1^* \ge \phi_2^*$ and $\varepsilon(\mathbf{x}_1^*) \ge \varepsilon(\mathbf{x}_2^*)$. This result can be expressed in (52), shown at the top of the next page. ■

APPENDIX C
PROOF OF PROPOSITION 4

Proof: Let $R_{\text{th}}^{(i)}$ denote the minimum secrecy rate requirement, and assume that the optimal solution to problem (21) is ϕ_i^*, where $i \in \{1, 2\}$. In order to simplify notations, we define the following vectors:

$$\mathbf{x}_i = \left(R_{\text{th}}^{(i)}, \phi_i \right) \quad \mathbf{x}_i^* = \left(R_{\text{th}}^{(i)}, \phi_i^* \right) \quad \mathbf{y}_i = \left(R_{\text{th}}^{(i)}, 1 \right), i \in \{1, 2\}. \tag{53}$$

Then, the optimal value of the objective function in (21) is

$$\begin{aligned} f(\mathbf{x}_i^*) &= \frac{w(\mathbf{x}_i^*)}{P_a} + \alpha_1 \ln \left(1 + \frac{(1-\phi_i^*)w(\mathbf{x}_i^*)}{\alpha_1} \right) \\ &\quad + \alpha_2 \ln \left(1 + \frac{w(\mathbf{x}_i^*)}{d} \right), \quad i \in \{1, 2\} \end{aligned} \tag{54}$$

where $w(\mathbf{x}_i^*)$ satisfies the following secrecy rate constraint:

$$R_{\text{th}}^{(i)} = \log(1 + \phi_i^* \gamma_B) - \log(1 + \phi_i^* w(\mathbf{x}_i^*)). \tag{55}$$

Then, from (23), the corresponding SOP can be calculated as

$$\varepsilon(\mathbf{x}_i^*) = 1 - \left(1 - e^{-f(\mathbf{x}_i^*)} \right)^K, \quad i \in \{1, 2\}. \tag{56}$$

Without loss of generality, we assume that $R_{\text{th}}^{(1)} < R_{\text{th}}^{(2)}$. In the following, we prove that $\phi_1^* \le \phi_2^*$ and $\varepsilon(\mathbf{x}_1^*) < \varepsilon(\mathbf{x}_2^*)$.

According to (22), $w(\mathbf{x}_i)$ and the derivative of $w(\mathbf{x}_i)$ with respect to ϕ_i can be expressed as

$$w(\mathbf{x}_i) = \frac{\gamma_B}{2^{R_{\text{th}}^{(i)}}} - \left(\frac{2^{R_{\text{th}}^{(i)}} - 1}{2^{R_{\text{th}}^{(i)}}} \right) \frac{1}{\phi_i} \quad w'(\mathbf{x}_i) = \left(\frac{2^{R_{\text{th}}^{(i)}} - 1}{2^{R_{\text{th}}^{(i)}}} \right) \frac{1}{\phi_i^2}. \tag{57}$$

From (53) and (57), we obtain that

$$w(\mathbf{y}_1) > w(\mathbf{y}_2) \qquad w'(\mathbf{y}_1) < w'(\mathbf{y}_2). \tag{58}$$

By (24), the derivative of $f(\mathbf{x}_i)$ with respect to ϕ_i is given by

$$\begin{aligned} f'(\mathbf{x}_i) &= \frac{w'(\mathbf{x}_i)}{P_a} + \frac{\alpha_1(1-\phi_i)w'(\mathbf{x}_i) - \alpha_1 w(\mathbf{x}_i)}{\alpha_1 + (1-\phi_i)w(\mathbf{x}_i)} + \frac{\alpha_2 w'(\mathbf{x}_i)}{w(\mathbf{x}_i) + d} \\ &= w'(\mathbf{x}_i) \left(\frac{1}{P_a} + \frac{\alpha_1}{\frac{\alpha_1}{1-\phi_i} + w(\mathbf{x}_i)} + \frac{\alpha_2}{w(\mathbf{x}_i) + d} \right) \\ &\quad - \frac{\alpha_1}{\frac{\alpha_1}{w(\mathbf{x}_i)} + (1-\phi_i)}. \end{aligned} \tag{59}$$

From (58) and (59), we conclude that $f'(\mathbf{y}_2) > f'(\mathbf{y}_1)$. Next, two cases are considered to complete the proof.

