Robust Secrecy Competition With Aggregate Interference Constraint in Small-Cell Networks

Xiao Tang, *Member, IEEE*, Ruonan Zhang, *Member, IEEE*, Wei Wang, *Member, IEEE*, Lin Cai, *Fellow, IEEE*, and Zhu Han, *Fellow, IEEE*

***Abstract*— In this article, we address the security issue in a tiered small-cell network aiming at security optimization for small-cell users (SUEs) to defend against eavesdropping. Meanwhile, the transmissions from small-cell base stations (SBSs) are subject to the aggregate interference constraints of macro-cell users (MUEs). In particular, we consider two-fold information uncertainties in small cells, i.e., the uncertainties regarding the eavesdroppers and interference channels to the MUEs. As such, the SBSs compete for robust secrecy rate with robust protection for the MUEs. We adopt the generalized robust Nash equilibrium problem (GRNEP) formulation, for which we confirm the existence of equilibrium and analyze the condition for the uniqueness with variational inequality-assisted analysis. Furthermore, to solve for the equilibrium, we introduce the pricing mechanism and decompose the original GRNEP as a nonlinear complementarity problem with a priced NEP, where the former provides solution of price coefficients and the latter for resource allocation strategies based on given prices. Finally, extensive simulation results are provided to demonstrate the impacts of the interference constraint and uncertainties upon the security performance of an individual SUE and the overall network, which also corroborate the effectiveness of our proposal in security provisioning for the SUEs and interference protection for the MUEs.**

Manuscript received February 19, 2020; revised August 21, 2020; accepted November 15, 2020. Date of publication December 8, 2020; date of current version April 9, 2021. The work of Xiao Tang was supported in part by the National Natural Science Foundation of China under Grant 61941119 and Grant 61901378 and in part by China Postdoctoral Science Foundation under Grant BX20190287 and Grant 2020M683563. The work of Ruonan Zhang was supported in part by the National Natural Science Foundation of China under Grant 61571370, in part by the Science and Technology Research Program of Shaanxi Province under Grant 2019ZDLGY07-10, in part by the Advance Research Program on Common Information System Technologies under Grant 315045204 and Grant 315075702. The work of Zhu Han was supported by US NSF under Grant EARS-1839818, Grant CNS1717454, Grant CNS-1731424, and Grant CNS-1702850. The associate editor coordinating the review of this article and approving it for publication was Y. Cui. *(Corresponding author: Ruonan Zhang.)*

Xiao Tang and Ruonan Zhang are with the Department of Communication Engineering, Northwestern Polytechnical University, Xi'an 710072, China (e-mail: tangxiao@nwpu.edu.cn; rzhang@nwpu.edu.cn).

Wei Wang is with the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China (e-mail: wei_wang@nuaa.edu.cn).

Lin Cai is with the Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC V8P 5C2, Canada (e-mail: cai@ece.uvic.ca).

Zhu Han is with the Department of Electrical and Computer Engineering, University of Houston, Houston, TX 77004 USA, and also with the Department of Computer Science and Engineering, Kyung Hee University, Seoul 446-701, South Korea (e-mail: zhan2@uh.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TWC.2020.3041339.

Digital Object Identifier 10.1109/TWC.2020.3041339

***Index Terms*— Small-cell networks, robust secrecy, interference constraint, resource allocation, pricing mechanism, equilibrium, distributed algorithm, variational inequality.**

I. Introduction

THE small-cell networks, including microcell, picocell, femtocell overlaying conventional macrocell, are envisioned as the essentials for the infrastructure in 5G era and beyond [1]. Small-cell base stations (SBSs) feature low-cost, low-power, and on-demand operation, enabling a flexible and agile network architecture that significantly reduces the capital expenditure and operating expense for the network operators. Meanwhile, with widely deployed small cells in the users' vicinity, the user experience can be remarkably enhanced with seamless services and spectral- and energy-efficient communications [2].

With the prosperity of various wireless services enhanced by small-cell networks, there have been growing concerns for wireless information security, as the dense network infrastructure not only supports the legitimate users, but also eases the eavesdropping. The existing security defenses in current systems mostly depend on encryption-based methods, a typical example is the hierarchical key generation architecture in the 5G standards [3]. However, with the skyrocketing number of wireless devices and increasing heterogeneity of wireless networks, the key-based methods are significantly challenged in terms of key management and distribution issues. Moreover, the limited capability and resources of small-cell base stations may not effectively support the required computation complexity of certain cryptography. In this regards, physical layer security has emerged as a promising technology with guaranteed security provisioning. The physical layer security exploits the intrinsic characteristics of wireless medium, such as fading, interference, and noise, enabling keyless secure transmissions and thus facilitating the implementation in the tiered and heterogeneous small-cell networks [4].

Generally, physical layer security can be achieved when the eavesdropping channel is a degraded version of the legitimate transmission channel. As such, most of the existing researches are devoted to enhance the legitimate transmissions or weaken the undesired receptions [5]. In this regard, the spatial diversity and cooperative transmission are often leveraged to enhance the security, such as multi-antenna beamforming [6], artificial noise injection [7], cooperative relay and jamming [8], and so on. Recently, due to the rapid development of the 5G

system, the physical layer security has been investigated under joint consideration with 5G transmission technologies, such as device-to-device (D2D) communications, full-duplex transmissions, massive multiple-input multiple-output (MaMIMO), millimeter wave (mmWave), non-orthogonal multiple access (NOMA), and so on [9].

Although there have been abundant research works on physical layer security, they mainly investigate the security for point-to-point transmission links. While in contrast, the security issue in a networked scope can be more complicated and thus has not been sufficiently addressed, where the works specially targeting at small-cell security are even less [10]. From the perspective of network, we need to not only elaborately design the link-level secure transmission strategy, but also consider the interactions among different users and their influence upon the overall security performance. In particular, for the small cells that usually operate in an autonomous manner, the user needs to appropriately adapt its security strategy with joint consideration on its surrounding environment and behavior of other users. Moreover, the concurrent transmissions among users in different tiers result in complicated interference. Although the interference conventionally appears as an unfavorable element in wireless networks, it can also exploited as a constructive factor in terms of wireless security to mitigate the eavesdropping. Consequently, the autonomous operation of small-cell network needs to tackle the interference smartly so as to implicitly exploit the interference for security enhancement.

Moreover, due to the limited resources and lightweight signaling in small cells, the users need to determine their security strategies independently in a distributed manner [11]. However, due to the hierarchical structure of small-cell networks, the users of different tiers are of diversified service requirements, where the macrocell users are usually of higher priorities and guaranteed protection. As such, the security issue of small cells needs to be addressed subject to quality-of-service constraints of the macrocell. Meanwhile, due to the limited capability of small cells, the perfect channel state information may not be available. Thus, secure transmission scheme needs to incorporate the uncertainties into consideration to achieve robust designs. Therefore, physical layer security for small-cell networks needs to integrate the practical constraints and uncertainties in distributed security strategy design, so as to provide better insight for real implementations.

Consider the aforementioned issues, we in this work investigate the physical layer security for a small-cell network under the interference constraint. In particular, we address the distributed secure transmissions for the small-cell users (SUEs) while guaranteeing their aggregate interference to the maceocell users (MUEs) to be below a threshold. Meanwhile, we incorporate multi-fold information uncertainties into consideration towards robust security design. We formulate the security issue under the generalized robust Nash equilibrium problem (GRNEP) framework with variational inequality (VI)-assisted analysis and a distributed secure resource allocation strategy is proposed. To be specific, the main contribution of this work is summarized as follows.

- We investigate the physical layer security for a small-cell network under interference constraint. We consider the information uncertainties regarding the eavesdropper and interference to the MUE, whereas the robust security is achieved for the SUEs with robust protection of the MUEs.
- We formulate the problem as a GRNEP, for which we confirm the existence of the equilibrium. Further, we derive the VI-equivalent problem for the original GRNEP and derive the condition for the unique equilibrium with VI-assisted analysis.
- We introduce the pricing mechanism and tackle the interference constraint as a price. Then, the GRNEP is decomposed as a nonlinear complementarity problem (NCP) and a priced Nash equilibrium problem, where the former is solved for price coefficients and the latter to determine the transmission strategy based on the obtained price.
- We provide extensive simulation results to demonstrate the influence of the considered multi-fold uncertainties and interference constraint upon the transmission behavior of SUEs and the performance. The results also verify the effectiveness of our proposal in terms of security provisioning for SUEs and protection for MUEs.

The rest of this article is organized as follows. In Sec. II, we review the related works. In Sec. III, a tiered small-cell network model is presented. In Sec. IV, we adopt the GRNEP to formulate the secrecy competition with interference constraint and analyze the properties of the equilibrium. In Sec. V, we decompose the GRNEP as a NCP with priced NEP and propose the algorithm design. Sec. VI provides the simulation results and Sec. VII concludes this article.

II. Related Works

Since small-cell network brings multi-fold benefits for both operators and users, it has attracted research interest from both academia and industries, covering a wide variety of topics [1], [2]. In [12], the authors investigate the distributed interference management in a small-cell network to maximize the network utility. In [13], the authors consider the energy minimization for small-cell networks, where power control and discontinuous transmissions are jointly optimized. Data dissemination in small cells is addressed in [14], where the authors propose to exploit caching with contract theory-assisted mechanism design. In [15], the authors propose a mobility-aware load balancing algorithm for small-cell networks with jointly optimization of handover and resource management. In [16], the authors exploit the fog-radio access network architecture and develop a wireless backhauling algorithm for small-cell networks through cooperative transmissions.

Meanwhile, physical layer security has been extensively addressed with rich results. Besides the classical approaches such as multi-antenna transmissions and cooperations, physical layer security has been more frequently investigated with 5G technologies recently [9], [17]. In [18], the authors consider the D2D communications overlaying cellular networks, where the D2D links conduct friendly jamming for transmission slots. In [19], the authors investigate the full-duplex active

eavesdropping where both the legitimate transmission strategy and jamming strategy are analyzed. The security issue under MaMIMO relaying is addressed in [20], where the joint power and transmission time optimization is conducted. The authors of [21] consider the mmWave communications and propose a hybrid phased-array time-modulated directional modulation for physical layer security. In [22], the authors consider a cognitive NOMA transmissions by pairing the primary user and secondary user to allow them to transmit simultaneously while guarantee the security for the primary users.

From a networked perspective, the security issue needs to be jointly considered with interactions among the users and thus generally becomes more complicated. In [23], the authors investigate the security issue in a two-tier heterogeneous networks with shared spectrum, where an interference cancellation scheme is proposed based on distributed antenna system so as to enhance the security of macrocell transmissions. In [24], the authors consider a three-tier wireless sensor network and derive the average secrecy rate with stochastic geometry-based modeling and analysis. The authors of [25] investigate security issue in a single-stream MIMO network with interference management. The problem is formualted as a non-cooperative game, based on which a distributed strategy is proposed. The authors of [26] address the security issue in a large-scale wireless network, where stochastic geometry and queueing theory are employed to analyze the tradeoff between security and delay performance. In [27], the authors consider a wireless network where coexist security-oriented users and regular users, for which they propose a priority-based transmission strategy that allows the security-oriented users an resource advantage to enhance the security.

The physical layer security solution for small-cell networks has emerged recently with growing attentions. In [28], the authors propose to enhance the small-cell security with different transmitter selection strategies. In [29], the authors exploit artificial-noise jamming to enhance the security along with stochastic geometry-based performance analysis. In [30], the authors investigate the security issue with caching cooperative transmission in small-cell networks to defend against randomly-located eavesdroppers. In [31], the authors investigate the mmWave small-cell security from the perspective of physical channel, where the influence of richness of radio environment over security performance is revealed. In [32], the authors address the security issue for a small-cell network and propose the security solution based on perfect channel state information.

III. System Model

We consider the downlink transmissions in a tiered network where there is a MBS covers N MUEs, denoted by $\mathcal{N} = \{1, 2, \cdots, N\}$. Also, there coexist J small cells, denoted by $\mathcal{J} = \{1, 2, \cdots, J\}$. In each small cell, there is a SBS having a SUE in service, while there also exists an eavesdropper from which the SBS-SUE transmissions need to be protected. Here we assume that the SBS has the channel state information of the SUE and the eavesdropper, but the information

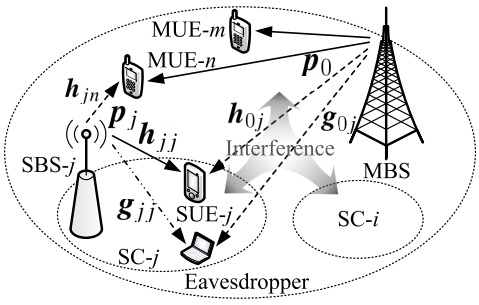


Fig. 1. System model.

regarding the latter is not perfectly known.[1] Meanwhile, there are K orthogonal channels, denoted by $\mathcal{K} = \{1, 2, \cdots, K\}$, accessible to macrocell as well as the small-cell system. The system model is shown in Fig. 1. For the transmissions in the j-th small cell, the transmit power in channel-k is denoted as $p_j(k)$. Due to limited power budget, the power vector of SBS-j, i.e., $\boldsymbol{p}_j = [p_j(k)]_{k\in\mathcal{K}}$, is constrained by

$$\boldsymbol{p}_j \in \mathcal{P}_j = \left\{ \boldsymbol{p}_j \in \mathbb{R}^K \left| \begin{array}{l} 0 \le p_j(k) \le p_j^{\max}, \forall k \in \mathcal{K}, \\ \sum\limits_{k\in\mathcal{K}} p_j(k) \le p_j^{\max} \end{array} \right. \right\}, \tag{1}$$

where $p_j^{\max}$ is the spectrum mask at each channel and $p_j^{\max}$ is the maximum allowed transmit power. Similarly, we use $\boldsymbol{p}_0 = [p_0(k)]_{k\in\mathcal{K}}$ to denote the transmit power of the macrocell base station. For the transmissions from SBS-i to SUE-j in channel-k, the link gain is denoted as $h_{ij}(k)$, and the link gain from the maceocell base station in the same channel is $h_{0j}(k)$. Meanwhile, for the wiretap channels, the link gain from SBS-i to the eavesdropper in the j-th small cell in channel-k is denoted as $g_{ij}(k)$, and also affected by the macrocell transmissions with link gain $g_{0j}(k)$. On the other hand, the transmissions in small cells also affect the receptions of MUEs in the macrocell. In this regard, the interference signal from SBS-j to MUE-n in channel-k experiences a link gain of $h_{jn}(k)$.

