Cooperative secure transmission against collusive eavesdroppers in Internet of Things

Xin Fan and Yan Huo

Abstract
As Internet of Things (IoT) has boomed in recent years, many security issues have also been exposed. Focusing on physical layer security in wireless Internet of Things network communication, a series of security methods have been widely studied. Nevertheless, cooperative jamming methods in physical layer security to fight against collusive eavesdroppers have not been thoroughly studied yet. In this article, we study a cooperative-jamming-based physical layer secure transmission scheme for Internet of Things wireless networks in the presence of collusive eavesdroppers. We design a cooperative jamming strategy without knowing the channel state information of eavesdroppers. Considering the cooperation of multiple nodes with multiple antennas, this strategy can maximize the signal-to-interference-plus-noise ratio at an actuator (legitimate receiver). Meanwhile, the generated cooperative jamming signals can reduce the signal-to-interference-plus-noise ratio at eavesdroppers. To explore the theoretical security performance of our strategy, we perform a secrecy outage probability analysis and an asymptotic analysis. In the cases of cooperative jamming and without cooperative jamming, the closed-form expressions of the secrecy outage probability are deduced, and the influence of system parameters on the secrecy outage probability becomes more intuitive through a strict mathematical asymptotic behavior analysis. In addition, considering the energy limitation of Internet of Things devices, we propose a power allocation algorithm to minimize the total transmission power given the security requirements. The numerical results show the effectiveness of our schemes and are consistent with the theoretical analysis.

Keywords
Internet of Things, collusive eavesdroppers, cooperative jamming, asymptote, secrecy outage probability, power allocation algorithm

Date received: 1 April 2020; accepted: 18 May 2020

Handling Editor: Yan Huang

Introduction
With the development of Internet of Things (IoT), the traditional industrial models have been gradually changed, triggering a new wave of industrial, economic, and social development. As a new form of Internet-based information technology, in addition to all the same types of cyber-attack threats as in the other wireless networks, the IoT field also faces more and more complex threats due to its multi-source heterogeneity, openness, ubiquity, and other characteristics. The issue of IoT security has also become one of the keys to development.
Traditionally, solutions to the security of information transmission are provided through cryptographic protocols implemented at the upper layers. Yet, due to the characteristics of IoT, modern cryptographic methods alone may become insufficient for achieving the desired communication security in many practical scenarios. For example, low-end IoT devices are inconvenient to adopt highly complex cryptographic measures due to their limited energy and computational power. Although there are some lightweight encryption methods, the highly heterogeneous IoT systems without unified cryptographic protocols also make the management and distribution of keys very difficult. As a result, it is imperative to explore complementary or alternative information security measures for IoT applications. Unlike cryptographic-technique-based security, physical layer security uses inherent properties of the channel uniqueness and reciprocity of physical channels that can achieve information-theoretic security regardless of eavesdroppers’ computational power. Physical layer security can provide an additional layer of protection without compromising the existing cryptographic-technique-based security protection, which has aroused extensive attention.

In the related research of physical layer security, the cooperative jamming (CJ) is the mainstream technology, the core idea of which is to send artificial noise (AN) to confuse eavesdroppers. CJ-based methods have been used in various scenarios, for example, cognitive radio networks (CRNs) and heterogeneous networks. Li et al. proposed a CJ scheme where secondary users (SUs) are selected as helpers to generate jamming signals to block eavesdroppers. Using the coalition formation game, they design an effective cooperation strategy to maximize secrecy capacity. Introducing the non-orthogonal multiple access (NOMA) technology into CRNs, Wei et al. analyzed the security performance of SUs and derived a closed-form expression of the secrecy sum rate (SSR) of all SUs. Huo et al. designed three different CJ schemes for different user requirements, with the cooperation of macro- and microcells. In scenarios where eavesdroppers’ channel state information (CSI) cannot be obtained, in some previous studies different physical layer security transmission schemes were designed, via secrecy encoding together with artificial-noise-aided signaling, pace power synthesis, and power allocation, respectively.

Naturally, this idea of CJ can be introduced into IoT networks to achieve secure transmission at the physical layer. Introducing the idea of cognitive radio into IoT to build a Consumer Internet of Things (CloT) network, Li et al. proposed a CJ scheme, in which a selected SU can harvest energy from a primary user (PU) and then use the harvested energy to send AN. Assuming that there is an error in the channel estimation, they optimized the worst-case secrecy rate in the presence of a single eavesdropper. Expanding the number of eavesdroppers from one to multiple, Hu et al. derived the secrecy outage probability (SOP) assuming only the statistical channel state information of eavesdroppers (ECI) can be obtained. Then they proposed a power allocation scheme to minimize the SOP. Zhang et al. studied the role of relays in IoT and analyzed the security performance of a two-hop network. In their network, the nodes can be relays and jammers in two different phases.

No matter how extensive is the research on CJ, no one has studied the secrecy performance of CJ in the following scenarios: (1) all nodes are multi-antenna; (2) multiple eavesdroppers can cooperate to improve their eavesdropping ability; and (3) ECSI cannot be obtained. In fact, with the development of millimeter-wave and large-scale antenna array technologies, the evolution trend of IoT devices from single antenna to multiple antennas is irresistible. With millions of devices, IoT networks can expose users to multiple eavesdroppers whose CSI may not be available due to their passive mode. Therefore, it is of great practical significance to study the CJ technology in multi-antenna scenarios with collusive eavesdroppers, which can promote the development of physical layer technology in the IoT field.

Motivated by the above issues, we designed a CJ scheme to fight collusive eavesdroppers without knowing ECSI in multi-antenna IoT networks. Specifically, we assume that all the considered nodes in our network are equipped with multiple antennas. Moreover, only perfect CSI for legitimate receivers can be obtained, while the ECSI of collusive eavesdroppers cannot. With the help of a friendly CJ node, the physical layer security transmission from a controller to an actuator is studied in this article. To the best of our knowledge, we are the first to study a CJ scheme in this more practical scenario. Our contributions can be summarized as follows:

- We propose a CJ scheme that needs the cooperation of a controller (transmitter), an actuator (receiver), and a friendly jammer. Through joint optimization, the proposed CJ scheme can maximize the received signal-to-interference-plus-noise ratio (SINR) of the actuator while maintaining the jamming to the collusive eavesdroppers despite unknown ECSI.
- We demonstrate the theoretical performance analysis of our proposed scheme through SOP analysis and asymptotic analysis. In the SOP analysis, based on computational mathematics, we derive two different closed-form expressions of the SOP: in the presence of cooperative nodes and in the absence of cooperative nodes. In the
derivation process, we solve the problem of multiple integrals. In the asymptotic analysis, based on rigorous mathematics, we explore the impact of different system parameters on SOP.

- In view of the fact that IoT devices are generally energy constrained, we propose a power allocation scheme to minimize the sum of transmission power while meeting the basic security requirements. We solve the power optimization problem which is non-convex and difficult to deal with.