1) *Case 1:* $f'(\mathbf{y}_1) \ge 0$. As discussed in Section III-B, we have $f'(\mathbf{y}_1) \ge 0$ and $\phi_1^* = 1$. Since $f'(\mathbf{y}_2) > f'(\mathbf{y}_1)$, it follows that $\phi_2^* = 1$. Then, combining (54) and (58), we get $f(\mathbf{x}_2^*) < f(\mathbf{x}_1^*)$. Thus, from (56), we have $\varepsilon(\mathbf{x}_2^*) > \varepsilon(\mathbf{x}_1^*)$.
2) *Case 2:* $f'(\mathbf{y}_1) < 0$. As discussed in Section III-C, we have $f'(\mathbf{x}_1^*) = 0$ and $\phi_L^{(1)} < \phi_1^* < 1$, where $\phi_L^{(1)} =$

$$\begin{cases} \phi_2^* = \phi_1^* = 1, & \varepsilon(\mathbf{x}_2^*) < \varepsilon(\mathbf{x}_1^*), \ \text{when} \left\|\mathbf{h}_{ba}^{(1)}\right\|^2 < \left\|\mathbf{h}_{ba}^{(2)}\right\|^2 \le \rho_{\text{th}} \\ \phi_L^{(2)} < \phi_2^* < \phi_1^* = 1, & \varepsilon(\mathbf{x}_2^*) < \varepsilon(\mathbf{x}_1^*), \ \text{when} \left\|\mathbf{h}_{ba}^{(1)}\right\|^2 \le \rho_{\text{th}} < \left\|\mathbf{h}_{ba}^{(2)}\right\|^2 \\ \phi_L^{(2)} < \phi_2^* < \phi_1^* < 1, & \varepsilon(\mathbf{x}_2^*) < \varepsilon(\mathbf{x}_1^*), \ \text{when} \left\|\mathbf{h}_{ba}^{(1)}\right\|^2 > \rho_{\text{th}} \end{cases} \tag{52}$$

$$\begin{cases} \phi_1^* = \phi_2^* = 1, & \varepsilon(\mathbf{x}_1^*) < \varepsilon(\mathbf{x}_2^*), \ \text{when } f'(\mathbf{y}_1) \ge 0 \\ \phi_L^{(1)} < \phi_1^* < \phi_2^* = 1, & \varepsilon(\mathbf{x}_1^*) < \varepsilon(\mathbf{x}_2^*), \ \text{when } f'(\mathbf{y}_1) < 0 \le f'(\mathbf{y}_2) \\ \phi_L^{(1)} < \phi_1^* < \phi_2^* < 1, & \varepsilon(\mathbf{x}_1^*) < \varepsilon(\mathbf{x}_2^*), \ \text{when } f'(\mathbf{y}_2) < 0 \end{cases} \tag{63}$$

$(2^{R_{\text{th}}^{(1)}} - 1)/\gamma_B$. In the next, two different situations are considered below.

a) *$f'(\mathbf{y}_2) \ge 0 > f'(\mathbf{y}_1)$:* In this case, we have $\phi_L^{(1)} < \phi_1^* < \phi_2^* = 1$, $f'(\mathbf{x}_2^*) \ge f'(\mathbf{x}_1^*) = 0$. To prove $w(\mathbf{x}_2^*) < w(\mathbf{x}_1^*)$, we assume in contradiction that $w(\mathbf{x}_2^*) \ge w(\mathbf{x}_1^*)$, meaning that

$$\frac{\gamma_B}{2^{R_{\text{th}}^{(2)}}} - w'(\mathbf{x}_2^*) \ge \frac{\gamma_B}{2^{R_{\text{th}}^{(1)}}} - w'(\mathbf{x}_1^*)\phi_1^*. \tag{60}$$