Based on the definitions noted above, we can obtain the signal-to-interference-plus-noise ratio (SINR) of the legitimate transmissions of SUE-j over channel-k as

$$\mathsf{SINR}_j^{\text{lgt}}(k) = \frac{p_j(k)\, h_{jj}(k)}{\sum\limits_{i\in\mathcal{J}\setminus\{j\}} p_j(k)\, h_{ij}(k) + p_0(k)\, h_{0j}(k) + \sigma_0^2}, \tag{2}$$

where the interference from both macrocell and small cells are incorporated, along with the background noise power denoted by σ_0^2. As we in this work mainly focus on the interference-limited communications, we assume the noise power is identical over all channels for all SUEs. Similarly, we can obtain

[1] A typical example to justify the assumptions here is that, the eavesdropper also belongs to the system, rather than being some external malicious node. But the eavesdropper is currently unscheduled and the channel information of it may be outdated and thus of uncertainties, as will be specified later.

the SINR of eavesdropper of SUE-j over channel-k as

$$\mathsf{SINR}_j^{\text{eve}}(k) = \frac{p_j(k)\, g_{jj}(k)}{\sum\limits_{i\in\mathcal{J}\setminus\{j\}} p_i(k)\, g_{ij}(k) + p_0(k)\, g_{0j}(k) + \sigma_0^2}, \tag{3}$$

where we can see that the eavesdropping in the small-cell systems are also affected by not only the interference from other small cells but also the macrocell. Given the SINRs in (2) and (3), we can obtain the secrecy rate of SUE-j as[2]

$$\begin{aligned} C_j &= \sum_{k\in\mathcal{K}} \left[\log\left(1+\mathsf{SINR}_j^{\text{lgt}}(k)\right) - \log\left(1+\mathsf{SINR}_j^{\text{eve}}(k)\right)\right]^+ \\ &= \sum_{k\in\mathcal{K}} \left[\log\frac{1+\mathsf{SINR}_j^{\text{lgt}}(k)}{1+\mathsf{SINR}_j^{\text{eve}}(k)}\right]^+, \end{aligned} \tag{4}$$

where $(\cdot)^+ = \max\{\cdot, 0\}$. In this work, we consider not only the secrecy optimization for the SUEs, but also the quality-of-service provisioning for the MUEs, as the transmissions in the macrocell are usually of higher priorities. Consider the interference imposed at the MUEs by small cells, we present an interference constraint to protect the receptions at MUEs. In particular, we assume there is an interference threshold at each MUE to limit the aggregated interference from the small cells, given as

$$\sum_{k\in\mathcal{K}}\sum_{j\in\mathcal{J}} p_j(k)\, h_{jn}(k) \le I_n^{\text{th}}, \quad \forall n\in\mathcal{N}, \tag{5}$$

where I_n^{th} is the interference threshold at MUE-n. Note the constraints in (5) are applied at all small cells at the same time.

The discussions above employ an implicit assumption of perfect channel state information, which may not be readily available in small-cell networks due to the limited capability and resources of the SBSs. From the perspective of real implementation, the SBS does not always interact with the eavesdropper and MUEs, whereas the related information can be difficult to be obtained. Thus, we consider two-fold uncertainties as detailed below. First, the SBS has imperfect channel state information regarding its eavesdropper. Specifically, consider the channel state information of the eavesdropper of SUE-j over channel-k, i.e., $\boldsymbol{g}_j(k) = [g_{ij}(k)]_{i\in\mathcal{J}\cup\{0\}}$, then we have

$$\boldsymbol{g}_j(k) = \hat{\boldsymbol{g}}_j(k) + \tilde{\boldsymbol{g}}_j(k), \tag{6}$$

where $\hat{\boldsymbol{g}}_j(k)$ is an estimate based on previous knowledge and $\tilde{\boldsymbol{g}}_j(k)$ denotes the unknown part. For $\tilde{\boldsymbol{g}}_j(k)$, we assume it is of bounded uncertainty defined as

$$\begin{aligned} &\tilde{\boldsymbol{g}}_j(k) \in \mathcal{G}_j(k) \\ &\quad= \left\{\tilde{\boldsymbol{g}}_j(k)\in\mathbb{R}^{J+1} \,\middle|\, \begin{array}{l} |\tilde{g}_{jj}(k)|^2 \le \epsilon_j(k) \\ \sum\limits_{i\in\mathcal{J}\setminus\{j\}\cup\{0\}} |\tilde{g}_{ij}(k)|^2 \le \varepsilon_j(k) \end{array}\right\}, \end{aligned} \tag{7}$$

[2]We will simply drop the non-differential operation $(\cdot)^+$ in the later discussions, as we only focus on the channels that positive secrecy rate can be achieved, while removing the channels with non-positive secrecy rate.

where $\epsilon_j(k)$ and $\varepsilon_j(k)$ are the constants specifying the uncertainty regions. Note that in (7), we present the uncertainty model for the wiretap channel and interference channels independently at the eavesdropper, as the former concerns the intended transmitter while the latter for unintended ones. As the wiretap channels relate to the transceivers within the same small cell while the interference channels correspond to inter-cell communications, the uncertainties therein can be different and model in (7) allows flexible treatments regarding different channels. Second, the information regarding interference channels from the SBSs to the MUEs is imperfectly known. Specifically, for the interference channels concerning MUE-n, i.e., $\boldsymbol{h}_n = [h_{jn}(k)]_{j\in\mathcal{J},k\in\mathcal{K}}$, it is modeled as

$$\boldsymbol{h}_n = \hat{\boldsymbol{h}}_n + \tilde{\boldsymbol{h}}_n, \tag{8}$$

where, similar to (7), $\hat{\boldsymbol{h}}_n$ is the known estimate and $\tilde{\boldsymbol{h}}_n$ is the uncertain part bounded by

$$\tilde{\boldsymbol{h}}_n \in \mathcal{H}_n = \left\{\tilde{\boldsymbol{h}}_n\in\mathbb{R}^{JK} \,\middle|\, \sum_{j\in\mathcal{J}}\sum_{k\in\mathcal{K}} \left|\tilde{h}_{jn}(k)\right|^2 \le e_n\right\}, \tag{9}$$

where e_n is a constant determining the size of bound region. Note in (9), the uncertainty at each MUE is related to the interference channels from all small cells at the same time.

IV. GRNEP Formulation and Equilibrium Analysis

In this section, we investigate the competitive secure transmissions among the SBSs under the interference constraints of MUEs. Due to the uncertainties on channel state information, we aim at robust secrecy maximization for SUEs with robust protection for MUEs. We formulate the problem as a GRNEP, along with the analysis of the properties of its equilibrium.

A. GRNEP Formulation

As the signaling and coordination in the small-cell networks is relatively expensive, it is more practical and rational for the SBSs to optimize their own security performance. However, due to the local uncertainties regarding the eavesdropper, the individual SBS then considers the robust secrecy rate, given as

$$\min_{[\tilde{\boldsymbol{g}}_j(k)]_{k\in\mathcal{K}}} \quad C_j \tag{10a}$$

$$\text{s.t. } \tilde{\boldsymbol{g}}_j(k) \in \mathcal{G}_j(k), \quad \forall k\in\mathcal{K}. \tag{10b}$$

For notation simplicity, we denote the solution to (10) as $\bar{C}_j$ hereinafter. On the other hand, consider the uncertainties of the interference channel from SBSs to MUEs, we introduce

$$\zeta_n(\boldsymbol{p}) = \max_{\tilde{\boldsymbol{h}}_n\in\mathcal{H}_n} \sum_{k\in\mathcal{K}}\sum_{j\in\mathcal{J}} p_j(k)\, h_{jn}(k) - I_n^{\text{th}} \tag{11}$$

to denote the worst-case interference at MUE-n, where $\boldsymbol{p} = \left[\boldsymbol{p}_j\right]_{j\in\mathcal{J}}$ is the power vector of all SBSs. Then, to guarantee a robust protection for the MUEs, the transmit power of SBSs needs to satisfy the following constraint

$$\boldsymbol{p}\in\tilde{\mathcal{P}} = \left\{\boldsymbol{p}\in\mathbb{R}^{JK} \,|\zeta_n \le 0, \forall n\in\mathcal{N}\right\}. \tag{12}$$

For the constraint in (12) that affects all SBSs simultaneously, we can reinterpret it in the sense of each individual SBS, given as

$$\tilde{\mathcal{P}}_j\left(\boldsymbol{p}_{-j}\right)=\left\{\boldsymbol{p}_j\in\mathbb{R}^K\,\middle|\,\left(\boldsymbol{p}_j,\boldsymbol{p}_{-j}\right)\in\tilde{\mathcal{P}}\right\} \tag{13}$$

for SBS-j, where $\boldsymbol{p}_{-j}=\left[\boldsymbol{p}_j\right]_{j\in\mathcal{J}\setminus\{j\}}$ is the power of all SBSs except SBS-j. Note that in (13), the SBS-specified power constraint is a function of the transmit power of other SBSs. Recall the maximum-allowed transmit power at each individual SBS defined in (1), the power constraint for SBS-j becomes

$$\bar{\mathcal{P}}_j\left(\boldsymbol{p}_{-j}\right)=\mathcal{P}_j\cap\tilde{\mathcal{P}}_j\left(\boldsymbol{p}_{-j}\right), \tag{14}$$

which is no longer independent, but influenced by the transmit power of other SBSs. Based on the discussions above, we can formulate individual optimization for SBSs, given as

$$\max_{\boldsymbol{p}_j}\ \bar{C}_j \tag{15a}$$

$$\text{s. t. } \boldsymbol{p}_j\in\bar{\mathcal{P}}_j\left(\boldsymbol{p}_{-j}\right) \tag{15b}$$

for SBS-$j\in\mathcal{J}$, which maximizes the robust secrecy rate while incorporating the robust protection for the MUEs.

We have formulated the problem for each SBS to maximize their own robust secrecy rate in the form of (15). Then, consider the problems of all SBSs in a networked scope, they share the network resources and behave in a competitive manner to optimize their own security performance. In this regard, by concatenating the problem in (15) for all SBSs, we arrive at a GRNEP, denoted as

$$\mathfrak{G}=\left\{\mathcal{J},\left\{\bar{\mathcal{P}}_j\right\}_{j\in\mathcal{J}},\left\{\bar{C}_j\right\}_{j\in\mathcal{J}}\right\}, \tag{16}$$

where SBSs are the players with robust secrecy as the utility function. For the terminology "GRNEP", the "NEP" reveals the competitive nature among SBSs and their behavior in a distributed manner, the "robust" emphasizes the robust secrecy rate optimization at each SBS, and it is "generalized" since the player's strategy space is no longer fixed as in a generic NEP, but is a function of the strategies of other players.

For the problem in (16), we can see three-fold difficulties when trying to solve for the equilibrium. First, only the legitimate channels are perfectly known, we need to tackle the uncertainties regarding the eavesdropper and interference channels to the MUEs. Second, from a mathematical perspective, for the individual problem at each SBS, the objective function needs to be obtained from another optimization problem in (10) and the feasible region is no longer independent, but a function of the strategies of its competitors as (14). Third, from a networked scope, we need to solve the individual optimization for each individual SBS and further address their interactions in a competitive manner to achieve the network equilibrium.

B. Equilibrium Analysis

For the GRNEP in (16), its solution is characterized by the equilibrium, which is generally defined as the strategy profile that no SBS will unilaterally deviate if all others remain at current strategies. Specifically, denote the equilibrium as $\boldsymbol{p}^\star=\left[\boldsymbol{p}_j^\star\right]_{j\in\mathcal{J}}$, then it satisfies

$$\bar{C}_j\left(\boldsymbol{p}_j^\star,\boldsymbol{p}_{-j}^\star\right)\geq\bar{C}_j\left(\boldsymbol{p}_j,\boldsymbol{p}_{-j}^\star\right),\quad\forall\boldsymbol{p}_j\in\bar{\mathcal{P}}_j\left(\boldsymbol{p}_{-j}^\star\right),\quad\forall j\in\mathcal{J}, \tag{17}$$

which indicates that the robust secrecy rate can not be further improved by deviating from current power allocation. For the equilibrium, we need to investigate the properties of the robust secrecy rate. To this end, we first consider the secrecy rate in (4). As we can see, the secrecy rate is a concave function of its own power allocation strategy. Then, revisit the optimization in (10) defining the robust secrecy rate, we can deduce that robust secrecy rate of SUE is also concave with respect to its own secrecy rate, because the concavity is preserved through minimization operation [33]. (The proof for concavity of the secrecy rate and robust secrecy rate is sketched in App. A.) As $\bar{C}_j$ is concave with respect to $\boldsymbol{p}_j$, then the individual optimality in (17) can be equivalently written as

$$\left(\boldsymbol{p}_j-\boldsymbol{p}_j^\star\right)^T\bar{\boldsymbol{F}}_j\left(\boldsymbol{p}_j^\star,\boldsymbol{p}_{-j}^\star\right)\geq 0,\quad\forall\boldsymbol{p}_j\in\bar{\mathcal{P}}_j\left(\boldsymbol{p}_{-j}^\star\right), \tag{18}$$

where $\bar{\boldsymbol{F}}_j\left(\boldsymbol{p}_j,\boldsymbol{p}_{-j}\right)=-\nabla_{\boldsymbol{p}_j}\bar{C}_j\left(\boldsymbol{p}_j,\boldsymbol{p}_{-j}\right)$ and is the negative gradient of the utility function.

Recall the knowledge of VI theories, we can see that the equation in (18) appears in the form of a quasi-VI (QVI) problem [34], denoted as $\mathsf{QVI}_j\left(\bar{\mathcal{P}}_j,\bar{\boldsymbol{F}}_j\right)$. The terminology "quasi" addresses the fact that the strategy space of one SBS is a function of the strategies of other SBSs (similar to "general" in GRNEP). Then, by concatenating the problem of all SBSs in the network, a QVI problem covers all SBSs is arrived, denoted by $\mathsf{QVI}\left(\bar{\mathcal{P}},\bar{\boldsymbol{F}}\right)$ and specified as

$$\left(\boldsymbol{p}-\boldsymbol{p}^\star\right)^T\bar{\boldsymbol{F}}\left(\boldsymbol{p}^\star\right)\geq 0,\quad\forall\boldsymbol{p}\in\bar{\mathcal{P}}\left(\boldsymbol{p}^\star\right), \tag{19}$$

where $\bar{\mathcal{P}}=\prod_{j\in\mathcal{J}}\bar{\mathcal{P}}_j$ and $\bar{\boldsymbol{F}}=\left[\bar{\boldsymbol{F}}_j\right]_{j\in\mathcal{J}}$.