The rest of our article is organized as follows. We provide our system model and formulate it in section “The system model.” In section “Secrecy analysis,” we present the theoretical performance analysis of our proposed secure transmission scheme through SOP and asymptotic analyses. Furthermore, we propose a power allocation problem and give the corresponding solution algorithm in section “The power allocation problem.” Finally, the numerical results of our schemes are provided in section “Numerical results” and our work is concluded in section “Conclusion.”

The notations used in this article are as follows. Bold upper and lower case letters denote matrices and vectors, respectively. $(\cdot)^H$, $\text{Tr}(\cdot)$, and $\|\cdot\|$ represent Hermitian transpose, trace, and Euclidean norm of a matrix, respectively; $\mathcal{CN}(\mu, \sigma^2)$ denotes a complex Gaussian variable with mean $\mu$ and variance $\sigma^2$; $X \in \mathbb{C}^{i \times j}$ means that $X$ is a complex matrix with $i$ rows and $j$ columns; $\mathbb{E}(\cdot)$ denotes the expectation operation.

The system model

In this article, we consider the transmission of private information from a controller (Alice) to an actuator (Bob) in an IoT network, as shown in Figure 1. One or more passive eavesdroppers (Eves) may coexist on the network trying to eavesdrop on the private information. To prevent eavesdropping, Alice or Bob needs to select one of the surrounding neighbor nodes as a CJ source (called as Jammer). The selected Jammer broadcasts AN to confuse the eavesdroppers when Alice sends the private information to Bob. Note that the selection of Jammer is beyond the scope of this article.

Alice, Bob, and Jammer are assumed to have $N_a$, $N_b$, and $N_e$ antennas, respectively. As claimed in previous studies,29–31 eavesdroppers can aggregate the information received by their antennas to improve eavesdropping capabilities, so they can be considered as a super eavesdropper (S-Eve) with $N_e$ antennas (Generally speaking, the synchronization between IoT devices is difficult to achieve. Therefore, a super eavesdropper is a worst-case assumption in this article). Here, $N_e$ represents the sum of the antennas of all eavesdroppers. All the considered wireless channels are assumed to be subject to independent Rayleigh slow-flat fading in our network. Specifically, $\mathbf{H}_{ab} \in \mathbb{C}^{N_a \times N_b}$ and $\mathbf{H}_{ae} \in \mathbb{C}^{N_a \times N_e}$ denote the channel matrices from Alice to Bob and Eve, respectively. Similarly, $\mathbf{H}_{jb} \in \mathbb{C}^{N_b \times N_j}$ and $\mathbf{H}_{je} \in \mathbb{C}^{N_b \times N_e}$ denote the channel matrices from Jammer to Bob and Eve, respectively. It is worth noting that we just assume that the CSI of legal channels (i.e. the channels from Alice and Jammer to Bob) can be obtained perfectly, while ECSI cannot be obtained (In general, if the eavesdropper is in the passive eavesdropping mode, it is difficult to obtain their CSI. Thus, this article considers this more practical scenario where ECSI is not available. Note that ECSI is not needed for the design of our CJ scheme, but statistical ECSI can help us analyze the security performance of our scheme). For performance analysis, without loss of generality, we assume that the elements in the matrices $\mathbf{H}_{ae}$ and $\mathbf{H}_{je}$ obey the independent circularly symmetric complex Gaussian (CSCG) distribution with zero mean and a variance of 1. For convenience, a list of notations is provided in Table 1.

Received signals at Bob and S-Eve

Assuming that Alice transmits private information to Bob while Jammer broadcasts AN, the received signals at Bob and S-Eve can be formulated as

$$y_b = \sqrt{P_a}\mathbf{H}_{ab}\mathbf{w}\mathbf{s}_a + \sqrt{P_j}\mathbf{H}_{jb}\mathbf{z}\mathbf{s}_z + \mathbf{n}_b$$  \hspace{1cm} (1)

$$y_e = \sqrt{P_a}\mathbf{H}_{ae}\mathbf{w}\mathbf{s}_a + \sqrt{P_j}\mathbf{H}_{je}\mathbf{z}\mathbf{s}_z + \mathbf{n}_e$$  \hspace{1cm} (2)

where $\mathbf{w} \in \mathbb{C}^{N_a \times 1}$ ($\|\mathbf{w}\|^2 = 1$) and $\mathbf{s}_a$ ($\mathbb{E}(|\mathbf{s}_a|^2) = 1$) are the precoding vector and the signal transmitted by Alice, respectively; $\mathbf{z} \in \mathbb{C}^{N_b \times 1}$ ($\|\mathbf{z}\|^2 = 1$) and $\mathbf{s}_z$ ($\mathbb{E}(|\mathbf{s}_z|^2) = 1$) are the AN vector and the signal transmitted by Jammer, respectively; and $P_a$ and $P_j$ are the

---

**Figure 1.** A physical-layer-secure transmission model for IoT.
transmission power of Alice and Jammer, respectively. Note that since the ECSI cannot be obtained, $P_j$ is evenly allocated to $N_j$ elements of $z$. In addition, $n_u \sim \mathcal{CN}(0, I_{N_u})$ and $n_e \sim \mathcal{CN}(0, I_{N_e})$ represent the corresponding additive complex white Gaussian noise (AWGN) at Bob and S-Eve, respectively.

### SINR

For enhancing the ability to decode the information, Bob and S-Eve can take different strategies to maximize their SINRs. Bob can work with Alice and Jammer, while S-Eve can use a more effective diversity receiving method. Next, we will describe their strategies.

**Bob’s SINR maximization.** Equipped with the multiple antennas, Bob can use the decoding vector $d_b \in \mathbb{C}^{1 \times N_b}$ to decode the received multiple signals, thereby improving its SINR. After decoding, the received signal and SINR at Bob can be expressed as follows

$$r_b = d_b y_b = \sqrt{P_a} d_b H_{ab} w s_a + \sqrt{P_j} d_b H_{jb} z_s + d_b n_b$$  
$$SINR_b = \frac{P_a |d_b H_{ab} w|^2}{P_j |d_b H_{jb} z_s|^2 + 1}$$

To maximize the received SINR of Bob, it is necessary to jointly optimize the precoding vector $w$, the decoding vector $d_b$, and the AN vector $d_b$. This joint optimization problem can be formulated by $\textbf{P1}$ as follows

$$\textbf{P1} : \{d_b, w, z\} = \arg \max_{d_b, w, z} \frac{P_a |d_b H_{ab} w|^2}{P_j |d_b H_{jb} z_s|^2 + 1}$$

Using singular value decomposition (SVD) and zero forcing beamforming (ZFBF), we can obtain the optimal solutions of the above problem, which can be given by Lemma 1.

**Lemma 1.** When $H_{ab}$ can be decomposed as $H_{ab} = USV^H$ by SVD, the optimal solution $\{d_b, w, z\}$ to Lemma 1 is obtained as follows

$$d_b = \text{the first row of } U^H$$
$$w = \text{the first column of } V$$
$$z = \left(I_{N_e} - \frac{H_{jb}^H d_b H_{jb}}{||d_b H_{jb}||^2} \right) a$$

where $a \in \mathbb{C}^{N_b \times 1}$ and $a \sim \mathcal{CN}(0, I_{N_y})$.