Since $R_{\text{th}}^{(2)} > R_{\text{th}}^{(1)}$, we have that $w'(\mathbf{x}_1^*)\phi_1^* > w'(\mathbf{x}_2^*)$, and hence $w'(\mathbf{x}_1^*) > w'(\mathbf{x}_2^*)$. Besides, since $f'(\mathbf{x}_2^*) \ge f'(\mathbf{x}_1^*) = 0$, it follows by (59) that:

$$\frac{w(\mathbf{x}_1^*)}{1 + \frac{(1-\phi_1^*)w(\mathbf{x}_1^*)}{\alpha_1}} > w(\mathbf{x}_2^*) \implies \phi_1^* > 1 \tag{61}$$

contradicting the fact that $\phi_1^* < 1$. We thus conclude that $w(\mathbf{x}_2^*) < w(\mathbf{x}_1^*)$. Then, by (54) we have $f(\mathbf{x}_1^*) > f(\mathbf{x}_2^*)$. Hence, by (56), $\varepsilon(\mathbf{x}_1^*) < \varepsilon(\mathbf{x}_2^*)$.

b) *$f'(\mathbf{y}_2) < 0$:* In this case, we conclude that $f'(\mathbf{x}_1^*) = f'(\mathbf{x}_2^*) = 0$. To prove $\phi_2^* > \phi_1^*$, we suppose in contradiction that $\phi_2^* \le \phi_1^*$. Then from (57) we have $w(\mathbf{x}_2^*) < w(\mathbf{x}_1^*)$ and $w'(\mathbf{x}_2^*) > w'(\mathbf{x}_1^*)$. Hence, from (59) we have $f'(\mathbf{x}_2^*) > f'(\mathbf{x}_1^*)$, which is a contradiction to $f'(\mathbf{x}_1^*) = f'(\mathbf{x}_2^*) = 0$. Thus, we can conclude that $\phi_2^* > \phi_1^*$. To prove $w(\mathbf{x}_2^*) < w(\mathbf{x}_1^*)$, assume in contradiction that $w(\mathbf{x}_2^*) \ge w(\mathbf{x}_1^*)$. Then, by (57), we have

$$\frac{\gamma_B}{2^{R_{\text{th}}^{(2)}}} - \phi_2^* w'(\mathbf{x}_2^*) \ge \frac{\gamma_B}{2^{R_{\text{th}}^{(1)}}} - \phi_1^* w'(\mathbf{x}_1^*). \tag{62}$$

Since $R_{\text{th}}^{(2)} > R_{\text{th}}^{(1)}$, we have $\phi_1^* w'(\mathbf{x}_1^*) > \phi_2^* w'(\mathbf{x}_2^*)$, and hence $w'(\mathbf{x}_1^*) > w'(\mathbf{x}_2^*)$. Then, from (59), we obtain that $f'(\mathbf{x}_1^*) > f'(\mathbf{x}_2^*)$, which is a contradiction to $f'(\mathbf{x}_1^*) = f'(\mathbf{x}_2^*) = 0$. Thus, we can conclude that $w(\mathbf{x}_2^*) < w(\mathbf{x}_1^*)$. Then by (54) we conclude that $f(\mathbf{x}_2^*) < f(\mathbf{x}_1^*)$, and thus by (56), $\varepsilon(\mathbf{x}_2^*) > \varepsilon(\mathbf{x}_1^*)$.

Hence, if $R_{\text{th}}^{(1)} < R_{\text{th}}^{(2)}$, then we have $\phi_1^* \le \phi_2^*$ and $\varepsilon(\mathbf{x}_1^*) < \varepsilon(\mathbf{x}_2^*)$. This result can be expressed in (63), as shown at the top of this page. ■

REFERENCES

[1] J. A. Stankovic, "Research directions for the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 3–9, Feb. 2014.