Based on the preceding discussions, we have reformulated the original GRNEP in (16) as a QVI problem in (19). This reformulation allows us to leverage the VI theories to assist the analysis, since directly tackling the GRNEP can be quite involved. For the reformulation, we have the following lemma.

Lemma 1: The GRNEP in (16) and QVI in (19) are equivalent in the sense that the strategy profile $\boldsymbol{p}^\star$ is an equilibrium to the GRNEP if and only if it is a solution to the QVI.

Proof: Based on previous discussions, we can see that the GRNEP and QVI share the identical SBS-specified first-order optimality condition as given in (18), the equivalence is then readily proved. ∎

Given the equivalence between the GRNEP and QVI, we now leverage the VI theories to assist the analysis of the equilibrium. For the QVI, we first tackle its feasible region. With simple mathematical manipulation, we have

$$\begin{aligned}\bar{\mathcal{P}}&=\prod_{j\in\mathcal{J}}\bar{\mathcal{P}}_j\left(\boldsymbol{p}_{-j}\right)=\prod_{j\in\mathcal{J}}\left(\mathcal{P}_j\cap\tilde{\mathcal{P}}_j\left(\boldsymbol{p}_{-j}\right)\right)\\&=\prod_{j\in\mathcal{J}}\mathcal{P}_j\bigcap\prod_{j\in\mathcal{J}}\tilde{\mathcal{P}}_j\left(\boldsymbol{p}_{-j}\right)\\&=\prod_{j\in\mathcal{J}}\mathcal{P}_j\bigcap\tilde{\mathcal{P}}.\end{aligned} \tag{20}$$

Revisit $\zeta_n(\boldsymbol{p})$ in (11) that defines $\tilde{\mathcal{P}}$ in (12), we can see that $\zeta_n(\boldsymbol{p})$ maximizes a linear function of $\boldsymbol{p}$, where convexity (linearity implying convexity) is preserved through maximization operation. Therefore, $\zeta_n(\boldsymbol{p})$ is a convex function, and thus $\tilde{\mathcal{P}}$ is a convex set. As $\prod_{j\in\mathcal{J}}\mathcal{P}_j$ is obviously a convex set, we derive that $\bar{\mathcal{P}}$ in (20) is convex. On the other hand, for the operator $\bar{\boldsymbol{F}}$ in the QVI, we consider the robust secrecy defined in (10). Based on the discussions in App. A, we derive that the robust secrecy rate can be written as

$$\bar{C}_j = \sum_{k\in\mathcal{K}} \log \frac{1+p_j(k)\,a_j(k)}{1+p_j(k)\,b_j(k)}, \tag{21}$$

where

$$a_j(k) = \frac{h_{jj}(k)}{\sum\limits_{i\in\mathcal{J}\setminus\{j\}\cup\{0\}} p_j(k)\,h_{ij}(k)+\sigma_0^2}, \tag{22}$$

and

$$b_j(k) = \frac{\hat{g}_{jj}(k)+\sqrt{\epsilon_j(k)}}{\sum\limits_{i\in\mathcal{J}\setminus\{j\}\cup\{0\}} p_i(k)\,\hat{g}_{ij}(k)-\sqrt{\varepsilon_j(k)\sum\limits_{i\in\mathcal{J}\setminus\{j\}\cup\{0\}} p_i^2(k)+\sigma_0^2}}. \tag{23}$$

From (21), we can see that $\bar{C}_j$ is a continuous and differential function with respect to $\boldsymbol{p}_j$, and thus $\bar{\boldsymbol{F}}_j\left(\boldsymbol{p}_j,\boldsymbol{p}_{-j}\right)$, as the negative of its gradient, is a continuous function. Therefore, we have the following conclusion.

Theorem 1: The solution to the QVI problem in (19) always exists, and thus equivalently, the equilibrium to the GRNEP in (16) always exists.

Proof: Based on the previous discussions, we can see that for QVI $\left(\bar{\mathcal{P}},\bar{\boldsymbol{F}}\right)$, the feasible region, i.e., $\bar{\mathcal{P}}$, can be regarded as fixed with respect to $\boldsymbol{p}$. In this regard, the QVI $\left(\bar{\mathcal{P}},\bar{\boldsymbol{F}}\right)$ reduces to a VI problem, denoted as VI $\left(\bar{\mathcal{P}},\bar{\boldsymbol{F}}\right)$. Also, we have proved that $\bar{\mathcal{P}}$ is compact and convex and $\bar{\boldsymbol{F}}$ is continuous. Then based on VI theories, we know that the problem VI $\left(\bar{\mathcal{P}},\bar{\boldsymbol{F}}\right)$ always admits a solution. Further based on equivalence between the QVI and GRNEP in Lemma 1, we know that the equilibrium of the GRNEP always exists. ∎

As we can see, we tackle the QVI from the perspective of a VI problem. For the problem of QVI $\left(\bar{\mathcal{P}},\bar{\boldsymbol{F}}\right)$, the "quasi" originates from $\bar{\mathcal{P}}=\prod_{j\in\mathcal{J}}\bar{\mathcal{P}}_j\left(\boldsymbol{p}_{-j}\right)$, indicating a parameterized feasible region. While for VI $\left(\bar{\mathcal{P}},\bar{\boldsymbol{F}}\right)$, $\bar{\mathcal{P}}$ is considered fixed in the form of $\prod_{j\in\mathcal{J}}\mathcal{P}_j\bigcap\bar{\mathcal{P}}$. Generally, a VI problem can be more conveniently tackled than a QVI problem. Therefore, this transformation facilitates the investigation on the existence and uniqueness of the equilibrium.

With Theorem 1 confirming the existence of the equilibrium, we further analyze the uniqueness of the equilibrium and reach the following conclusion.

Theorem 2: The equilibrium of the GRNEP in (16) is unique on condition that $\Upsilon=[\gamma_{ij}]_{i\in\mathcal{J},j\in\mathcal{J}}$ is positive definite, with

$$\gamma_{ij} = \begin{cases} \lambda_{\min}\left(-\nabla^2_{\boldsymbol{p}_j}\bar{C}_j\left(\boldsymbol{p}_j;\boldsymbol{p}_{-j}\right)\right) & \text{if } i=j,\\ -\max\limits_{\boldsymbol{p}}\left\|\nabla^2_{\boldsymbol{p}_j\boldsymbol{p}_i}\bar{C}_j(\boldsymbol{p})\right\| & \text{else}, \end{cases} \tag{24}$$

where $\lambda_{\min}(\cdot)$ denotes the minimum eigenvalue of a matrix.

Proof: Please refer to App. B. ∎

Theorem 2 can be interpreted as follows. The diagonal elements of Υ refer to the local operations of the SBS, while the non-diagonal ones concerns the mutual influence among the SBSs. As such, the positive definiteness of Υ requires that the transmissions at one SBS need to have sufficiently small impacts on other SBSs. Intuitively, under such a condition, the distributed secrecy competition among SBSs tends to approximate the independent optimization within each individual small cell, and thus is more likely to result in the unique equilibrium. Also, note that although the condition in Theorem 2 appears relatively strong, it is a sufficient condition rather than necessary. As we can see in the simulation results, the unique equilibrium can also be observed in rather mild conditions.

V. Problem Decomposition and Algorithm

We in preceding discussions have analyzed the properties of the equilibrium of GRNEP. In this section, we propose distributed algorithms to solve for the equilibrium. In particular, we introduce the pricing mechanism to decompose the GRNEP as a NCP with a priced NEP, through which the pricing coefficients and power allocation strategies are obtained, respectively, along with detailed algorithm designs.

A. Problem Decomposition

For the GRNEP in (16), we have analyzed that one of the main difficulties is that the SBSs compete for their own secrecy rate maximization while the interference constraints imposed by MUEs affect all SBSs concurrently. Targeting at this issue, we introduce the pricing mechanism to tackle the aggregate interference constraints. In particular, we introduce the pricing coefficient $\boldsymbol{\kappa}=[\kappa_n]_{n\in\mathcal{N}}$ and define

$$\mathcal{C}_j = \bar{C}_j - \boldsymbol{\kappa}\cdot\boldsymbol{\zeta}, \quad \forall j\in\mathcal{J}, \tag{25}$$

where $\boldsymbol{\zeta}=[\zeta_n]_{n\in\mathcal{N}}$ and $\boldsymbol{\kappa}$ satisfies

$$0\le\boldsymbol{\kappa}\perp\boldsymbol{\zeta}\le 0, \tag{26}$$

with $0\le\boldsymbol{x}\perp\boldsymbol{y}\le 0$ indicating $\boldsymbol{x}\ge 0$, $\boldsymbol{y}\le 0$, and $\boldsymbol{x}^T\boldsymbol{y}=0$. As we can see, $\mathcal{C}_j$ is a interference-priced version of robust secrecy rate $\bar{C}_j$. In this regard, the aggregate interference constraints are now tackled at individual SBSs as part of the utility function. Meanwhile, the condition in (26) guarantees that the aggregate interference constraints are always satisfied.

Since the shared interference constraint is now addressed at each SBS, the original SBS-specified problem in (15) becomes

$$\max_{\boldsymbol{p}_j}\ \mathcal{C}_j \tag{27a}$$

$$\text{s. t. } \boldsymbol{p}_j\in\mathcal{P}_j. \tag{27b}$$

Compare the problems in (15) and (27), we can see that the former has the robust secrecy rate as objective and the feasible region is a function of the strategies of other SBSs, while the latter has the interference-priced robust secrecy as the objective and the feasible region becomes independent.

From the problem in (27) to the problem in (15), the difficulty is much relieved, as the feasible region in (15b) in the form of point-to-set mapping can be quite tricky to dealt with. Then, from a networked scope, the problems of all SBSs constitute a $\boldsymbol{\kappa}$-parameterized NEP, given as

$$\mathfrak{G}_{\boldsymbol{\kappa}} = \left\{\mathcal{J}, \{\mathcal{P}_j\}_{j\in\mathcal{J}}, \{\mathcal{C}_j\}_{j\in\mathcal{J}}\right\}. \tag{28}$$

Note the problem in (28) is a generic NEP, as the strategy space of each SBS is independent. The SBSs compete to maximize the priced robust secrecy rate to determine their transmission strategies. As the NEP is parameterized by the price coefficient $\boldsymbol{\kappa}$, its equilibrium is also price-parameterized. Let us denote the equilibrium of (28) as $\boldsymbol{p}^\star(\boldsymbol{\kappa}) = \left[\boldsymbol{p}_j^\star(\boldsymbol{\kappa})\right]_{j\in\mathcal{J}}$, then the interference condition in (26) at the equilibrium can be written as

$$\mathbf{0} \le \boldsymbol{\kappa} \perp \boldsymbol{\zeta}\left(\boldsymbol{p}^\star(\boldsymbol{\kappa})\right) \le \mathbf{0}. \tag{29}$$

Based on the terminologies in VI theories [34], we know that the problem in the form of (29) is noted a NCP, for which we denote the problem in (29) as $\mathsf{NCP}(\boldsymbol{\kappa})$.

For the decomposition, we have the following conclusion.

Theorem 3: The GRNEP $\mathfrak{G}$ (or equivalently $\mathsf{QVI}(\bar{\mathcal{P}}, \bar{\boldsymbol{F}})$) and the decomposed NCP $\mathsf{NCP}(\boldsymbol{\kappa})$ with priced NEP $\mathfrak{G}_{\boldsymbol{\kappa}}$ are equivalent in the following sense:

- *Suppose $\boldsymbol{p}^{\mathsf{v}}$ is the equilibrium of $\mathfrak{G}$, then there exists $\boldsymbol{\kappa}^{\mathsf{v}}$ as the multiplier associated with the aggregate interference constraint in (12) such that $\boldsymbol{p}^{\mathsf{v}}$ is also the equilibrium of $\mathfrak{G}_{\boldsymbol{\kappa}}$ and $\boldsymbol{\kappa}^{\mathsf{v}}$ is the solution to $\mathsf{NCP}(\boldsymbol{\kappa})$;*
- *Suppose $\boldsymbol{\kappa}^{\mathsf{e}}$ solves the $\mathsf{NCP}(\boldsymbol{\kappa})$ with $\boldsymbol{p}^{\mathsf{e}}(\boldsymbol{\kappa}^{\mathsf{e}})$ being the equilibrium of $\mathfrak{G}_{\boldsymbol{\kappa}}$, then $\boldsymbol{p}^{\mathsf{e}}(\boldsymbol{\kappa}^{\mathsf{e}})$ is also the equilibrium of $\mathfrak{G}$.*

Proof: Please refer to App. C. ■

Thanks to such an equivalence, we can solve GRNEP through the NCP with a priced NEP, which alleviates the difficulties to directly tackle the original problem. From the NCP with a priced NEP, we can obtain the price and further obtain the equilibrium so as to determine the transmission strategies for each SBS. In this regard, the NCP acts as the outer problem while the priced NEP is the inner problem, where the inner problem is parameterized by the solution of outer problem and the outer problem exploits the equilibrium of the inner problem. We will then endeavor to tackle the two problems, respectively, along with the algorithm designs.

B. Algorithm Design

We first investigate the priced NEP as the inner problem to achieve the priced equilibrium, with given price coefficient. For NEP $\mathfrak{G}_{\boldsymbol{\kappa}}$, its equilibrium $\boldsymbol{p}^\star(\boldsymbol{\kappa})$ satisfies the following condition[3]

$$\mathcal{C}_j\left(\boldsymbol{p}_j^\star, \boldsymbol{p}_{-j}^\star\right) \ge \mathcal{C}_j\left(\boldsymbol{p}_j, \boldsymbol{p}_{-j}^\star\right), \quad \forall \boldsymbol{p}_j \in \mathcal{P}_j, \quad \forall j \in \mathcal{J}, \tag{30}$$

which is a strategy profile that no SBS will unilaterally deviate from. Before solving for the equilibrium, we first analyze its properties, including its existence and uniqueness, and have the following conclusions.

Theorem 4: The NEP $\mathfrak{G}_{\boldsymbol{\kappa}}$ always admits the equilibrium, regardless of the price coefficient $\boldsymbol{\kappa}$.