For the proof of Lemma 1, see Appendix 1.

As a result, we can derive the SINR at Bob as

$$SINR_b = \frac{P_a \lambda_{\text{max}}}{P_j}$$

where $\lambda_{\text{max}}$ denotes the largest singular value of $H_{ab}$ (Only taking the signal with the largest singular value will inevitably cause performance loss. The largest singular value signal is chosen because the AN that Jammer sends is orthogonal to the largest singular value signal. This means that all other signals will be affected by AN. From this point of view, even with the addition of other signals, the performance is not greatly improved due to AN).

**S-Eve’s SINR maximization.** In the worst case where eavesdroppers can conspire perfectly, the maximum ratio combining (MRC) is their optimal diversity receiving method to enhance their SINR. According to Sklar,32 we can give the MRC weight as follows

$$\sigma = (H_{ae} w)^H H_{ae}^{H}$$

After MRC, the output signals at S-Eve can be rewritten as

$$r_e = \sigma y_e = \sqrt{P_a} \sigma H_{ae} w s_a + \sqrt{P_j} \sigma H_{je} z_e + \sigma n_e$$

Therefore, the SINR at S-Eve can be further derived as

$$SINR_e = \frac{P_a |\sigma H_{ae} w|^2}{P_j |\sigma H_{je} z_e|^2 + |\sigma|^2}$$

$$SINR_e = \frac{P_a |\sigma|^2}{P_j |\psi|^2 + 1}$$

$$SINR_e = \frac{X}{Y + 1}$$

where $X = P_a |\sigma|^2$, $Y = P_j |\psi|^2$, and $\psi = \sigma H_{je} z_e / |\sigma|$. After the analysis, we can easily get $X \sim \Gamma(\alpha, \theta)$ and $Y \sim \exp(\theta_1)$, where $\alpha = \frac{N_e}{\gamma}$, $\theta = 1/P_a$, and $\theta_1 = 1/P_j$. 

### Table 1. List of the main notations.

| Notation | Definition |
|----------|------------|
| $N_a$    | Number of the antennas of Alice |
| $N_b$    | Number of the antennas of Bob |
| $N_j$    | Number of the antennas of Jammer |
| $N_e$    | Number of the antennas of all Eves |
| $N_l$    | Number of the antennas of all Eves |
| $H_{ab}$ | Channel between Alice and Bob |
| $H_{ae}$ | Channel between Alice and S-Eve |
| $H_{jb}$ | Channel between Jammer and Bob |
| $H_{je}$ | Channel between Jammer and S-Eve |
| $P_a$    | Transmission power of Alice |
| $P_j$    | Transmission power of Jammer |
| $\eta$   | SOP with CJ |
| $\eta_j$ | SOP without CJ |

SOP: secrecy outage probability; CJ: cooperative jamming.
Secrecy analysis

In this section, we explore the safety performance of our proposed CJ scheme in terms of the SOP and asymptotic analyses. With or without a cooperative jammer, we derive the closed-form expressions of the SOP. Moreover, the asymptotic behavior of SOP is given by strict mathematical derivation.

SOP

Before signal transmission, assuming that the private information is encoded by Wyner’s33 wiretap code, we can get the achievable secrecy rate of the transmission link between Alice and Bob as follows

\[ R_s = \max\{R_b - R_e, 0\} \]

where

\[ R_b = \log(1 + \text{SINR}_b) \quad \text{and} \quad R_e = \log(1 + \text{SINR}_e) \]

are the achievable rates for Bob and S-Eve, respectively. Note that the rate \( R_e \) is treated as a random variable that varies with \( \text{SINR}_e \), due to the fact that only the statistical CSI of S-Eve is available.

According to Wyner,33 if \( R_b > R_e \), such as \( R_b > R_{th} \) where \( R_{th} > 0 \) is the minimum secrecy rate requirement, secure transmission can be guaranteed. Otherwise, secure transmission is interrupted, that is, secrecy outage. Based on Barros and Rodrigues,34 the probability of secrecy outage (i.e., SOP) can be used for evaluating the security of an information transmission, which can be expressed as follows

\[ \eta = \Pr\{R_s < R_b\} = \Pr\{R_b - R_e < R_{th}\} \]
\[ = \Pr\{R_b > R_e - R_{th}\} \]
\[ = \Pr\{\text{SINR}_e > 2^{R_{th} - R_b} - 1\} \]

(16)

where \( F_{\text{SINR}_e}(x) \) represents the complementary cumulative distribution function (CCDF) of \( \text{SINR}_e \).

To derive the closed-form expression of SOP in equation (16), Proposition 1 is needed to be given first.

Proposition 1. The CCDF of \( \text{SINR}_e \) can be characterized in the following closed form

\[ F_{\text{SINR}_e}(\tau) = \frac{1}{P_j} \exp\left(-\frac{\tau}{P_j}\right) \sum_{k=0}^{N_e-1} \frac{1}{\binom{N_e}{k}} \left(\frac{\tau}{P_a}\right)^k \]
\[ \times \sum_{i=0}^{k} C^i_k \left( \frac{\tau}{P_a} + \frac{1}{P_j} \right)^{i-1} \Gamma(i+1) \]

(17)

where \( \tau > 0 \) and \( C^i_k = k! / i!(k-i)! \).

For the proof of Proposition 1, see Appendix 1.

According to equations (9) and (15), for a given value of \( R_{th} \), we can further calculate the maximum acceptable \( \text{SINR} \) of S-Eve as \( \mu = 2^{R_{th} - R_b} - 1 \). Therefore, the closed-form expression of SOP can be derived as

\[ \eta(\mu) = F_{\text{SINR}_e}(\mu). \]

(18)

If we cannot find any node to be a Jammer, that is, \( P_j = 0 \), the closed-form expression of SOP can be given by Proposition 2.

Proposition 2. Without Jammer, the closed-form expression of SOP can be characterized as

\[ \eta^{NJ}(\mu) = \exp\left(-\frac{\tau}{P_a}\right) \sum_{k=0}^{N_e-1} \frac{1}{\binom{N_e}{k}} \left(\frac{\tau}{P_a}\right)^k \]

(19)

Proof. When \( P_j = 0 \), that is, \( Y = 0 \), the CCDF of \( \text{SINR}_e \) can be simplified as

\[ F_{\text{SINR}_e}(\tau) = \Pr(\text{SINR}_e > \tau) \]
\[ = \Pr(X > \tau) = \int_{\tau}^{\infty} f_X(x)dx. \]

(20)

Similar to the proof of Proposition 1, the CCDF of \( \text{SINR}_e \) without Jammer can be calculated in the following closed form

\[ F_{\text{SINR}_e}(\tau) = \exp\left(-\frac{\tau}{P_a}\right) \sum_{k=0}^{N_e-1} \frac{1}{\binom{N_e}{k}} \left(\frac{\tau}{P_a}\right)^k. \]

(21)

Accordingly, for a given \( \mu > 0 \), we can finally obtain the closed-form expression of the SOP without Jammer as follows

\[ \eta^{NJ}(\mu) = F_{\text{SINR}_e}^{NJ}(\mu). \]

(22)

Hence, we have completed the proof of Proposition 2.