[2] S. Verma, Y. Kawamoto, Z. Fadlullah, H. Nishiyama, and N. Kato, "A survey on network methodologies for real-time analytics of massive IoT data and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1457–1477, 3rd Quart., 2017.

[3] P. Yang *et al.*, "Identifying the most valuable workers in fog-assisted spatial crowdsourcing," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1193–1203, Oct. 2017.

[4] Y. Kawamoto *et al.*, "A feedback control-based crowd dynamics management in IoT system," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1466–1476, Oct. 2017.

[5] K. Zhang *et al.*, "Security and privacy in smart city applications: Challenges and solutions," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 122–129, Jan. 2017.

[6] B. Schneier, "Cryptographic design vulnerabilities," *Computer*, vol. 31, no. 9, pp. 29–33, Sep. 1998.

[7] N. Yang *et al.*, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[8] H. Wen, *Physical Layer Approaches for Securing Wireless Communication Systems*. New York, NY, USA: Springer-Verlag, 2013.

[9] D. Chen *et al.*, "S2M: A lightweight acoustic fingerprints-based wireless device authentication protocol," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 88–100, Feb. 2017.

[10] 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.

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

[12] S. K. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[13] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[14] 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.

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

[16] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1728–1740, Sep. 2013.

[17] H.-M. Wang, T.-X. Zheng, and X.-G. Xia, "Secure MISO wiretap channels with multiantenna passive eavesdropper: Artificial noise vs. artificial fast fading," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 94–106, Jan. 2015.

[18] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170–2181, Jun. 2013.

[19] N. Yang *et al.*, "Artificial noise: Transmission optimization in multi-input single-output wiretap channels," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1771–1783, May 2015.

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

[21] J. Xiong, K.-K. Wong, D. Ma, and J. Wei, "A closed-form power allocation for minimizing secrecy outage probability for MISO wiretap channels via masked beamforming," *IEEE Commun. Lett.*, vol. 16, no. 9, pp. 1496–1499, Sep. 2012.

[22] T.-X. Zheng, H.-M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4347–4362, Nov. 2015.

[23] T.-X. Zheng and H.-M. Wang, "Optimal power allocation for artificial noise under imperfect CSI against spatially random eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8812–8817, Oct. 2016.
[24] L. Hu, H. Wen, B. Wu, J. Tang, and F. Pan, "Adaptive secure transmission for physical layer security in cooperative wireless networks," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 524–527, Mar. 2017.
[25] L. J. Rodriguez *et al.*, "Physical layer security in wireless cooperative relay networks: State of the art and beyond," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 32–39, Dec. 2015.
[26] M. Heitzler and J. C. Lam, "JGPU-accelerated rendering methods to visually analyze large-scale disaster simulation data," *J. Geovisualization Spatial Anal.*, vol. 1, no. 3, pp. 1–18, 2017.
[27] A. Behnad, M. B. Shahbaz, T. J. Willink, and X. Wang, "Statistical analysis and minimization of security vulnerability region in amplify-and-forward cooperative systems," *IEEE Trans. Wireless Commun.*, vol. 16, no. 4, pp. 2534–2547, Apr. 2017.
[28] T.-X. Zheng, H.-M. Wang, F. Liu, and M. H. Lee, "Outage constrained secrecy throughput maximization for DF relay networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1741–1755, May 2015.
[29] Q. Xu, P. Ren, H. Song, and Q. Du, "Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations," *IEEE Access*, vol. 4, pp. 2840–2853, 2016.
[30] X. Hu, P. Mu, B. Wang, and Z. Li, "On the secrecy rate maximization with uncoordinated cooperative jamming by single-antenna helpers," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 4457–4462, May 2017.
[31] P. Mu, X. Hu, B. Wang, and Z. Li, "Secrecy rate maximization with uncoordinated cooperative jamming by single-antenna helpers under secrecy outage probability constraint," *IEEE Commun. Lett.*, vol. 19, no. 12, pp. 2174–2177, Dec. 2015.
[32] L. Hu, B. Wu, J. Tang, F. Pan, and H. Wen, "Outage constrained secrecy rate maximization using artificial-noise aided beamforming and cooperative jamming," in *Proc. IEEE ICC*, Kuala Lumpur, Malaysia, May 2016, pp. 1–5.
[33] H.-M. Wang, F. Liu, and M. Yang, "Joint cooperative beamforming, jamming, and power allocation to secure AF relay systems," *IEEE Trans. Veh. Technol.*, vol. 64, no. 10, pp. 4893–4898, Oct. 2015.
[34] Y. Zhang, Y. Shen, H. Wang, J. Yong, and X. Jiang, "On secure wireless communications for IoT under eavesdropper collusion," *IEEE Trans. Autom. Sci. Eng.*, vol. 13, no. 3, pp. 1281–1293, Jul. 2016.
[35] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[36] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 8th ed. New York, NY, USA: Academic, 2015.
[37] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, "Compound wiretap channels," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, pp. 1–12, Mar. 2009.
[38] R. B. Ash, *Basic Probability Theory*. Mineola, NY, USA: Dover, 2012.