Proof: For $\mathfrak{G}_{\boldsymbol{\kappa}}$ as a generic NEP, we can see that the strategy space of each SBS is compact and convex. Meanwhile, for utility function $\mathcal{C}_j$, we know from previous discussion that $\bar{C}_j$ is concave and ζ_n is convex with respect to $\boldsymbol{p}_j$, which implies that $\mathcal{C}_j$ is concave with respect to its own strategy $\boldsymbol{p}_j$. Therefore, NEP $\mathfrak{G}_{\boldsymbol{\kappa}}$ is a concave problem. According to the properties of concave game allowing an equilibrium [35], we know that the equilibrium always exists for NEP $\mathfrak{G}_{\boldsymbol{\kappa}}$. ■

Theorem 5: Given the condition in Theorem 2, i.e., Υ being positive definite, NEP $\mathfrak{G}_{\boldsymbol{\kappa}}$ admits a unique equilibrium.

Proof: Please refer to App. D. ■

Therefore, the equilibrium always exists and the positive definiteness of Υ guarantees the uniqueness of the equilibrium $\mathfrak{G}_{\boldsymbol{\kappa}}$. As a further note, the physical interpretation of Theorem 5 can be similarly elaborated as that of Theorem 2, as they share the same sufficient condition for unique equilibrium. Both the GRNEP and NEP aim at robust secrecy maximization, while the shared interference constraint is tackled through parameterized feasible region of the GRNEP, while as part of the utility function in NEP. The positive definiteness of Υ implies insignificant mutual influence among the SBSs, which ensures the unique equilibrium physically, regardless of specific mathematical formulations.

With the properties of the equilibrium of $\mathfrak{G}_{\boldsymbol{\kappa}}$ being explored, we then attempt to obtain the equilibrium. For $\mathfrak{G}_{\boldsymbol{\kappa}}$ as a generic NEP, we know that the individual optimality is given as

$$\boldsymbol{p}_j^\star = \mathsf{BR}_j\left(\boldsymbol{p}_{-j}\right) = \arg\max_{\boldsymbol{p}_j\in\mathcal{P}_j} \mathcal{C}_j\left(\boldsymbol{p}_j, \boldsymbol{p}_{-j}\right), \quad \forall j \in \mathcal{J}, \tag{31}$$

where BR_j denotes the best-response function of SBS-j. Then, the equilibrium condition can be rewritten as

$$\boldsymbol{p}_j^\star = \mathsf{BR}_j\left(\boldsymbol{p}_{-j}^\star\right), \quad \forall j \in \mathcal{J}. \tag{32}$$

Further, by considering the best response for all SBSs simultaneously, we can organize the equilibrium condition as $\boldsymbol{p}^\star = \mathsf{BR}(\boldsymbol{p}^\star)$, where BR is the vector function to concatenate the best-response functions of all SBSs. Therefore, the equilibrium is a fixed point of the best-response function.

Now we consider the best response of a single SBS, with the strategies of other SBSs being fixed. By analyzing the interference price function in (11) along with the uncertainties in (9), we can derive the explicit expression of the priced robust secrecy rate and specify the individual optimality of the SBS in (27) as

$$\begin{aligned}\max_{\boldsymbol{p}_j}\ \mathcal{C}_j &= \sum_{k\in\mathcal{K}} \log\frac{1+p_j(k)\,a_j(k)}{1+p_j(k)\,b_j(k)} \\ &\quad - \sum_{n\in\mathcal{N}} \kappa_n \left(\sum_{k\in\mathcal{K}}\sum_{j\in\mathcal{J}} p_j(k)\,\hat{h}_{jn}(k)\right. \qquad \text{(33a)} \\ &\quad \left. + \sqrt{e_n \sum_{k\in\mathcal{K}}\sum_{j\in\mathcal{J}} p_j^2(k) - I_n^{\text{th}}}\right) \\ \text{s. t. } & 0 \le p_j(k) \le p_j^{\text{msk}}, \quad \forall k \in \mathcal{K}, \qquad \text{(33b)}\end{aligned}$$

[3]For the rest discussions in this section, without causing ambiguity, we will omit the parameter $\boldsymbol{\kappa}$ when discussing the equilibrium $\boldsymbol{p}^\star(\boldsymbol{\kappa})$ for notation simplicity.

$$\sum_{k\in\mathcal{K}} p_j(k) \le p_j^{\max}. \tag{33c}$$

As we have shown before, the robust secrecy rate is concave while the price term is convex, then the objective function in (33a), as the difference between a concave function and a convex function, is concave. Also, the feasible region is evidently a convex set, the problem in (33) can be conveniently solved through Lagrange multiplier method. As solving (33) follows a standard routine, here we omit the details given the space limitation.

Now that we have solved the individual optimal for each SBS, the network equilibrium can be then obtained through the best-response iterations among the SBSs, as inspired by the fixed-point nature of the equilibrium. The algorithm is specified in the following table, where t specifies the iterations and σ is a predefined threshold to terminate the algorithm.

Algorithm 1 Best-Response Iteration for Priced Equilibrium

Initialization: Specify the price coefficient $\boldsymbol{\kappa}$; $t \leftarrow 0$, randomly allocate the power for all SBSs as $\boldsymbol{p}(t)$, with the individual power constraint satisfied, i.e., $\boldsymbol{p}_j(t) \in \mathcal{P}_j, \forall j \in \mathcal{J}$;
repeat
  $t \leftarrow t+1$;
  for *all SBS-*$j \in \mathcal{J}$ **do**
    Calculate $a_j(l)$ and $b_j(k)$ for all the channels and specify the priced robust secrecy rate in (33a) based on the power strategies of others $\boldsymbol{p}_{-j}$ and price $\boldsymbol{\kappa}$;
    Update the power strategy for SBS-j as
    $$\boldsymbol{p}_j(t) = \mathsf{BR}_j\left(\boldsymbol{p}_{-j}(t-1)\right)$$
    by solving the optimization in (33);
until $\|\boldsymbol{p}(t) - \boldsymbol{p}(t-1)\| / \|\boldsymbol{p}(t-1)\| < \sigma$;

Then we consider the outer NCP to determine the price. For the NCP in the form of (29), the price is updated with determined equilibrium of the inner priced NEP. In this regard, we can adopt the standard variable-step projection algorithm to obtain the price, as detailed in Alg. 2, where τ specifies the iterations and ς is a predefined threshold to claim the termination of the algorithm.

For the provided algorithms, we have the following conclusion.

Theorem 6: Given the condition in Theorem 2, i.e., Υ being positive definite, Alg. 1 converges to the unique equilibrium of the priced NEP. Furthermore, with positive definite Υ and step size in Alg. 2 satisfying $0 < \inf \varrho \le \sup \varrho < \frac{2c_{sm}}{(\max_{\boldsymbol{p}} \|\nabla_{\boldsymbol{p}} \boldsymbol{\zeta}(\boldsymbol{p})\|)^2}$, Alg. 2 is guaranteed to converge, where c_{sm} is the strongly monotone constant associated with $\bar{\boldsymbol{F}}$.

Proof: Please refer to App. E. ∎

As shown in App. E, the convergence of Alg. 1 is proved based on contraction mapping, and thus features a geometric convergence rate. As for Alg. 2, the convergence rate depends on the specified choice of step size, for which we provide numerical observations in later discussions. As the proposed

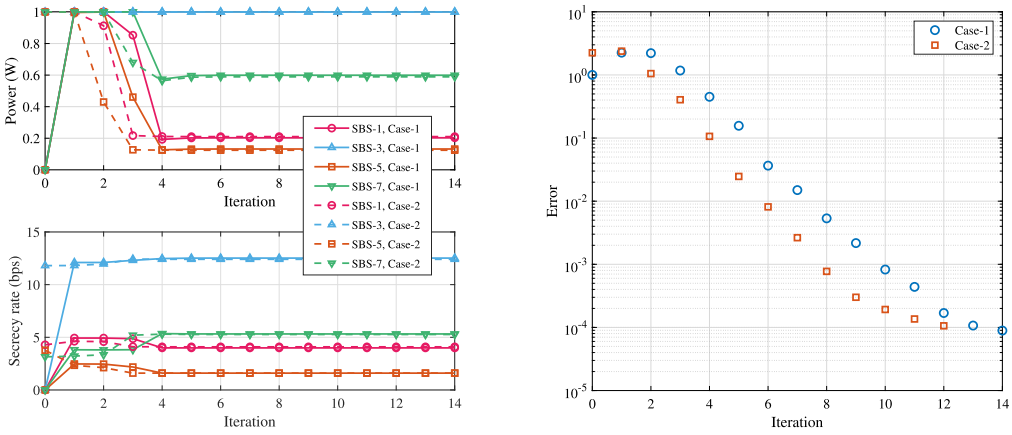
Algorithm 2 Projection Algorithm for Price

Initialization: Specify a sufficiently small step parameter $\varrho > 0$; $\tau \leftarrow 0$ and randomly choose a price coefficient $\boldsymbol{\kappa}(\tau)$;
repeat
  $\tau \leftarrow \tau + 1$;
  Calculate the equilibrium of the priced NEP $\mathfrak{G}_{\boldsymbol{\kappa}(\tau-1)}$ as $\boldsymbol{p}^\star(\boldsymbol{\kappa}(\tau-1))$;
  Update the price coefficient as
  $$\boldsymbol{\kappa}(\tau) = \left[\boldsymbol{\kappa}(\tau-1) + \varrho\boldsymbol{\zeta}\left(\boldsymbol{p}^\star(\boldsymbol{\kappa}(\tau-1))\right)\right]^+.$$
until $\|\boldsymbol{\kappa}(\tau) - \boldsymbol{\kappa}(\tau-1)\| / \|\boldsymbol{\kappa}(\tau-1)\| < \varsigma$;

algorithm are iterative, we denote the number of iterations needed for Alg. 1 and Alg. 2 as $R^{(\text{in})}$ and $R^{(\text{out})}$, respectively, and then analyze the complexity. As we can see, the algorithm implementation consists of triple loops, i.e., obtaining the best response at the each SBS by solving (33), best-response iterations among SBSs, and price updates. In particular, to solve problem in (33) with Lagrange multiplier method, it concerns the power allocation over K channels and one multiplier. For the power allocation, as the power at different channels affects each other though the uncertainty-related term, a fix-point iteration is required, for which the required times of iterations is denoted by $T^{(\text{pwr})}$. Also, the multiplier needs $T^{(\text{mltp})}$ iterations by the subgradient descent. Therefore, the per-iteration per-SBS computational complexity is $\mathcal{O}\left(T^{(\text{pwr})}T^{(\text{mltp})}K\right)$. Further consider the best-response iterations among the SBSs to reach the equilibrium and the price updates, the overall computational complexity at each SBS is $\mathcal{O}\left(R^{(\text{out})}R^{(\text{in})}T^{(\text{pwr})}T^{(\text{mltp})}K\right)$. Meanwhile, the price updates are conducted at the MBS. Since the price updates only concern simple arithmetic calculations, the computation complexity is thus $\mathcal{O}\left(R^{(\text{out})}N\right)$.

We further investigate the communication overhead for the algorithm implementation, since each SBS needs external information to assist their decision makings. Revisiting the individual optimization in (33), we can see that besides the local information concerning the SUE and eavesdropper, the SBS needs to know the price coefficients, power strategies of other SBSs, and the interference channel state information. In particular, the price coefficients are updated at the MBS based on the interference measured by the MUEs. The individual power strategy is determined by the SBS and fed back to the MBS. For the interference channel state information, they are measured by the MUEs and reported to the MBS. During the algorithm implementation, the MBS collects the information and broadcasts to the small cells to facilitate their strategy updates.

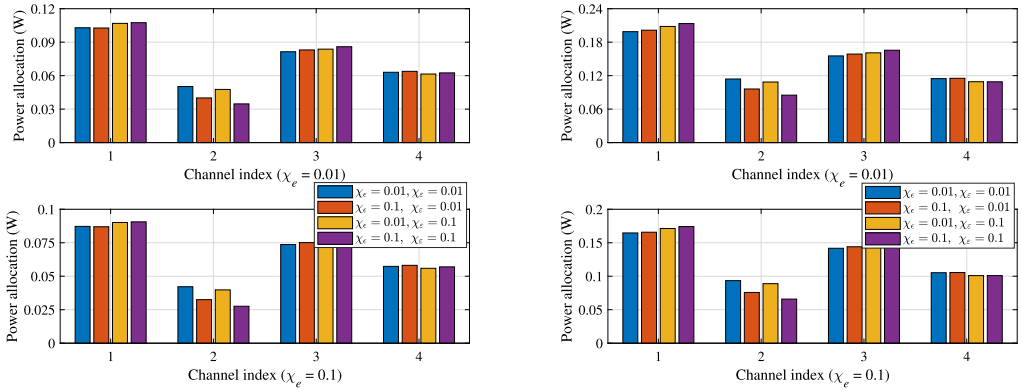
In the preceding discussions, we have addressed the implementation issues, including the convergence, complexity, and communication overhead. As we can see, the computation burden are distributed among all participants in the network, where they need a mild level of communication overhead for information exchanges. Moreover, as we can see in the simulation results, the convergence is often achieved within



(a) Convergence from different initial states

(b) Error during iteration

Fig. 2. Demo of convergence.



(a) Interference constraint $I^{\text{th}} = 5 \times 10^{-12}$ W

(b) Interference constraint $I^{\text{th}} = 10 \times 10^{-12}$ W

Fig. 3. Power allocation of a single SBS with respect to uncertainties and interference constraint.

a few iterations. Therefore, the proposed schemes can be efficiently implemented in practice.