Asymptotic analysis

To better design a CJ scheme, it is meaningful to explore the influence of system parameters on \( \eta(\mu) \) and \( \eta^{NJ}(\mu) \), such as \( P_a \), \( P_j \), and \( N_e \). However, we cannot directly characterize the relationship between these system parameters and the SOP because of their complex coupling in equations (18) and (19). Therefore, we perform the asymptotic behavior analysis with strict mathematical derivation, which can be collated into the following three properties.

Property 1. When \( \mu > 0 \), \( \eta(N_e) \) and \( \eta^{NJ}(N_e) \) both increase monotonously with \( N_e \) and finally converge to 1. We
can obtain the asymptotic expressions of $\eta(N_e)$ and $\eta^{NJ}(N_e)$ with the infinite value of $N_e$ as

$$\eta(N_e) \xrightarrow{N_e \to \infty} 1$$  \hspace{1cm} (23)

$$\eta^{NJ}(N_e) \xrightarrow{N_e \to \infty} 1$$  \hspace{1cm} (24)

**Property 2.** When $\mu > 0$, $\eta(P_a)$ and $\eta^{NJ}(P_a)$ converge to different constant values as $P_a \to \infty$. We can obtain the asymptotic expressions of $\eta(P_a)$ and $\eta^{NJ}(P_a)$ with the infinite value of $P_a$ as

$$\eta(P_a) \xrightarrow{P_a \to \infty} \sum_{k=0}^{N_e-1} \frac{k!}{k!} s^k \text{ for } P_a \geq P_{a_{max}}$$  \hspace{1cm} (25)

$$\eta^{NJ}(P_a) \xrightarrow{P_a \to \infty} \exp(-s) \sum_{k=0}^{N_e-1} \frac{1}{k!} s^k$$  \hspace{1cm} (26)

where $s = \lambda_{max}/2^{\frac{h_a}{N_e}}$ and $\tilde{s} = \frac{s}{(s + (1/P_j))}$.

**Property 3.** When $\mu > 0$, we can obtain the asymptotic expressions of $\eta(P_j)$ with the infinite value of $P_j$ as

$$\eta(P_j) \xrightarrow{P_j \to \infty} 0$$  \hspace{1cm} (27)

For the proof of the three properties, refer to Appendix 1.

**Remark 1.** Property 1 demonstrates that, in the case of a sufficient number of S-Eve’s antennas, secure transmission is impossible despite the assistance of Jammer.

**Remark 2.** Property 2 implies that the continued increase in Alice’s transmission power is not always conducive to improved security.

**Remark 3.** Property 3 theoretically confirms that, if Jammer’s transmission power is sufficient, secure transmission can always be guaranteed.

**The power allocation problem**

Since IoT devices are generally energy constrained, the optimization of the power allocation problem in the design of IoT wireless networks is important, involving greenness and sustainability. Generally, the following two power optimization problems should be considered: (1) how to minimize the SOP given the limited global transmission power and (2) how to minimize the sum of the transmission power given the security requirements. In contrast, the latter optimization problem has more practical significance in real-time application scenarios, which is therefore mainly focused in this article. The purpose of this optimization problem is to save energy as much as possible while meeting the security requirements. In this section, we formulate this optimization problem and give the corresponding solution algorithm.

**Formulation of power allocation**

When considering the optimization of the transmission power of Alice and Jammer, not only must the security requirements be met, but Bob’s reliable communication requirement should also be met. In addition, each node has an upper limit of its transmission power. Thus, considering both the upper limit of the transmission power and the minimum quality of service (QoS) requirement of Bob, the power optimization problem P3 can be formulated as follows

$$\textbf{P3 : } \min_{P_a, P_j} P_a + P_j$$  \hspace{1cm} (28a)

$$\text{s.t. } \eta(P_a, P_j) \leq \eta_{th}$$  \hspace{1cm} (28b)

$$\text{SINR}_b \geq \gamma_{th}$$  \hspace{1cm} (28c)

$$P_a \leq P_{a_{max}}$$  \hspace{1cm} (28d)

$$P_j \leq P_{j_{max}}$$  \hspace{1cm} (28e)

$$P_j > 0$$  \hspace{1cm} (28f)

where $P_{a_{max}}$ and $P_{j_{max}}$ are the maximum power limit values of Alice and Jammer, and $\eta_{th}$ and $\gamma_{th}$ are Bob’s maximum acceptable SOP and minimum acceptable SINR requirement, respectively.

**Optimization of power allocation**

From the closed-form expression of SOP which leads to non-convexity, we can see that it is very difficult to directly solve this optimization problem. To deal with this problem, we use a relaxation method and Taylor expansion formula to convert it into a convex problem. Finally, an iterative algorithm is designed to get the solution of the original problem.

First, after some operations of transposition and equivalent substitution, we rewrite the constraints (equation (28b)) in the following form

$$G(P_a, P_j) \leq 0$$  \hspace{1cm} (29)

where

$$G(P_a, P_j) = G1(P_a, P_j) - G2(P_a, P_j)$$  \hspace{1cm} (30)

$$G1(P_a, P_j) = \sum_{k=0}^{N_e-1} \sum_{i=0}^{k} \frac{s_i^{k-i}}{(k-i)!} s^k$$  \hspace{1cm} (31)
\[ G_2(P_a, P_j) = \eta_{th} e^{\mu} (P_j + 1) \] (32)

According to the convex optimization theory, only when \( G(P_a, P_j) \) is a convex function, the power optimization problem P3 is convex and solvable. Unfortunately, although \( G_1(P_a, P_j) \) and \( G_2(P_a, P_j) \) are convex functions, \( G(P_a, P_j) \) is not. Using the convex optimization transformation idea of Smola et al.,\(^{35}\) we can replace \( G_2(P_a, P_j) \) with its first-order Taylor expansion, so that \( G(P_a, P_j) \) is a convex function and then the original problem P3 can be transformed into a convex optimization problem. Specifically, the first-order Taylor expansion of \( G_2(P_a, P_j) \) at a certain point \( P_a = \bar{P}_a \) can be given by

\[
T(P_a, P_j, \bar{P}_a) = G_2(\bar{P}_a, P_j) + G_2(\bar{P}_a, P_j)(P_a - \bar{P}_a)
= \eta_{th} e^{\mu} \left( \frac{P_j}{P_a} + 1 \right)
- \eta_{th} e^{\mu} \left( P_j e^{\mu} + P_j \frac{\mu}{P_a} + 1 \right)(P_a - \bar{P}_a)
= \eta_{th} e^{\mu} \left( \frac{P_j}{P_a} + 1 \right)
- \eta_{th} e^{\mu} \left( P_j e^{\mu} + P_j \frac{\mu}{P_a} + 1 \right)(P_a - \bar{P}_a)
\] (33)

Since the above formula is a linear function, after replacement, the constraint (equation (28b)) can be turned into a convex function (it is well known that convex functions minus linear functions are still convex functions). It is worth noting that \( G_2(P_j) \) itself is a linear function, so Taylor expansion is not performed on \( P_j \).