Lin Hu is currently pursuing the Ph.D. degree at the National Key Laboratory of Communications, University of Electronic Science and Technology of China, Chengdu, China.

His current research interests include physical layer security of wireless communications, convex optimization for signal processing, and cooperative communication systems.

Hong Wen (M'06–SM'17) was born in Chengdu, China. She received the M.Sc. degree in electrical engineering from the Sichuan Union University of Sichuan, Chengdu, in 1997, and the Ph.D. degree from the Department of Communication and Computer Engineering, Southwest Jiaotong University, Chengdu.

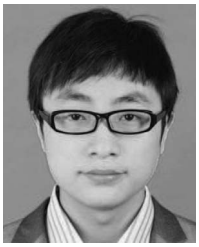
From 2008 to 2009, she was a Visiting Scholar and a Post-Doctoral Fellow with the Electrical and Computer Engineering Department, University of Waterloo, Waterloo, ON, Canada. She is currently a Professor with UESTC. Her current research interest includes wireless communication systems and security.

Bin Wu (S'04–M'07) received the Ph.D. degree in electrical and electronic engineering from the University of Hong Kong, Hong Kong, in 2007.

He was a Post-Doctoral Research Fellow with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada, from 2007 to 2012. He is currently a Professor with the School of Computer Science and Technology, Tianjin University, Tianjin, China. His current research interests include computer systems and networking, IP, optical and wireless communications and networking, and network survivability and security issues.

Fei Pan was born in Yaan, China. She received the bachelor's degree from Northwest University, Xi'an, China, in 2011. She is currently pursuing the Ph.D. degree in communication and information system at the National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu, China.

Her current research interest includes wireless communication systems security.



Run-Fa Liao was born in Chongqing, China. He is currently pursuing the Ph.D. degree in communication and information system at the National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China, Chengdu, China.

His current research interest includes wireless communication system security combined with intelligent algorithms.

Huanhuan Song was born in Zaozhuang, China. She is currently pursuing the Ph.D. degree in communication and information system at the National Key Laboratory of Science and Technology on Communications, Chengdu, China.

Her current research interests include wireless communication system and intelligent optimization algorithms.

Jie Tang was born in Chengdu, China. He is currently pursuing the Ph.D. degree in communication and information system at the National Key Laboratory of Science and Technology on Communications, Chengdu.

His current research interests include wireless communication system and information security.

Xiumin Wang received the B.S. degree in communication and electronic system from the Dalian University of Technology, Dalian, China.

She is currently a Professor and an Associate Dean of the College of Information Engineering, China Jiliang University, Hangzhou, China. Her current research interests include signal and information processing.