VI. Simulation Results

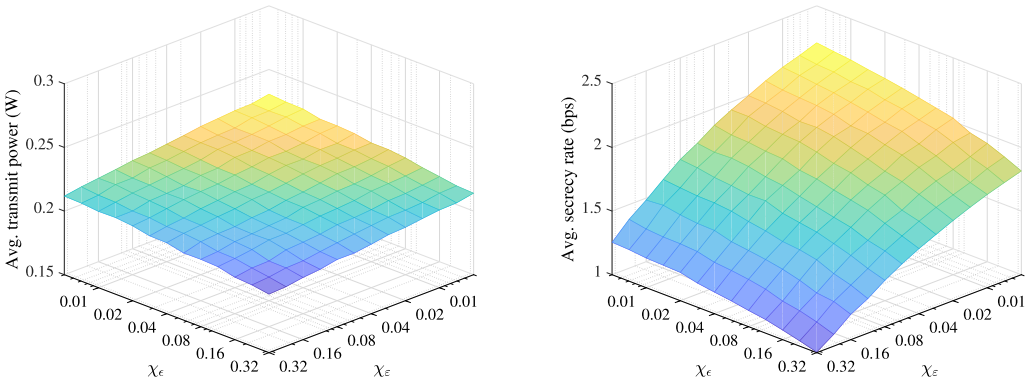
In this section, we present the simulation results to show the effectiveness of our proposals and verify our theoretical findings. We will illustrate the behavior of individual SBS as well as the networked performance. In particular, we consider a square area with one macro-base station located at the origin and a MUE, along with a certain number of small cells. There are 4 channels available to all users, each channel is of unit bandwidth. The wireless transmissions experience path loss, shadowing, Rayleigh fading, and affected by the background noise. For the uncertainties, we model them as a fraction of their corresponding estimate, i.e., $\epsilon_j(k) = \chi_\epsilon |\hat{g}_{jj}(k)|$, $\varepsilon_j(k) = \chi_\varepsilon \left\| [\hat{g}_{ij}(k)]_{i \in \mathcal{J} \setminus \{j\} \cup \{0\}} \right\|$, and $e_n = \chi_e \left\| \left[\hat{h}_{jn}(k) \right]_{j \in \mathcal{J}, k \in \mathcal{K}} \right\|$, and consider the scalar coefficients χ_ϵ, χ_ε, and χ_e numerically. The listed simulation parameters in Table I are used as default until otherwise stated.

TABLE I
Simulation Parameters

Parameter	Value
Area size	1000 m × 1000 m
Number of channels	4
Transmitter-receiver distance	Uniformly in [80, 120] m
Transmitter-eavesdropper distance	Uniformly in [100, 140] m
Maximum power	1 W
Spectral mask	0.5 W
Thermal noise power	−120 dBm
Interference threshold	−110 dBW
Path loss model	$127.1 + 37.6 \log_{10}(d[\text{km}])$ dB
Shadowing	Log-normal with std. 10 dB
Fading	Rayleigh flat fading

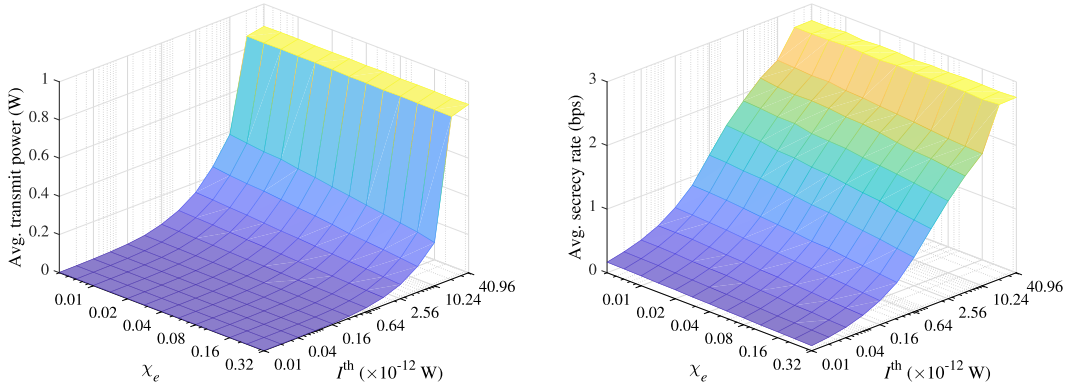
A. Convergence

For the proposed distributed schemes, we first verify the convergence. In Fig. 2, we consider a network with 8 small cells and iterations of the secrecy competition. In particular, in Fig. 2(a) we show two iterative processes with two different initial states. The solid lines correspond to the case all SBSs initiate with all-zero transmit power, and the dashed lines for the case that all SBSs begin with full-power transmissions with equally allocated power at each channel. The upper subfigure shows the sum power at each SBS, and lower subfigure for the secrecy rate. For a clear demonstration, only the SBSs labeled with odd numbers are shown. The



(a) Average transmit power. (b) Average secrecy rate.

Fig. 4. The average performance of SBSs with with respect to the uncertainties regarding the eavesdropper.



(a) Average transmit power. (b) Average secrecy rate.

Fig. 5. The average performance of SBSs with with respect to interference constraint and uncertainties of interference channels.

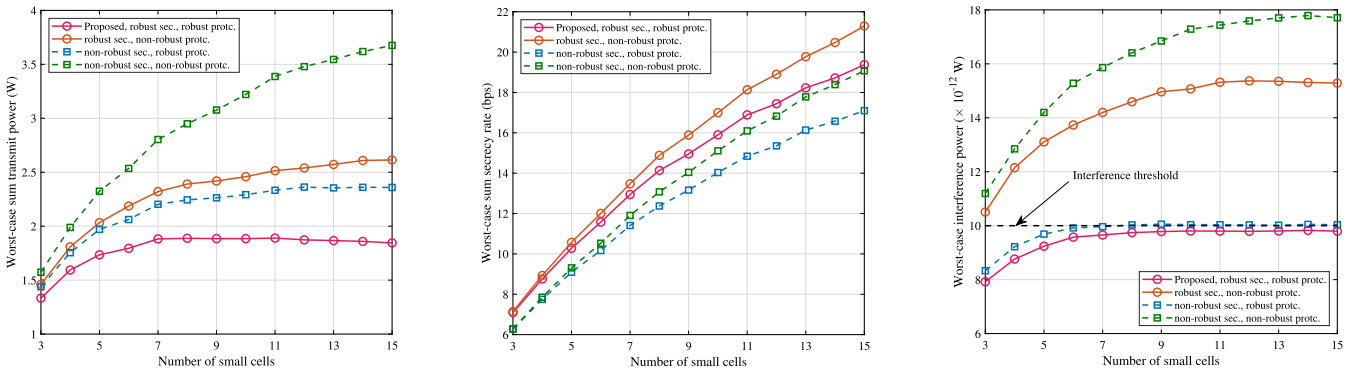
convergence can be rather fast to be achieved with dozens of iterations. Moreover, the two cases with different initial states results in the same convergence state, indicating a unique equilibrium. In Fig. 2(b), the error while iterating, defined as $\|\boldsymbol{p}(t) - \boldsymbol{p}^\star\| / \|\boldsymbol{p}^\star\|$, is shown for the two cases, which quantitatively verifies the convergence rate.

B. Performance of Single SBS

We consider the performance from the perspective of individual SBS and demonstrate how the uncertainties and interference constraints affect the transmission behavior of the SBS. First, we in Fig. 3 show the power allocation over different channels at one SBS in one realization of the secrecy competition. As we can see in Fig. 3(a), when we fix the interference constraint and the uncertainties on the interference channel, the SBS tends to allocate more power to the better-quality (the quality here is defined as the advantage of legitimate channel quality over wiretap channel) channels as the uncertainties regarding the eavesdropper becomes larger. In particular, we can infer that the quality of channel-1 and channel-3 are generally better than that of channel-2 and channel-4, since the former two are allocated with higher power. Consequently, compared with the case of $\chi_\epsilon = \chi_\varepsilon = 0.01$ with smaller uncertainty, the SBS will allocate higher power in channel-1 and channel-3 (and thus lower power in channel-2 and channel-4) when in the case of $\chi_\epsilon = \chi_\varepsilon = 0.1$ with higher uncertainties. Similar phenomena can be observed in Fig. 3(b). Therefore, we know that when there exist higher uncertainties regarding the eavesdropper, the transmission behavior of the SBS becomes more conservative, as they tends to concentrate their power on the channels with better quality, while not willing to fully exploit the channel diversity.

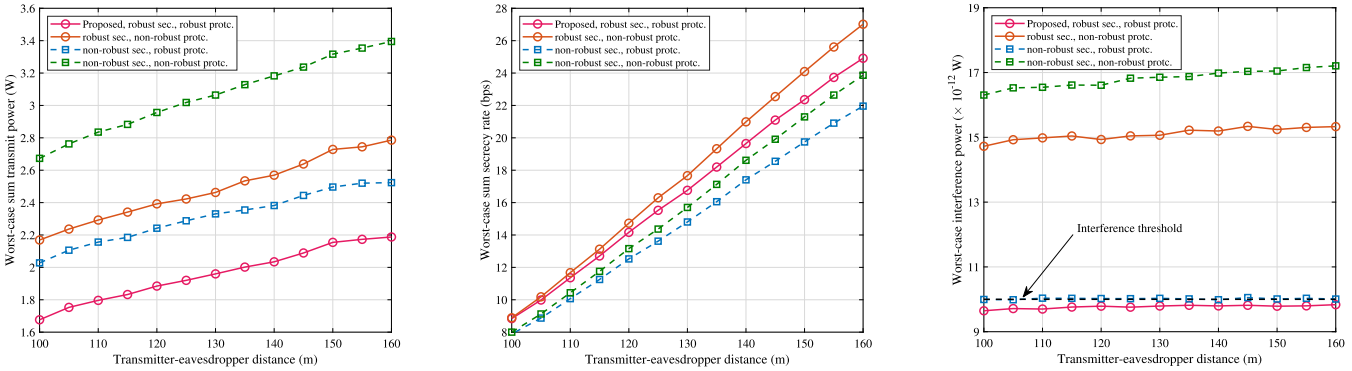
Then, we fix the uncertainties regarding the eavesdropper and consider the influence of the interference constraint. Compare the left subfigure and right subfigure in Fig. 3, we can see that when the interference constraint is more relaxed, the SBS is allowed with higher power budget. Meanwhile, compare the upper subfigure and lower subfigure, we can see that when the uncertainties regarding the interference channels are enlarged, the power allocation is also reduced so as to achieve robust protection for the MUEs.

Moreover, we consider how the uncertainties and interference constraint jointly affect the average performance of SBSs. The results are shown in Fig. 4, where the interference constraint and the coefficient of uncertainties regarding the



(a) Sum transmit power of SBSs. (b) Sum secrecy rate of SUEs. (c) Interference power at the MUE.

Fig. 6. Networked performance with respect to number of SBSs.



(a) Sum transmit power of SBSs. (b) Sum secrecy rate of SUEs. (c) Interference power at the MUE.

Fig. 7. Networked performance with respect to average distance between the legitimate transmitter and eavesdropper.

interference channel are fixed as $I^{\text{th}} = 5 \times 10^{-12}$ W and $\chi_e = 0.01$. As we can see from Fig. 4(a), the average transmit power of SBSs becomes smaller with increasing uncertainties regarding the eavesdropper. This is as expected as we have shown in Fig. 4(a) that the transmission behavior of SBS becomes conservative. However, we can see that the sum transmit power per SBS does not change significantly. In contrast, we can see in Fig. 4(b), the change of average secrecy rate is much more evident. Also as expected, with higher uncertainties, the secrecy rate becomes lower. From Fig. 4(a) showing relatively slight change of sum power per SBS and Fig. 4(b) showing significant change of the secrecy rate, we can see that the different power allocation over the channels significantly affects the security performance.

Also, we evaluate the average performance of SBSs with respect to the interference constraint and the uncertainties regarding the interference channels. The results are provided in Fig. 5, where we fix the uncertainties regarding the eavesdroppers as $\chi_\epsilon = 0.01$ and $\chi_\varepsilon = 0.01$. Generally, we can see that lower interference threshold and higher uncertainties therein result in lower transmit power and secrecy rate of SBSs. Specifically, we can see that when the interference threshold is sufficiently large, i.e., $I^{\text{th}} = 20 \times 10^{-12}$ W in this case, the interference constraint is no longer active. Note ideally in this case, the SBSs shall adopt full-power transmissions, yet due to the competition among the SBSs, the actual transmit power is lower than upper bound. Moreover, we can see in Fig. 5(a), the transmit power along with the interference threshold decreases exponentially, while in Fig. 5(b), the secrecy rate decreases linearly as the interference threshold decreases exponentially. As such, we can see that the power optimization over different channels can compensate the reduced resources.

C. Networked Performance

Besides the individual performance, we also demonstrate the overall performance of the network. We evaluate the performance with respect to different number of small cells and the average distance between the transmitter and eavesdropper. For the results, we assume the uncertainty coefficients as $\chi_\epsilon = \chi_\varepsilon = \chi_e = 0.1$ and interference threshold as $I^{\text{th}} = 10 \times 10^{-12}$ W. As compared with our proposal aiming at robust secrecy for SUEs with robust protection for MUEs, we consider the cases including, robust SUE security with non-robust MUE protection, non-robust SUE secrecy with robust MUE protection, and non-robust SUE secrecy with non-robust MUE protection. We evaluate the performance in terms of sum transmit power, secrecy rate, and interference power at the MUE under the worst-case scenarios.

In Fig. 6, we show the network performance with different numbers of small cells. In Fig. 6(a), generally, the sum power increases with more small cells. In particular, the transmission behavior is more conservative under robust

designs, as suggested by previous results, and thus induces lower transmit power as compared with non-robust schemes. Evidently, the transmit power can be significantly higher if we do not consider robust protection for the MUE. In Fig. 6(b), we can see that, as compared with schemes of non-robust secrecy, the schemes with robust secrecy achieves better security provisioning under the worst case. Revisit the results in Fig. 6(a), we can see that although the non-robust schemes utilize more power, the achieved secrecy rate is lower, this is mainly due to the mismatch between the non-robust power allocation and worst-case scenarios. Moreover, we can see that, as expected, the scheme without robust protection for MUEs achieves higher secrecy rate as shown in Fig. 6(b), but this is at the price of significant interference constraint violation as shown in Fig. 6(c). Meanwhile, we can see in Fig. 6(c) that interference constraint is always satisfied under our proposal with robust MUE protection.

In Fig. 7, we show the networked performance considering different distance between the legitimate transmitter and eavesdropper, where we consider the cases with 8 SBSs. Generally, we can see that when the eavesdropper locates farther away, the transmit power as well as the secrecy rate becomes higher. In particular, in Fig. 7(a), we can see, similarly, the transmission behavior becomes more aggressive with non-robust considerations and results in higher power. In Figs. 7(b) and 7(c), we can see that the our proposal with robust secrecy achieves better security performance as compared with non-robust designs, while strictly satisfying the interference constraints.