Eventually, the power optimization problem can be transformed into the convex optimization problem P4

\[
P_4: \min_{P_a, P_j} P_a + P_j \quad \text{s.t.} \quad G_1(P_a, P_j) - T(P_a, P_j, \bar{P}_a) \leq 0 \quad \text{(34b)}
\]

\[
P_a \geq \frac{\gamma_{th}}{\lambda_n \max} \quad \text{(34c)}
\]

\[
P_a \leq P_{max} \quad \text{(34d)}
\]

\[
P_j \leq P_{max} \quad \text{(34e)}
\]

\[
P_j > 0 \quad \text{(34f)}
\]

Generally speaking, a convex optimization problem can be solved efficiently by common solvers such as CVX.\(^{36}\) However, in order to obtain the solution of the original optimization problem P3, multiple iterations are needed. Therefore, the whole power allocation optimization algorithm that we proposed can be summarized using Algorithm 1.

**Algorithm 1**  A Power allocation optimization algorithm

**Initialization:**
- \( \delta \): a convergence threshold;
- \( k \): the number of iterations

1. Transform the original problem P3 into a convex optimization problem P4;
2. Set \( k = 0 \);
3. Initialize \( P_a^{(k)} = P_{max} / 2, \ P_j^{(k)} = P_{max} / 2 \);
4. Set \( P_a^{(k)} \) to any positive values;
5. While \( |P_a^{(k)} - P_a^{(k-1)}| \leq \delta \) do
6. Set \( k = k + 1 \);
7. Solve problem P4 with \( P_a^{(k)} \) to find an optimal solution for \( \{P_a^{(k)}, P_j^{(k)}, \bar{P}_a^{(k)}\} \);
8. \( P_a^{(k)} = P_a^{(k)} \);
9. end while
10. return \( \{P_a^{(k)}, P_j^{(k)}, \bar{P}_a^{(k)}\} = \{P_a^{(k)}, P_j^{(k)}, \bar{P}_a^{(k)}\} \).

**Remark 4.** Algorithm 1 should be executed at the controller Alice due to its stronger computational power. To execute Algorithm 1, Alice needs to know the CSI between all the legitimate nodes. Alice can easily obtain the CSI between it and Bob by channel estimation, but it cannot obtain the CSI between Bob and the cooperative jammer. Therefore, Jammer or Bob needs to send the CSI to Alice before the execution of Algorithm 1.

**Remark 5.** Algorithm 1 is an algorithm based on the ideas of approximation and iteration. According to Yuille and Rangarajan,\(^ {37} \) after multiple iterations to solve an approximate optimization problem, the algorithm is proven to converge to the optimal solution of the original problem.

**Numerical results**

In this section, we provide the numerical results to verify the performance of our proposed schemes. Here, the power of AWGN is set to 1 mw (i.e. 0 dBm). Unless otherwise stated, other parameters are set as \( N_a = N_e = N_j = 4 \) and \( R_{th} = 6 \) bits/s/Hz.

Figure 2 illustrates the effect of the number of nodes’ antennas on the SOP with \( P_a = 30 \) dBm. It can be seen that no matter with or without Jammer, the SOP decreases as the numbers of Alice and Bob antennas increase. However, the SOP is increasing until it converges to 1 with the increase of the number of Eve’s antennas, which is consistent with Property 1. In addition, security can hardly be guaranteed without the help of Jammer (the SOP is always above 0.7).

As \( N_e \) changes, Figures 3 and 4 show the effect of \( P_a \) on \( \eta \) and \( \eta^{\nu} \), respectively. As we can see, \( \eta \) and \( \eta^{\nu} \) are indeed decreasing with increasing \( P_a \). However, the trend of SOP decline is not obvious and has a certain lower bound, especially without Jammer. The observation confirms that \( P_a \) has only a limited impact on SOP, which verifies Property 2 and Remark 2.

As we can see from Property 1 and Property 3, the effects of \( N_e \) and \( P_a \) on SOP are the opposite. Therefore, a heat map of SOP over \((P_j, N_e)\) with \( P_a = 30 \) dBm is
provided to further explore their relationship, as shown in Figure 5. We can observe that Jammer only needs to provide 30 dBm transmission power to keep the SOP below 0.1, despite facing S-Eve with 80 antennas. Thus, it could be inferred that our CJ scheme is effective but needs to determine the appropriate $P_j$ according to the security requirements.

In addition to SOP performance verification, we also perform Monte Carlo simulation experiments 10,000 times with random channel parameters to evaluate the impact of $P_j$ and $P_a$ on the average secrecy rate (ASR). It can be seen from Figure 6 that, given the sum of $P_a$ and $P_j$ as a fixed value, there is an optimal power allocation scheme to maximize the ASR. It also shows that there can be different power allocation methods to achieve the same ASR. Therefore, it is of great significance to study the power allocation problem under the total power limit or to minimize the total transmission power given the security requirements.

In this article, we mainly focus on the power minimization problem, expecting to save energy in IoT devices. In Figure 7, we provide the convergence results of the proposed Algorithm 1 to solve this optimization problem. As we can see, the results are consistent with Remark 5 that the algorithm converges after several iterations. In addition to convergence, we can also draw the following conclusions from Figure 7: (1) the higher the requirements (including the security requirement and Bob’s reliable communication requirement), the higher the energy required, as shown in Figure 7(a); (2) the optimized $P_a$ is almost only related to reliable

---

**Figure 2.** SOP versus $N_e$.

**Figure 4.** $\eta^N$ versus $P_a$ without Jammer.

**Figure 3.** $\eta$ versus $P_a$ with Jammer.

**Figure 5.** $\eta$ over $(P_j, N_e)$.
communication requirements, which is shown in Figure 7(b); and (3) whether the security requirements can be met depends on $P_j$, which again proves the conclusion of Figure 3.

Finally, we compare the performance of our proposed scheme with that of the methods proposed by Hu et al.\textsuperscript{26} and Zhang et al.\textsuperscript{27} as illustrated in Figure 8. To be fair, we set the transmission power of all transmitters to be 30 dBm in all the schemes, including source nodes, relays, and jammers. It is worth mentioning that only the transmitters are equipped with multiple antennas in Hu et al.\textsuperscript{26} and all the nodes are equipped with a single antenna in Zhang et al.\textsuperscript{27} According to the result in Figure 8, we can easily draw the conclusion that our proposed scheme with the advantages of multiple antennas is superior to the other two schemes in the fight against collusive eavesdroppers.