VII. Conclusion

In this article, we consider the secrecy competition in a small-cell network under interference constraints. We consider the information uncertainties regarding both the eavesdropper and the interference channels, and propose to maximize the robust secrecy rate with robust protection of MUEs. With numerical results, we show the transmission behavior of SBSs becomes more conservative with increasing uncertainties, as they tend to concentrate the power budget on the channels with better conditions rather than fully exploiting the resources. Also, with similar power budget, the power allocation has a prominent influence on the security performance. Moreover, we show that the uncertainties and interference constraint both affect the security performance in a negative manner, and our proposal effectively protects the security while strictly satisfying the interference constraint.

Appendix A
On the Robust Secrecy Rate

First, for the secrecy rate in (4), taking second-order derivative of the SUE's secrecy rate with respect to its own power allocation, we can see that $\frac{\partial^2 C_j}{\partial p_j^2(k)} \leq 0$ if non-negative secrecy rate can be achieved in channel-k and $\frac{\partial^2 C_j}{\partial p_j(k)\partial p_j(l)} = 0$. As such, we know that the secrecy rate is concave with respect to its own power allocation. Then, we show that the robust secrecy rate $\bar{C}_j\left(\boldsymbol{p}_j, \boldsymbol{p}_{-j}\right)$ is also a concave function with respect to its own power allocation $\boldsymbol{p}_j$. To this end, we assume $\boldsymbol{p}_j^{(1)}, \boldsymbol{p}_j^{(2)} \in \bar{\mathcal{P}}_j\left(\boldsymbol{p}_{-j}\right)$ and $\mu \in [0,1]$, then we have

$$\begin{aligned}
&\bar{C}_j\left(\mu \boldsymbol{p}_j^{(1)} + (1-\mu)\boldsymbol{p}_j^{(2)}, \boldsymbol{p}_{-j}\right) \\
&= \min_{\left[\tilde{\boldsymbol{g}}_j(k)\right]_{k\in\mathcal{K}}} C_j\left(\mu \boldsymbol{p}_j^{(1)} + (1-\mu)\boldsymbol{p}_j^{(2)}, \boldsymbol{p}_{-j}\right) \\
&\overset{(a)}{\geq} \min_{\left[\tilde{\boldsymbol{g}}_j(k)\right]_{k\in\mathcal{K}}} \mu C_j\left(\boldsymbol{p}_j^{(1)}, \boldsymbol{p}_{-j}\right) + (1-\mu) C_j\left(\boldsymbol{p}_j^{(2)}, \boldsymbol{p}_{-j}\right) \\
&\geq \mu \min_{\left[\tilde{\boldsymbol{g}}_j(k)\right]_{k\in\mathcal{K}}} C_j\left(\boldsymbol{p}_j^{(1)}, \boldsymbol{p}_{-j}\right) + (1-\mu) \\
&\quad \times \min_{\left[\tilde{\boldsymbol{g}}_j(k)\right]_{k\in\mathcal{K}}} C_j\left(\boldsymbol{p}_j^{(2)}, \boldsymbol{p}_{-j}\right) \\
&\geq \mu \bar{C}_j\left(\boldsymbol{p}_j^{(1)}, \boldsymbol{p}_{-j}\right) + (1-\mu)\bar{C}_j\left(\boldsymbol{p}_j^{(2)}, \boldsymbol{p}_{-j}\right),
\end{aligned} \tag{34}$$

where inequality (a) comes from the concavity of secrecy rate in (4) and this derivation confirms the concavity of robust secrecy rate.

As the uncertainties in (7) only concern the eavesdropper of in definition of robust secrecy rate, the problem in (10) can be then equivalently formulated as

$$\max_{\left[\tilde{\boldsymbol{g}}_j(k)\right]_{k\in\mathcal{K}}} \quad \mathsf{SINR}_j^{\text{eve}}(k) = \frac{p_j(k)\left(\hat{g}_{jj}(k) + \tilde{g}_{jj}(k)\right)}{\sum\limits_{i\in\mathcal{J}\setminus\{j\}\cup\{0\}} p_i(k)\left(\hat{g}_{ij}(k) + \tilde{g}_{ij}(k)\right) + \sigma_0^2} \tag{35a}$$

$$\text{s.t. } \left|\tilde{g}_{jj}(k)\right|^2 \leq \epsilon_j(k), \quad \forall k \in \mathcal{K}. \tag{35b}$$

$$\sum_{i\in\mathcal{J}\setminus\{j\}\cup\{0\}} \left|\tilde{g}_{ij}(k)\right|^2 \leq \varepsilon_j(k), \quad \forall k \in \mathcal{K}. \tag{35c}$$

As we can see, the optimization variables in (35) are in the numerator and denominator, respectively, which can be tackled independently and leads to the results in (21).

Appendix B
Proof of Theorem 2

Based on VI theories, a VI problem admits only a unique solution if it satisfies the strongly monotone property [34]. For our formulated VI problem $\mathsf{VI}\left(\bar{\mathcal{P}}, \bar{\boldsymbol{F}}\right)$, it satisfies the strongly monotone condition if there is a constant $c_{\text{sm}} > 0$ such that the following inequality holds

$$\begin{aligned}
&\left(\boldsymbol{p}^{(1)} - \boldsymbol{p}^{(2)}\right)^T \left(\bar{\boldsymbol{F}}\left(\boldsymbol{p}^{(1)}\right) - \bar{\boldsymbol{F}}\left(\boldsymbol{p}^{(2)}\right)\right) \\
&\qquad \geq c_{\text{sm}} \left\|\boldsymbol{p}^{(1)} - \boldsymbol{p}^{(2)}\right\|^2, \quad \forall \boldsymbol{p}^{(1)}, \ \boldsymbol{p}^{(2)} \in \mathcal{P},
\end{aligned} \tag{36}$$

or equivalently

$$\begin{aligned}
&\sum_{j\in\mathcal{J}} \left(\boldsymbol{p}_j^{(1)} - \boldsymbol{p}_j^{(2)}\right)^T \left(\bar{\boldsymbol{F}}_j\left(\boldsymbol{p}^{(1)}\right) - \bar{\boldsymbol{F}}_j\left(\boldsymbol{p}_j^{(2)}\right)\right) \\
&\qquad \geq c_{\text{sm}} \left\|\boldsymbol{p}^{(1)} - \boldsymbol{p}^{(2)}\right\|^2, \quad \forall \boldsymbol{p}^{(1)}, \ \boldsymbol{p}^{(2)} \in \mathcal{P}.
\end{aligned} \tag{37}$$

To investigate the condition for the above inequality to hold, we can derive that

$$\begin{aligned}
&\left(\boldsymbol{p}_j^{(1)}-\boldsymbol{p}_j^{(2)}\right)^T\left(\bar{\boldsymbol{F}}_j\left(\boldsymbol{p}^{(1)}\right)-\bar{\boldsymbol{F}}_j\left(\boldsymbol{p}_j^{(2)}\right)\right)\\
&=\left(\boldsymbol{p}_j^{(1)}-\boldsymbol{p}_j^{(2)}\right)^T\left[-\left(\nabla_{\boldsymbol{p}_j}\bar{C}_j\left(\boldsymbol{p}^{(1)}\right)-\nabla_{\boldsymbol{p}_j}\bar{C}_j\left(\boldsymbol{p}^{(2)}\right)\right)\right]\\
&\overset{(b)}{=}\left(\boldsymbol{p}_j^{(1)}-\boldsymbol{p}_j^{(2)}\right)^T\left[-\nabla^2_{\boldsymbol{p}_j,\boldsymbol{p}}\bar{C}_j\left(\boldsymbol{p}^{(\mu)}\right)\right]\left(\boldsymbol{p}^{(1)}-\boldsymbol{p}^{(2)}\right)\\
&=\left(\boldsymbol{p}_j^{(1)}-\boldsymbol{p}_j^{(2)}\right)^T\left[-\sum_{i\in\mathcal{J}}\nabla^2_{\boldsymbol{p}_j,\boldsymbol{p}_i}\bar{C}_j\left(\boldsymbol{p}^{(\mu)}\right)\right]\left(\boldsymbol{p}_i^{(1)}-\boldsymbol{p}_i^{(2)}\right)\\
&\geq\left(\boldsymbol{p}_j^{(1)}-\boldsymbol{p}_j^{(2)}\right)^T\left[-\nabla^2_{\boldsymbol{p}_j}\bar{C}_j\left(\boldsymbol{p}^{(\mu)}\right)\right]\left(\boldsymbol{p}_j^{(1)}-\boldsymbol{p}_j^{(2)}\right)\\
&\quad-\sum_{i\in\mathcal{J}\setminus\{j\}}\left\|\boldsymbol{p}_j^{(1)}-\boldsymbol{p}_j^{(2)}\right\|\left\|\nabla^2_{\boldsymbol{p}_j,\boldsymbol{p}_i}\bar{C}_j\left(\boldsymbol{p}^{(\mu)}\right)\right\|\left\|\boldsymbol{p}_i^{(1)}-\boldsymbol{p}_i^{(2)}\right\|,
\end{aligned}\tag{38}$$

where the equality (b) is derived based on differential mean value theorem and $\boldsymbol{p}^{\mu}=\mu\boldsymbol{p}^{(1)}+(1-\mu)\boldsymbol{p}^{(2)}$ for some $\mu\in[0,1]$. Based on (38) and the definition of Υ in (24), we further have

$$\begin{aligned}
&\sum_{j\in\mathcal{J}}\left(\boldsymbol{p}_j^{(1)}-\boldsymbol{p}_j^{(2)}\right)^T\left(\bar{\boldsymbol{F}}_j\left(\boldsymbol{p}^{(1)}\right)-\bar{\boldsymbol{F}}_j\left(\boldsymbol{p}_j^{(2)}\right)\right)\\
&\quad\geq\sum_{j\in\mathcal{J}}\gamma_{jj}\left\|\boldsymbol{p}_j^{(1)}-\boldsymbol{p}_j^{(2)}\right\|^2\\
&\qquad-\sum_{j\in\mathcal{J}}\sum_{i\in\mathcal{J}\setminus\{j\}}\gamma_{ij}\left\|\boldsymbol{p}_j^{(1)}-\boldsymbol{p}_j^{(2)}\right\|\left\|\boldsymbol{p}_i^{(1)}-\boldsymbol{p}_i^{(2)}\right\|\\
&\qquad=\left[\left\|\boldsymbol{p}_j^{(1)}-\boldsymbol{p}_j^{(2)}\right\|\right]^T_{j\in\mathcal{J}}\Upsilon\left[\left\|\boldsymbol{p}_j^{(1)}-\boldsymbol{p}_j^{(2)}\right\|\right]_{j\in\mathcal{J}}\\
&\qquad\geq\lambda_{\min}(\Upsilon)\left\|\boldsymbol{p}^{(1)}-\boldsymbol{p}^{(2)}\right\|^2.
\end{aligned}\tag{39}$$

Therefore, we can see that if Υ is positive definite, then the VI problem $\mathsf{VI}\left(\bar{\mathcal{P}},\bar{\boldsymbol{F}}\right)$ is strongly monotone with the constant $c_{\mathrm{sm}}=\lambda_{\min}(\Upsilon)$, which further guarantees the uniqueness of the solution. Due to the equivalence between the QVI and GRNEP as indicated in Lemma 1, we know that the condition suggests the unique equilibrium, which completes the proof for Theorem 2.

Appendix C
Proof of Theorem 3

To facilitate the proof, we first introduce the concepts of normal cone and subdifferential. In particular, for a n-dimensional set $\mathcal{X}$ and a vector $\boldsymbol{x}\in\mathcal{X}$, the normal cone of $\mathcal{X}$ at $\boldsymbol{x}$ is defined as

$$\mathsf{N}_{(\mathcal{X})}(\boldsymbol{x})=\left\{\boldsymbol{z}\in\mathbb{R}^n\,\middle|\,\boldsymbol{z}^T(\boldsymbol{y}-\boldsymbol{x})\leq 0,\quad\forall\boldsymbol{y}\in\mathcal{X}\right\}.\tag{40}$$

For a convex (not necessarily differential) function $f:\mathcal{X}\to\mathbb{R}$, where $\mathcal{X}\subseteq\mathbb{R}^n$ is a convex set, a subgradient of f at $\boldsymbol{x}\in\mathcal{X}$ is a vector $\boldsymbol{z}$ such that

$$f(\boldsymbol{y})\geq f(\boldsymbol{x})+\boldsymbol{z}^T(\boldsymbol{y}-\boldsymbol{x}),\quad\forall\boldsymbol{y}\in\mathcal{X}.\tag{41}$$

The set of all subgradients are called subdifferential and denoted by $\partial_{\boldsymbol{x}}f$. The subdifferential reduces to differential if f can be differentiated.