**Figure 6.** ASR versus $P_a$ with $N_c = 16$.

**Figure 7.** The convergence of Algorithm 1 for various variables with different requirements: (a) convergence of the objective function $P_a + P_j$, (b) convergence of the variable $P_a$, and (c) convergence of the variable $P_j$.
In this article, considering multiple passive and collusive eavesdroppers in IoT networks, a CJ scheme is proposed. In the CJ scheme, by jointly optimizing the beamforming vector at a controller (transmitter), the decoding vector at an actuator (receiver), and the CJ vector at a friendly jammer (helper), the receiving SINR at the actuator can be maximized. Assuming that the eavesdroppers can collude perfectly, the closed-form SOPs with and without CJ are derived. Moreover, we provide some insights into the impact of various system parameters on the SOP by the asymptotic analysis. In addition, expecting to save the energy of IoT devices, we propose a power allocation algorithm to optimize the transmission power of devices, which can achieve the minimum total transmission power given the security requirements. Finally, the numerical results verify the theoretical analytical results and the effectiveness of the CJ scheme. Our scheme requires that CSI of legitimate nodes can be obtained perfectly. In view of the influence of channel estimation error, we need to further study secure transmission schemes under imperfect channels in our future work. And we just consider Rayleigh fading that is not comprehensive. Thus, in future work, we will also study the performance under other channel models.

Declaration of conflicting interests
The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the Fundamental Research Funds for the Central Universities (Grant No. 2019YJS010).

ORCID iD
Xin Fan https://orcid.org/0000-0003-1660-4290

References
1. Miraz MH, Ali M, Excell PS, et al. A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT). In: Proceedings of the 5th international conference on 2015 internet technologies and applications (ITA), Wrexham, 8–11 September 2015, pp. 219–224. New York: IEEE.
2. Cai Z and He Z. Trading private range counting over big IoT data. In: Proceedings of the 2019 IEEE 39th international conference on distributed computing systems (ICDCS), Dallas, TX, 7–10 July 2019, pp. 144–153. New York: IEEE.
3. Zheng X, Cai Z and Li Y. Data linkage in smart internet of things systems: a consideration from a privacy perspective. IEEE Commun Mag 2018; 56(9): 55–61.
4. Zheng X, Cai Z, Li J, et al. Location-privacy-aware review publication mechanism for local business service systems. In: Proceedings of the IEEE conference on computer communications: IEEE INFOCOM 2017, Atlanta, GA, 1–4 May 2017, pp. 1–9. New York: IEEE.
5. Zheng X, Cai Z, Yu J, et al. Follow but no track: privacy preserved profile publishing in cyber-physical social systems. IEEE IoT J 2017; 4(6): 1868–1878.
6. Cai Z, Zheng X and Yu J. A differential-private framework for urban traffic flows estimation via taxi companies. IEEE Trans Ind Inform 2019; 15(12): 6492–6499.
7. Zou Y, Zhu J, Wang X, et al. A survey on wireless security: technical challenges, recent advances, and future trends. Proc IEEE 2016; 104(9): 1727–1765.
8. Cai Z and Zheng X. A private and efficient mechanism for data uploading in smart cyber-physical systems. IEEE Trans Netw Sci Eng. Epub ahead of print 24 April 2018. DOI: 10.1109/TNSE.2018.2830307.
9. He Z, Cai Z and Yu J. Latent-data privacy preserving with customized data utility for social network data. IEEE Trans Veh Technol 2017; 67(1): 665–673.
10. Cai Z, He Z, Guan X, et al. Collective data-sanitization for preventing sensitive information inference attacks in social networks. IEEE Trans Depend Sec Comput 2016; 15(4): 577–590.
11. Liang Y, Cai Z, Yu J, et al. Deep learning based inference of private information using embedded sensors in smart devices. IEEE Netw 2018; 32(4): 8–14.
12. Sun L and Du Q. A review of physical layer security techniques for internet of things: challenges and solutions. Entropy 2018; 20(10): 730.
13. Soni A, Upadhyay R and Jain A. Internet of things and wireless physical layer security: a survey. In: S Satapathy, V Bhateja, K Raju, et al. (eds) Computer communication, networking and internet security. Cham: Springer, 2017, pp. 115–123.
14. Huo Y, Tian Y, Ma L, et al. Jamming strategies for physical layer security. IEEE Wirel Commun 2018; 25(1): 148–153.
15. Liu Y, Chen H and Wang L. Physical layer security for next generation wireless networks: theories, technologies, and challenges. *IEEE Commun Surv Tutor* 2017; 19(1): 347–376.

16. Atallah M, Kaddoum G and Kong L. A survey on cooperative jamming applied to physical layer security. In: *Proceedings of the 2015 IEEE international conference on ubiquitous wireless broadband (ICUWB)*, Montreal, QC, Canada, 4–7 October 2015, pp. 1–5. New York: IEEE.

17. Mukherjee A, Fakoorian SAA, Huang J, et al. Principles of physical layer security in multiuser wireless networks: a survey. *IEEE Commun Surv Tutor* 2014; 16(3): 1550–1573.

18. Li Z, Jing T, Huo Y, et al. Achieving secure communications in multi-antenna cooperative cognitive radio networks using cooperative jamming. *Int J Sensor Netw* 2016; 22(2): 100–110.

19. Wei L, Jing T, Fan X, et al. The secrecy analysis over physical layer in NOMA-enabled cognitive radio networks. In *Proceedings of the 2018 IEEE international conference on communications (ICC)*, Kansas City, MO, 20–24 May 2018, pp. 1–6. New York: IEEE.

20. Huo Y, Fan X, Ma L, et al. Secure communications in tiered 5g wireless networks with cooperative jamming. *IEEE Trans Wirel Commun* 2019; 18: 3265–3280.

21. Jameel F, Wyne S, Kaddoum G, et al. A comprehensive survey on cooperative relaying and jamming strategies for physical layer security. *IEEE Commun Surv Tutor* 2019; 21: 2734–2771.

22. Zheng TX, Wang HM and Deng H. Improving anti-eavesdropping ability without eavesdroppers CSI: a practical secure transmission design perspective. *IEEE Wirel Commun Lett* 2018; 7(6): 946–949.

23. Fan X, Huang L., Huo Y, et al. Space power synthesis-based cooperative jamming for unknown channel state information. In: *Proceedings of the 2017 international conference on wireless algorithms, systems, and applications*, Guilin, China, 19–21 June 2017. New York: Springer, pp. 483–495.

24. Huang L, Fan X, Huo Y, et al. A novel cooperative jamming scheme for wireless social networks without known CSI. *IEEE Access* 2017; 5: 26476–26486.

25. Li Z, Jing T, Ma L, et al. Worst-case cooperative jamming for secure communications in CIoT networks. *Sensors* 2016; 16(3): 339.

26. Hu L, Wen H, Wu B, et al. Cooperative jamming for physical layer security enhancement in Internet of Things. *IEEE IoT J* 2018; 5(1): 219–228.

27. Zhang Y, Shen Y, Wang H, et al. On secure wireless communications for IoT under evesdropper collusion. *IEEE Trans Automat Sci Eng* 2016; 13(3): 1281–1293.