We have show that the GRNEP is equivalent to $\mathsf{VI}\left(\bar{\mathcal{P}},\bar{\boldsymbol{F}}\right)$. From the perspective of VI problem, the convex feasible region $\bar{\mathcal{P}}$ indicates that its solution satisfies the Karush-Kuhn-Tucker condition. In particular, for a solution $\boldsymbol{p}^{\star}$, it satisfies the following condition

$$\mathbf{0}\in\bar{\boldsymbol{F}}(\boldsymbol{p}^{\star})+\sum_{n\in\mathcal{N}}\kappa_n^{\star}\partial_{\boldsymbol{p}}\zeta_n(\boldsymbol{p}^{\star})+\mathsf{N}_{(\mathcal{P})}(\boldsymbol{p}^{\star}),\tag{42}$$

with subdifferential and normal cone expressions detailed above, and $\kappa^{\star}$ is the Lagrange multiplier that satisfies the complementarity condition as

$$0\leq\boldsymbol{\kappa}^{\star}\perp\boldsymbol{\zeta}(\boldsymbol{p}^{\star})\leq 0.\tag{43}$$

Note here we adopt the sub-differential since we have not yet obtained the closed-form expression for ζ_n. According to properties of sub-differential and normal cone [36], we have

$$\sum_{n\in\mathcal{N}}\kappa_n\partial_{\boldsymbol{p}}\zeta_n(\boldsymbol{p})=\prod_{j\in\mathcal{J}}\sum_{n\in\mathcal{N}}\kappa_n\partial_{\boldsymbol{p}_j}\zeta_n\left(\boldsymbol{p}_j,\boldsymbol{p}_{-j}\right)\tag{44}$$

and

$$\mathsf{N}_{(\mathcal{P})}(\boldsymbol{p})=\prod_{j\in\mathcal{J}}\mathsf{N}_{(\mathcal{P}_j)}\left(\boldsymbol{p}_j,\boldsymbol{p}_{-j}\right),\tag{45}$$

based on the Cartesian structure of $\mathcal{P}$ with $\mathcal{P}=\prod_{j\in\mathcal{J}}\mathcal{P}_j$. Then, we can rewrite the equilibrium condition in (42) as

$$\mathbf{0}\in\bar{\boldsymbol{F}}_j\left(\boldsymbol{p}_j^{\star},\boldsymbol{p}_{-j}^{\star}\right)+\sum_{n\in\mathcal{N}}\kappa_n^{\star}\partial_{\boldsymbol{p}_j}\zeta_n\left(\boldsymbol{p}_j^{\star},\boldsymbol{p}_{-j}^{\star}\right)+\mathsf{N}_{(\mathcal{P}_j)}\left(\boldsymbol{p}_j^{\star},\boldsymbol{p}_{-j}^{\star}\right),\quad\forall j\in\mathcal{J},\tag{46}$$

for the individual SBSs. On the other hand, for $\mathsf{NCP}(\boldsymbol{\kappa})$ with priced NEP $\mathfrak{G}_{\boldsymbol{\kappa}}$, we denote the solution as $\boldsymbol{\kappa}^{\star}$ and $\boldsymbol{p}^{\star}(\boldsymbol{\kappa}^{\star})$, then it satisfies

$$\mathbf{0}\in\bar{\boldsymbol{F}}_j\left(\boldsymbol{p}^{\star}(\boldsymbol{\kappa}^{\star})\right)+\sum_{n\in\mathcal{N}}\kappa_n^{\star}\partial_{\boldsymbol{p}_j}\zeta_n\left(\boldsymbol{p}^{\star}(\boldsymbol{\kappa}^{\star})\right)+\mathsf{N}_{(\mathcal{P}_j)}\left(\boldsymbol{p}^{\star}(\boldsymbol{\kappa}^{\star})\right),\quad\forall j\in\mathcal{J},\tag{47}$$

with

$$\mathbf{0}\leq\boldsymbol{\kappa}^{\star}\perp\boldsymbol{\zeta}\left(\boldsymbol{p}^{\star}(\boldsymbol{\kappa}^{\star})\right)\leq\mathbf{0}.\tag{48}$$

which are obtained based on the individual optimality of SBSs in $\mathfrak{G}_{\boldsymbol{\kappa}}$ and the solution condition of $\mathsf{NCP}(\boldsymbol{\kappa})$. Obviously, we can see that the optimality condition for the GRNEP specified in (46) and (43) and the solution condition of the decomposed NCP with priced NEP in (47) and (48) are identical. Therefore, the decomposition has been conducted in an solution-equivalent sense.

Appendix D
Proof of Theorem 5

To investigate the uniqueness of the equilibrium of $\mathfrak{G}_{\boldsymbol{\kappa}}$, we also resort to VI-assisted analysis. Based on the discussions in App. C, we can introduce the negative sub-differential of $\mathcal{C}_j$ as

$$\boldsymbol{\mathcal{F}}_j\left(\boldsymbol{p}_j,\boldsymbol{p}_{-j}\right)=\bar{\boldsymbol{F}}_j\left(\boldsymbol{p}_j,\boldsymbol{p}_{-j}\right)+\partial_{\boldsymbol{p}_j}\sum_{n\in\mathcal{N}}\kappa_n\zeta_n\left(\boldsymbol{p}_j,\boldsymbol{p}_{-j}\right).\tag{49}$$

Then, we can formulate the generalized VI (GVI) problem[4] for SBS-j, denoted by $\mathsf{GVI}_j\left(\mathcal{P}_j, \boldsymbol{\mathcal{F}}_j\right)$, which is to find $\boldsymbol{p}_j^\star \in \mathcal{P}_j$ with $\boldsymbol{u}_j^\star \in \boldsymbol{\mathcal{F}}_j\left(\boldsymbol{p}_j^\star\right)$ such that

$$\left(\boldsymbol{p}_j - \boldsymbol{p}_j^\star\right)^T \boldsymbol{u}_j^\star \geq 0, \quad \forall \boldsymbol{p}_j \in \mathcal{P}_j. \tag{50}$$

Based on concavity of $\mathcal{C}_j$, we know that the optimization in (27) is equivalent to the problem $\mathsf{GVI}_j\left(\mathcal{P}_j, \boldsymbol{\mathcal{F}}_j\right)$, where the equivalence can be similarly proved as Lemma 1. Then, for the priced NEP in the networked scope, it is equivalent to $\mathsf{GVI}\left(\mathcal{P}, \boldsymbol{\mathcal{F}}\right)$ which concatenates the problem of all SBSs with $\mathcal{P} = \prod_{j\in\mathcal{J}} \mathcal{P}_j$, and $\boldsymbol{\mathcal{F}} = \prod_{j\in\mathcal{J}} \boldsymbol{\mathcal{F}}_j$.

Since the NEP $\mathfrak{G}_{\boldsymbol{\kappa}}$ and GVI $\mathsf{GVI}\left(\mathcal{P}, \boldsymbol{\mathcal{F}}\right)$ are equivalent, we explore the condition for the unique solution to the GVI problem. Similar to the proof in App. B, the strongly monotone property guarantees a unique solution. For $\mathsf{GVI}\left(\mathcal{P}, \boldsymbol{\mathcal{F}}\right)$, the strongly monotone is satisfied when $\boldsymbol{p}^{(1)}, \boldsymbol{p}^{(2)} \in \mathcal{P}$ with $\boldsymbol{u}^{(1)} \in \boldsymbol{\mathcal{F}}\left(\boldsymbol{p}^{(1)}\right), \boldsymbol{u}^{(2)} \in \boldsymbol{\mathcal{F}}\left(\boldsymbol{p}^{(2)}\right)$ satisfies the following inequality

$$\left(\boldsymbol{p}^{(1)} - \boldsymbol{p}^{(2)}\right)^T \left(\boldsymbol{u}^{(1)} - \boldsymbol{u}^{(2)}\right) \geq c_{\text{gsm}} \left\|\boldsymbol{p}^{(1)} - \boldsymbol{p}^{(2)}\right\|^2, \tag{51}$$

where c_{gsm} is a positive constant. Then, we seek for condition for strongly monotone GVI. For the inequality in (51), we can expand the left-hand side as

$$\begin{aligned}
&\left(\boldsymbol{p}^{(1)} - \boldsymbol{p}^{(2)}\right)^T \left(\boldsymbol{u}^{(1)} - \boldsymbol{u}^{(2)}\right) \\
&= \left(\boldsymbol{p}^{(1)} - \boldsymbol{p}^{(2)}\right)^T \left(\left(\bar{\boldsymbol{F}}\left(\boldsymbol{p}^{(1)}\right) - \bar{\boldsymbol{F}}\left(\boldsymbol{p}^{(2)}\right)\right)\right. \\
&\quad \left. + \sum_{n\in\mathcal{N}} \kappa_n \left(\boldsymbol{v}_n^{(1)} - \boldsymbol{v}_n^{(2)}\right)\right) \\
&= \left(\boldsymbol{p}^{(1)} - \boldsymbol{p}^{(2)}\right)^T \left(\bar{\boldsymbol{F}}\left(\boldsymbol{p}^{(1)}\right) - \bar{\boldsymbol{F}}\left(\boldsymbol{p}^{(2)}\right)\right) \\
&\quad + \sum_{n\in\mathcal{N}} \kappa_n \left(\boldsymbol{p}^{(1)} - \boldsymbol{p}^{(2)}\right)^T \left(\boldsymbol{v}_n^{(1)} - \boldsymbol{v}_n^{(2)}\right),
\end{aligned} \tag{52}$$

where $\boldsymbol{v}_n^{(1)} \in \partial_{\boldsymbol{p}} \zeta_n\left(\boldsymbol{p}^{(1)}\right)$ and $\boldsymbol{v}_n^{(2)} \in \partial_{\boldsymbol{p}} \zeta_n\left(\boldsymbol{p}^{(2)}\right)$. Since $\zeta_n\left(\boldsymbol{p}\right)$ is a convex function, we have

$$\zeta_n\left(\boldsymbol{p}^{(1)}\right) - \zeta_n\left(\boldsymbol{p}^{(2)}\right) \geq \left(\boldsymbol{v}_n^{(2)}\right)^T \left(\boldsymbol{p}^{(1)} - \boldsymbol{p}^{(2)}\right), \tag{53}$$

$$\zeta_n\left(\boldsymbol{p}^{(2)}\right) - \zeta_n\left(\boldsymbol{p}^{(1)}\right) \geq \left(\boldsymbol{v}_n^{(1)}\right)^T \left(\boldsymbol{p}^{(2)} - \boldsymbol{p}^{(1)}\right). \tag{54}$$

By summing up these two inequalities and rearranging the terms, we arrive that

$$\left(\boldsymbol{p}^{(1)} - \boldsymbol{p}^{(2)}\right)^T \left(\boldsymbol{v}_n^{(1)} - \boldsymbol{v}_n^{(2)}\right) \geq 0. \tag{55}$$

Then, from (52) and (55), we can derive that

$$\begin{aligned}
&\left(\boldsymbol{p}^{(1)} - \boldsymbol{p}^{(2)}\right)^T \left(\boldsymbol{u}^{(1)} - \boldsymbol{u}^{(2)}\right) \\
&\quad \geq \left(\boldsymbol{p}^{(1)} - \boldsymbol{p}^{(2)}\right)^T \left(\bar{\boldsymbol{F}}\left(\boldsymbol{p}^{(1)}\right) - \bar{\boldsymbol{F}}\left(\boldsymbol{p}^{(2)}\right)\right).
\end{aligned} \tag{56}$$

Recall in Theorem 2 that the positive definiteness of Υ supports the inequality in (36), then together with (56), we know that it confirms the strongly monotone of GVI in (51). Therefore, the condition in Theorem 2 guarantees the uniqueness of the solution to $\mathsf{GVI}\left(\mathcal{P}, \boldsymbol{\mathcal{F}}\right)$, and thus the unique equilibrium of $\mathfrak{G}_{\boldsymbol{\kappa}}$, which completes the proof.

[4]Based on the norms in VI theories [34], the terminology "generalized" in GVI indicates that the operator $\boldsymbol{\mathcal{F}}_j$ is a point-to-set mapping, which is different from the terminology "generalized" in GRNEP implying non-independent strategy space.

Appendix E
Proof of Theorem 6

For Alg. 1, we consider two iterative series given by $\left[\boldsymbol{p}^{(1)}(t)\right]_{t=0,1,\cdots}$ and $\left[\boldsymbol{p}^{(2)}(t)\right]_{t=0,1,\cdots}$. The iterative process is based on the best-response strategy by solving (33), which leads to the following inequality based on the concavity of the priced robust secrecy rate at SUE-j

$$\left(\boldsymbol{q} - \boldsymbol{p}_j^{(1)}(t)\right)^T \left(-\nabla_{\boldsymbol{p}_j} \mathcal{C}_j\left(\boldsymbol{p}\right)\Big|_{\boldsymbol{p}_j = \boldsymbol{p}_j^{(1)}(t), \boldsymbol{p}_{-j} = \boldsymbol{p}_{-j}^{(1)}(t-1)}\right) \geq 0, \quad \forall \boldsymbol{q} \in \mathcal{P}_j, \tag{57}$$

and

$$\left(\boldsymbol{q} - \boldsymbol{p}_j^{(2)}(t)\right)^T \left(-\nabla_{\boldsymbol{p}_j} \mathcal{C}_j\left(\boldsymbol{p}\right)\Big|_{\boldsymbol{p}_j = \boldsymbol{p}_j^{(2)}(t), \boldsymbol{p}_{-j} = \boldsymbol{p}_{-j}^{(2)}(t-1)}\right) \geq 0, \quad \forall \boldsymbol{q} \in \mathcal{P}_j. \tag{58}$$

By letting $\boldsymbol{q} = \boldsymbol{p}_j^{(2)}(t)$ and $\boldsymbol{q} = \boldsymbol{p}_j^{(1)}(t)$ in (57) and (58), respectively, and summing up these two inequalities, we have

$$\begin{aligned}
&\left(\boldsymbol{p}_j^{(1)}(t) - \boldsymbol{p}_j^{(2)}(t)\right)^T \left(\nabla_{\boldsymbol{p}_j} \mathcal{C}_j\left(\boldsymbol{p}\right)\Big|_{\boldsymbol{p}_j = \boldsymbol{p}_j^{(1)}(t), \boldsymbol{p}_{-j} = \boldsymbol{p}_{-j}^{(1)}(t-1)}\right. \\
&\quad \left. - \nabla_{\boldsymbol{p}_j} \mathcal{C}_j\left(\boldsymbol{p}\right)\Big|_{\boldsymbol{p}_j = \boldsymbol{p}_j^{(2)}(t), \boldsymbol{p}_{-j} = \boldsymbol{p}_{-j}^{(2)}(t-1)}\right) \geq 0,
\end{aligned} \tag{59}$$

and further arrive at

$$\begin{aligned}
&\left(\boldsymbol{p}_j^{(1)}(t) - \boldsymbol{p}_j^{(2)}(t)\right)^T \left(\nabla^2_{\boldsymbol{p}_j, \boldsymbol{p}} \mathcal{C}_j\left(\boldsymbol{p}^\mu\right)\right) \\
&\quad \cdot \left(\left[\boldsymbol{p}_j^{(1)}(t), \boldsymbol{p}_{-j}^{(1)}(t)\right] - \left[\boldsymbol{p}_j^{(2)}(t), \boldsymbol{p}_{-j}^{(2)}(t)\right]\right) \geq 0,
\end{aligned} \tag{60}$$

which is based on the mean-value theorem and $\boldsymbol{p}^\mu$ is similar defined as its counterpart in (38). Then, we separate the terms regarding SUE-j and others in the inequality above and reach

$$\begin{aligned}
&\left(\boldsymbol{p}_j^{(1)}(t) - \boldsymbol{p}_j^{(2)}(t)\right)^T \left(-\nabla^2_{\boldsymbol{p}_j, \boldsymbol{p}_j} \mathcal{C}_j\left(\boldsymbol{p}^\mu\right)\right) \left(\boldsymbol{p}_j^{(1)}(t) - \boldsymbol{p}_j^{(2)}(t)\right) \\
&\leq \left(\boldsymbol{p}_j^{(1)}(t) - \boldsymbol{p}_j^{(2)}(t)\right)^T \sum_{i\in\mathcal{J}\setminus\{j\}} \left(\nabla^2_{\boldsymbol{p}_j, \boldsymbol{p}_i} \mathcal{C}_j\left(\boldsymbol{p}^\mu\right)\right) \\
&\quad \times \left(\boldsymbol{p}_i^{(1)}(t) - \boldsymbol{p}_i^{(2)}(t)\right).
\end{aligned} \tag{61}$$

Leveraging the definition of matrix Υ in (24), we further have

$$\begin{aligned}
&\gamma_{jj} \left\|\boldsymbol{p}_j^{(1)}(t) - \boldsymbol{p}_j^{(2)}(t)\right\|^2 \\
&\geq \sum_{i\in\mathcal{J}\setminus\{j\}} \gamma_{ji} \left\|\boldsymbol{p}_j^{(1)}(t) - \boldsymbol{p}_j^{(2)}(t)\right\| \\
&\quad \times \left\|\boldsymbol{p}_j^{(1)}(t-1) - \boldsymbol{p}_j^{(2)}(t-1)\right\|.
\end{aligned} \tag{62}$$

By concactating the inequality above at all SBSs, we have

$$\begin{aligned}
&\left[\left\|\boldsymbol{p}_j^{(1)}(t) - \boldsymbol{p}_j^{(2)}(t)\right\|\right]_{j\in\mathcal{J}} \\
&\quad \leq \Gamma \left[\left\|\boldsymbol{p}_j^{(1)}(t-1) - \boldsymbol{p}_j^{(2)}(t-1)\right\|\right]_{j\in\mathcal{J}},
\end{aligned} \tag{63}$$

where matrix Γ is defined as

$$[\Gamma]_{ij} = \begin{cases} 0 & \text{if } i = j, \\ -\dfrac{\gamma_{ji}}{\gamma_{jj}} & \text{else.} \end{cases} \tag{64}$$

Finally, through norm inequality, we have

$$\left\| \boldsymbol{p}^{(1)}(t) - \boldsymbol{p}^{(2)}(t) \right\| \leq \rho\left(\Gamma\right) \left\| \boldsymbol{p}^{(1)}(t-1) - \boldsymbol{p}^{(2)}(t-1) \right\|, \tag{65}$$

where $\rho\left(\cdot\right)$ denotes the spectral norm. Based on the concept of P-matrix [37], we know that the positive definiteness of Υ leads to $\rho\left(\Gamma\right) < 1$. Therefore, the iterations in Alg. 1 produce a contraction mapping, which is thus guaranteed to converge.

For Alg. 2, it is in essence an application of the projection algorithm with variable steps [34], [38]. With Υ being positive definite, suggesting strongly monotone of $\bar{\boldsymbol{F}}$ in (18), price term being convex in (33), and the step size condition given in Theorem 6, then the convergence conditions specified in [38, Theorem 4.5] (or equivalently [34, Theorem 12.1.8]) are all satisfied, which guarantees the convergence of Alg. 2.

REFERENCES

[1] F. Al-Turjman, E. Ever, and H. Zahmatkesh, "Small cells in the forthcoming 5G/IoT: Traffic modelling and deployment overview," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 28–65, 1st Quart., 2019.

[2] D. Muirhead, M. A. Imran, and K. Arshad, "A survey of the challenges, opportunities and use of multiple antennas in current and future 5G small cell base stations," *IEEE Access*, vol. 4, pp. 2952–2964, 2016.

[3] J. Cao *et al.*, "A survey on security aspects for 3GPP 5G networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 170–195, 1st Quart., 2020.

[4] Y. Wu, T. Q. Duong, and A. L. Swindlehurst, "Safeguarding 5G-and-beyond networks with physical layer security," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 4–5, Oct. 2019.

[5] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game: Interaction between source, eavesdropper, and friendly jammer," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, no. 1, pp. 1–10, Dec. 2010.

[6] W. Zhang, J. Chen, Y. Kuo, and Y. Zhou, "Transmit beamforming for layered physical layer security," *IEEE Trans. Veh. Technol.*, vol. 68, no. 10, pp. 9747–9760, Oct. 2019.

[7] Q. Li, Y. Yang, W.-K. Ma, M. Lin, J. Ge, and J. Lin, "Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks," *IEEE Trans. Signal Process.*, vol. 63, no. 1, pp. 206–220, Jan. 2015.

[8] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2734–2771, 3rd Quart., 2019.

[9] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[10] L. Wang, K.-K. Wong, S. Jin, G. Zheng, and R. W. Heath, Jr., "A new look at physical layer security, caching, and wireless energy harvesting for heterogeneous ultra-dense networks," *IEEE Commun. Mag.*, vol. 56, no. 6, pp. 49–55, Jun. 2018.

[11] C. Yang, J. Li, R. Q. Hu, and J. Xiao, "Distributed optimal cooperation for spectral and energy efficiency in hyper-dense small cell networks," *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 154–160, Jun. 2017.

[12] J. Wang, W. Guan, Y. Huang, R. Schober, and X. You, "Distributed optimization of hierarchical small cell networks: A GNEP framework," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 2, pp. 249–264, Feb. 2017.

[13] R. Bonnefoi, C. Moy, and J. Palicot, "Power control and cell discontinuous transmission used as a means of decreasing small-cell networks' energy consumption," *IEEE Trans. Green Commun. Netw.*, vol. 2, no. 4, pp. 899–914, Dec. 2018.

[14] J. Li, S. Chu, F. Shu, J. Wu, and D. N. K. Jayakody, "Contract-based small-cell caching for data disseminations in ultra-dense cellular networks," *IEEE Trans. Mobile Comput.*, vol. 18, no. 5, pp. 1042–1053, May 2019.

[15] M. M. Hasan, S. Kwon, and J.-H. Na, "Adaptive mobility load balancing algorithm for LTE small-cell networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 4, pp. 2205–2217, Apr. 2018.

[16] Z. Li, M. L. Sichitiu, and X. Qiu, "Fog radio access network: A new wireless backhaul architecture for small cell networks," *IEEE Access*, vol. 7, pp. 14150–14161, 2019.

[17] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Quart., 2017.

[18] J. Wang, Y. Huang, S. Jin, R. Schober, X. You, and C. Zhao, "Resource management for device-to-device communication: A physical layer security perspective," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 946–960, Apr. 2018.

[19] X. Tang, P. Ren, Y. Wang, and Z. Han, "Combating full-duplex active eavesdropper: A hierarchical game perspective," *IEEE Trans. Commun.*, vol. 65, no. 3, pp. 1379–1395, Mar. 2017.

[20] J. Chen, X. Chen, W. H. Gerstacker, and D. W. K. Ng, "Resource allocation for a massive MIMO relay aided secure communication," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1700–1711, Aug. 2016.

[21] W.-Q. Wang and Z. Zheng, "Hybrid MIMO and phased-array directional modulation for physical layer security in mmWave wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1383–1396, Jul. 2018.

[22] Z. Xiang, W. Yang, G. Pan, Y. Cai, and Y. Song, "Physical layer security in cognitive radio inspired NOMA network," *IEEE J. Sel. Topics Signal Process.*, vol. 13, no. 3, pp. 700–714, Jun. 2019.

[23] Y. Zou, M. Sun, J. Zhu, and H. Guo, "Security-reliability tradeoff for distributed antenna systems in heterogeneous cellular networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 8444–8456, Dec. 2018.

[24] Y. Deng, L. Wang, M. Elkashlan, A. Nallanathan, and R. K. Mallik, "Physical layer security in three-tier wireless sensor networks: A stochastic geometry approach," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1128–1138, Jun. 2016.

[25] P. Siyari, M. Krunz, and D. N. Nguyen, "Power games for secure communications in single-stream MIMO interference networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 9, pp. 5759–5773, Sep. 2018.

[26] Y. Zhong, X. Ge, T. Han, Q. Li, and J. Zhang, "Tradeoff between delay and physical layer security in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1635–1647, Jul. 2018.

[27] X. Tang, P. Ren, and Z. Han, "Hierarchical competition as equilibrium program with equilibrium constraints towards security-enhanced wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1564–1578, Jul. 2018.

[28] J. Zhang, C. Kundu, O. A. Dobre, E. Garcia-Palacios, and N.-S. Vo, "Secrecy performance of small-cell networks with transmitter selection and unreliable backhaul under spectrum sharing environment," *IEEE Trans. Veh. Technol.*, vol. 68, no. 11, pp. 10895–10908, Nov. 2019.

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

[30] T.-X. Zheng, H.-M. Wang, and J. Yuan, "Physical-layer security in cache-enabled cooperative small cell networks against randomly distributed eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 17, no. 9, pp. 5945–5958, Sep. 2018.

[31] K. Xiao, W. Li, M. Kadoch, and C. Li, "On the secrecy capacity of 5G mmWave small cell networks," *IEEE Wireless Commun.*, vol. 25, no. 4, pp. 47–51, Aug. 2018.

[32] X. Tang, P. Ren, and Z. Han, "Securing small cell networks under interference constraint: A quasi-variational inequality approach," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Abu Dhabi, UAE, Dec. 2018, pp. 1–6.

[33] S. Boyd and L. Vandenberghe, *Convex Optimization*. New York, NY, USA: Cambridge Univ. Press, 2004.

[34] F. Facchinei and J. Pang, *Finite-Dimensional Variational Inequalities and Complementarity Problems*. New York, NY, USA: Springer-Verlag, 2003.

[35] Z. Han, D. Niyato, W. Saad, and T. Başar, *Game Theory for Next Generation Wireless and Communication Networks*. Cambridge, U.K.: Cambridge Univ. Press, 2019.

[36] J. Wang, M. Peng, S. Jin, and C. Zhao, "A generalized Nash equilibrium approach for robust cognitive radio networks via generalized variational inequalities," *IEEE Trans. Wireless Commun.*, vol. 13, no. 7, pp. 3701–3714, Jul. 2014.
[37] R. W. Cottle, J.-S. Pang, and R. E. Stone, *The Linear Complementarity Problem*. Philadelphia, PA, USA: SIAM, 2009.
[38] G. Scutari, D. P. Palomar, F. Facchinei, and J.-S. Pang, "Monotone games for cognitive radio systems," in *Distributed Decision Making and Control*, R. Johansson and A. Rantzer, Eds. London, U.K.: Springer, 2012, pp. 83–112.

Xiao Tang (Member, IEEE) received the B.S. degree in information engineering (elite class named after Tsien Hsue-Shen) and the Ph.D. degree in information and communication engineering from Xi'an Jiaotong University in 2011 and 2018, respectively. From 2015 to 2016, he was a Visiting Student with the Department of Electrical and Computer Engineering, University of Houston. He is currently with the Department of Communication Engineering, Northwestern Polytechnical University. His research interests include wireless communications and networking, game theory, and physical layer security.

Ruonan Zhang (Member, IEEE) received the B.S. and M.Sc. degrees in electrical and electronics engineering from Xian Jiaotong University, Xian, China, in 2000 and 2003, respectively, and the Ph.D. degree in electrical and electronics engineering from the University of Victoria, Victoria, BC, Canada, in 2010. He was an IC Design Engineer with Motorola, Inc., and Freescale Semiconductor, Inc., Tianjin, China, from 2003 to 2006. Since 2010, he has been with the Department of Communication Engineering, Northwestern Polytechnical University, Xi'an, where he is currently a Professor. His current research interests include wireless channel measurement and modeling, architecture and protocol design of wireless networks, and satellite communications. Dr. Zhang was a recipient of the New Century Excellent Talent Grant from the Ministry of Education of China. He has served as a Local Arrangement Co-Chair for the IEEE/CIC International Conference on Communications in China in 2013. He has served as an Associate Editor for the *Journal of Communications and Networks*.

Wei Wang (Member, IEEE) received the B.Eng. degree in information countermeasure technology and the M.Eng. degree in signal and information processing from Xidian University in 2011 and 2014, respectively, and the Ph.D. degree in electrical and electronic engineering from Nanyang Technological University in 2018. From 2018 to 2019, he was a Post-Doctoral Fellow with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. He is currently a Professor with the Nanjing University of Aeronautics and Astronautics. His research interests include wireless communications, space–air–ground integrated networks, wireless security, and blockchain. He was a recipient of the IEEE Student Travel Grants at the IEEE ICC 2017 and the Chinese Government Award for outstanding self-financed students abroad.

Lin Cai (Fellow, IEEE) received the M.A.Sc. and Ph.D. degrees in electrical and computer engineering from the University of Waterloo, Waterloo, Canada, in 2002 and 2005, respectively. Since 2005, she has been with the Department of Electrical and Computer Engineering, University of Victoria, where she is currently a Professor. Her research interests span several areas in communications and networking, with a focus on network protocol and architecture design supporting emerging multimedia traffic, and the Internet of Things. She is an NSERC E.W.R. Steacie Memorial Fellow. In 2020, she was elected as a member of the Royal Society of Canada's College of New Scholars, Artists and Scientists. She was a recipient of the Outstanding Achievement in Graduate Studies for her Ph.D. thesis.

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

Zhu Han (Fellow, IEEE) received the B.S. degree in electronic engineering from Tsinghua University in 1997 and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Maryland, College Park, in 1999 and 2003, respectively.

From 2000 to 2002, he was a Research and Development Engineer with JDSU, Germantown, MD, USA. From 2003 to 2006, he was a Research Associate with the University of Maryland. From 2006 to 2008, he was an Assistant Professor with Boise State University, Idaho. He is currently a John and Rebecca Moores Professor with the Department of Electrical and Computer Engineering and also the Department of Computer Science, University of Houston, TX, USA. His research interests include wireless resource allocation and management, wireless communications and networking, game theory, big data analysis, security, and smart grid. He has been an AAAS Fellow since 2019 and the ACM Distinguished Member since 2019. He was an IEEE Communications Society Distinguished Lecturer from 2015 to 2018. He received the NSF Career Award in 2010, the Fred W. Ellersick Prize of the IEEE Communication Society in 2011, the EURASIP Best Paper Award for the *Journal on Advances in Signal Processing* in 2015, IEEE Leonard G. Abraham Prize in the field of Communications Systems (Best Paper Award in IEEE JSAC) in 2016, and several best paper awards in IEEE conferences. He also received the 2021 IEEE Kiyo Tomiyasu Award for outstanding early to mid-career contributions to technologies holding the promise of innovative applications for contributions to game theory and distributed management of autonomous communication networks. He has been a 1% highly cited researcher since 2017 according to Web of Science.