28. Xu L, Chen J, Liu M, et al. Active eavesdropping detection based on large-dimensional random matrix theory for massive MIMO-enabled IoT. *Electronics* 2019; 8(2): 146.

29. Goel S and Negi R. Secret communication in presence of colluding eavesdroppers. In: *MILCOM 2005—2005 IEEE military communications conference*, vol. 3, Atlantic City, NJ, 17–20 October 2005, pp. 1501–1506. New York: IEEE.

30. Pinto PC, Barros J and Win MZ. Wireless physical-layer security: the case of colluding eavesdroppers. In: *2009 IEEE international symposium on information theory*, Seoul, South Korea, 28 June–3 July 2009, pp. 2442–2446. New York: IEEE.

31. Pinto PC, Barros J and Win MZ. Secure communication in stochastic wireless networks—part II: maximum rate and collusion. *IEEE Trans Inf Forensec Secur* 2011; 7(1): 139–147.

32. Sklar B. *Digital communications*. Upper Saddle River, NJ: Prentice Hall, 2001.

33. Wyner AD. The wire-tap channel. *Bell System Tech J* 1975; 54(8): 1355–1387.

34. Barros J and Rodrigues MRD. Secrecy capacity of wireless channels. In: *2006 IEEE international symposium on information theory*, Seattle, WA, 9–14 July 2006, pp. 356–360. New York: IEEE.

35. Smola AJ, Vishwanathan S and Hofmann T. Kernel methods for missing variables. In: *Proceedings of the 10th international workshop on artificial intelligence and statistics*, 2005. CiteSeer, http://www.gatsby.ucl.ac.uk/aistats/fullpapers/234.pdf

36. Grant MC and Boyd SP. Graph implementations for nonsmooth convex programs. In: VD Blondel, SP Boyd and H Kimura (eds) *Recent advances in learning and control*. New York: Springer, 2008, pp. 95–110.

37. Yuille AL and Rangarajan A. The concave-convex procedure. *Neural Comput* 2003; 15(4): 915–936.

38. Horn RA and Johnson CR. *Matrix analysis*. Cambridge: Cambridge University Press, 1990.

39. Gradshteyn IS and Ryzhik IM. *Table of integrals, series, and products*. Waltham, MA: Academic Press, 2014.

40. Bolton D. The multinomial theorem. *Math Gazette* 1968; 52(382): 336–342.

**Appendix I**

**Proof of Lemma 1**

To maximize the SINR at Bob, it is necessary to eliminate the influence of the jamming signal on Bob. Thus, \( z \) should be designed appropriately to make \( d_b^T H_{jb} z = 0 \).

It is easy for us to work out such a solution that \( z = Z a \), where \( a \in \mathbb{C}^{N_j \times 1} \sim \mathcal{C}N(0, I_{N_j}) \) is a complex Gaussian noise vector and \( Z \in \mathbb{C}^{N_j \times N^2} \) is a symmetric idempotent matrix (with the characteristics of \( Z^H = Z \) and \( ZZ = Z \)), satisfying

\[
Z = \left( I_{N_j} - \frac{H_{jb}^T d_b^T d_b H_{jb}}{\|d_b H_{jb}\|^2} \right) \quad (35)
\]

Once the jamming signal is eliminated at Bob, problem \( \textbf{P1} \) can be reduced to \( \textbf{P2} \)

\[
\textbf{P2} : \quad \{d_b, w\} = \arg \max_{d_b, w} P_{a1} |d_b H_{ab} w|^2 \quad (36)
\]

Suppose that \( H_{ab} \) has the following form of SVD
\[ \mathbf{H}_{ab} = \mathbf{USV}^H \]  

(37)

where \( \mathbf{U} \in \mathbb{C}^{N_x \times N_\text{x}} \) and \( \mathbf{V} \in \mathbb{C}^{N_y \times N_\text{y}} \) are both unitary matrices and \( \mathbf{S} \in \mathbb{C}^{N_\text{x} \times N_\text{y}} \) is a semi-definite diagonal matrix.

Assuming that the diagonal elements \( \lambda_1 \geq \lambda_2 \cdots \geq \lambda_r \) of \( \mathbf{S} \) are the ordered singular values of matrix \( \mathbf{H}_{ab} \), where \( r = \text{Rank}(\mathbf{H}_{ab}) \), we can obtain the optimal \( \mathbf{d}_a \) and \( \mathbf{w} \) that are the master left singular vector and the master right singular vector, respectively, to maximize \( \mathbf{d}_a^H \mathbf{H}_{ab} \mathbf{w} \), that is

\[ \mathbf{d}_a = \text{the first row of } \mathbf{U}^H \]  

(38)

\[ \mathbf{w} = \text{the first column of } \mathbf{V} \]  

(39)

According to Horn and Johnson,\(^{38}\) the maximum value of \( |\mathbf{d}_a^H \mathbf{H}_{ab} \mathbf{w}| \) is the largest singular value \( \lambda_{\text{max}} \) of \( \mathbf{H}_{ab} \). As a result, \( \mathbf{d}_a \mathbf{H}_{ab} \mathbf{w} = \lambda_1 \), and these complete the proof of Lemma 1.

**Proof of Proposition 1**

Under the assumption that all the wireless channels are independent Rayleigh slow-flat fading, we can rewrite X as \( X = P_a \sum_{i=1}^{N_\text{c}} |u_{x,i}|^2 \), where \( u_{x,i} \sim \mathcal{CN}(0,1) \) is the received signal at the \( i \)th antenna of S-Eve. Thus, we can easily confirm that \( X \sim \Gamma(\alpha, \theta) \), and then the probability density function (PDF) of \( X \) can be expressed as follows

\[ f_X(x) = \frac{x^{N_\text{c}-1}}{P_a^N \Gamma(N_\text{c})} e^{-\frac{1}{2}x}, \quad x > 0 \]  

(40)

where \( \Gamma(x) = \int_0^\infty t^{x-1} e^{-t} \, dt \) is the gamma function.

Furthermore, it is not difficult to find that \( Y \sim \chi^2(\alpha) \) and \( Y \sim \exp(1/P_j) \). Therefore, we can give the PDF of \( Y \) as follows

\[ f_Y(y) = \frac{1}{P_j} e^{-\frac{1}{P_j} y}, \quad y > 0 \]  

(41)

From equations (40) and (41), we can calculate the CCDF of \( \text{SINR}_c \) as follows

\[ F_{\text{SINR}}(\tau) = \Pr(\text{SINR}_c > \tau) = \Pr(X > \tau + \tau Y) = \int_0^\infty \left( \int_0^\infty f_X(x) \, dx \right) \, dy \]  

(42)

where \( \tau > 0 \).

As we can see, the inner integral in equation (42) should be first solved. Substituting equation (40) into equation (42), we can calculate the inner integral as

\[ \int_0^\infty f_X(x) \, dx = \frac{1}{P_a} \Gamma(N_\text{c}) \int_0^\infty x^{N_\text{c}-1} \exp\left(-\frac{x}{P_a}\right) \, dx \]  

(43)

where \( \Gamma(m, x) = \int_x^\infty x^{m-1} \exp(-t) \, dt \) represents the upper incomplete gamma function.

According to Gradshteyn and Ryzhik,\(^{39}\) due to the fact that \( N_\text{c} \) is an integer, the closed-form of equation (43) can be rewritten as

\[ \int_0^\infty f_X(x) \, dx = \frac{\Gamma(N_\text{c}, (\tau + \tau y)/P_a)}{\Gamma(N_\text{c})} = \exp\left(-\frac{\tau + \tau y}{P_a}\right) \sum_{k=0}^{N_\text{c}-1} \frac{(\frac{1}{P_a})^k}{k!} (\tau + \tau y)^k \]  

(44)

Based on the binomial theorem,\(^{40}\) we can obtain

\[ (\tau + \tau y)^k = \sum_{i=0}^k C_i y^i \tau^k \]  

(45)

where \( C_i = \frac{k!}{i!(k-i)!} \) represents the binomial expansion coefficient.

According to equations (41)-(45), we can further calculate the CCDF of \( \text{SINR}_c \) as follows

\[ F_{\text{SINR}}(\tau) = \exp\left(-\frac{\tau}{P_j}\right) \sum_{k=0}^{N_\text{c}-1} \frac{1}{k!} \left(\frac{1}{P_a}\right)^k \tau^k \sum_{i=0}^k C_i \left(\frac{\tau}{P_a} + \frac{1}{P_j}\right)^i \]  

(46)

Let \( \beta = \gamma((\tau/P_a) + (1/P_j)) \); then the integral in equation (46) can be converted into

\[ \int_0^\infty y^i \exp\left(-y \left(\frac{\tau}{P_a} + \frac{1}{P_j}\right)\right) \, dy = \left(\frac{\tau}{P_a} + \frac{1}{P_j}\right)^{-i-1} \int_0^\infty y^i \exp(-\beta) \, d\beta = \left(\frac{\tau}{P_a} + \frac{1}{P_j}\right)^{-i-1} \Gamma(i + 1) \]  

(47)
Eventually, by substituting equation (47) into equation (46), the closed-form expression of the CCDF of $SINR_e$ can be given as follows

$$F_{SINR_e}(\tau) = \frac{1}{P_a} \exp \left( -\frac{\mu}{P_a} \right) \sum_{k=0}^{N_e-1} \frac{1}{k!} \left( \frac{\mu}{P_a} \right)^k$$

$$\times \sum_{i=0}^k C_i \left( \frac{\mu}{P_a} + \frac{1}{P_a} \right)^{i-1} \Gamma(i+1). \tag{48}$$

The proof of Proposition 1 is completed.

**Proof of Properties 1–3**

For Property 1, the well-known Taylor series expansion of the exponential function $e^x$ at $x_0 = 0$ can be given by

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots = \sum_{n=0}^{\infty} \frac{x^n}{n!}. \tag{49}$$

Then, the asymptotic expression of $\eta^{NJ}(\mu)$ with the infinite value of $N_e$ can be derived as

$$\lim_{N_e \to \infty} \eta^{NJ}(\mu) = \lim_{N_e \to \infty} \exp \left( -\frac{\mu}{P_a} \right) \sum_{k=0}^{N_e-1} \frac{1}{k!} \left( \frac{\mu}{P_a} \right)^k$$

$$= \exp \left( -\frac{\mu}{P_a} \right) \sum_{k=0}^{\infty} \frac{1}{k!} \left( \frac{\mu}{P_a} \right)^k \tag{50}$$

(a) $\approx \exp \left( -\frac{\mu}{P_a} \right) \exp \left( \frac{\mu}{P_a} \right) = 1,$

where the step (a) requires $0 < \frac{\mu}{P_a} \leq 1$ to achieve a better approximation result according to the McLaughlin expansion.

Moreover, we can obtain the asymptotic expression of $\eta(\mu)$ with the infinite value of $N_e$ as follows

$$\lim_{N_e \to \infty} \eta(\mu) = \lim_{N_e \to \infty} \frac{1}{P_a} \exp \left( -\frac{\mu}{P_a} \right) \sum_{k=0}^{N_e-1} \frac{1}{k!} \left( \frac{\mu}{P_a} \right)^k$$

$$\times \sum_{i=0}^k C_i \left( \frac{\mu}{P_a} + \frac{1}{P_a} \right)^{i-1} \Gamma(i+1)$$

$$= \lim_{N_e \to \infty} \sum_{i=0}^k \frac{1}{k!} \left( \frac{\mu}{P_a} + \frac{1}{P_a} \right)^{i-1} \Gamma(i+1)$$

$$= \lim_{N_e \to \infty} \frac{1}{P_a} \exp \left( P_a s + 1 \right)$$

$$\times \sum_{k=0}^{\infty} \frac{s^k \xi^k}{(k-1)!} + \frac{s^{k-1} \xi^k}{(k-2)!} + \cdots + \frac{\xi^k}{k!}$$

$$= \frac{s^0 \xi^0 + s^1 \xi^1 + \cdots + s^k}{e^s(P_a s + 1)}$$

$$= \frac{1}{1-e^s} \frac{e^s}{e^{P_a s + 1}} \frac{1}{P_a s + 1} \left( 1 - \frac{1}{e^s} \right) = 1 \tag{51}$$

where $s = \mu / P_a$ and $\xi = s / (s + (1 / P_a))$. It is worth noting that we apply the sum formula of geometric progression and the closed-form expression of SOP in step (b).

For Property 2, $\lim_{P_a \to \infty} s$ needs to be calculated as

$$\lim_{P_a \to \infty} s = \lim_{P_a \to \infty} \frac{2R_a - R_b - 1}{P_a}$$

$$= \lim_{P_a \to \infty} \frac{1 + \frac{SINR_b}{2R_a} - 1}{P_a} \tag{52}$$

$$= \lim_{P_a \to \infty} \left( \frac{1 + \frac{R_{\text{max}}^2}{2R_a P_a} - 1}{P_a} \right) = \frac{\lambda_{\text{max}}^2}{2R_a}$$

Then substituting equation (52) into equations (18) and (19), respectively, we can calculate the asymptotic expressions in Property 2 as

$$\lim_{P_a \to \infty} \eta(\mu) = \frac{N_e - k}{e^{\xi P_a} P_a} \tag{53}$$

$$\lim_{P_a \to \infty} \eta^{NJ}(\mu) = \exp(-\xi) \sum_{k=0}^{\infty} \frac{1}{k!} \xi^k \tag{54}$$

where $\xi = \lambda_{\text{max}}^2 / 2R_a$ and $\overline{\xi} = \overline{s} / (\overline{s} + (1 / P_a))$.

As for Property 3, we can draw this conclusion directly from the closed-form expression of SOP that $\eta(P_a) \xrightarrow{\Delta} 0$ as $P_a \to \infty$. Thus, we have completed the proof of all properties.