Secure User-Centric Clustering for Energy Efficient Ultra Dense Networks: Design and Optimization

Yan Lin, *Student Member, IEEE*, Rong Zhang, *Senior Member, IEEE*, Luxi Yang, *Member, IEEE*, and Lajos Hanzo, *Fellow, IEEE*

***Abstract*—With an unprecedented amount of sensitive private data generated by mobile user equipment (UE), securing the emerging ultra dense networks (UDNs) becomes critical. Hence we investigate secure UDNs in the context of user-centric clustering architectures relying on both a dedicated jamming strategy and an embedded jamming strategy. We formulate the secure user-centric clustering design for both strategies both with and without the eavesdropper's channel state information (CSI) from a secrecy-energy-efficiency perspective. Explicitly, we conceive secure transmission schemes, while guaranteeing both the throughput quality of service (TQoS) and the secrecy quality of service (SQoS). To efficiently solve the underlying NP-hard problem, a set of heuristic greedy algorithms are developed for diverse operating scenarios. Finally, our numerical results reveal the quantitative benefits of the proposed secure user-centric clustering architectures as a function of the network densities (i.e. AP, UE and eavesdropper) and of both the TQoS and the SQoS constraints on the secrecy-energy-efficiency trade-off in different scenarios.**

***Index Terms*—UDN, physical layer security, secure user-centric clustering, secrecy-energy-efficiency.**

I. Introduction

A. Motivation and Scopes

The explosive proliferation of mobile user equipment (UE), such as smart phones and wearable devices, has resulted in ultra dense networks (UDNs) supporting high-rate multimedia services [1]–[4]. Given the unprecedented amount of sensitive private data transmitted over wireless channels, such as mobile payment relying on these UEs, their security has become a critical issue. As one of the popular techniques of protecting the networks from the eavesdroppers, physical layer security (PLS) has become a promising complement to the upper layer encryption techniques to guarantee secure end-to-end transmissions over wireless channels, paving the way for secure UDNs [5]–[7].

Conceptually, UDNs are fundamental to support a high connection density (potentially coping with 10,000 devices per square kilo-meter) at a high data rate [8]. In contrast to the traditional cell-centric network, UDNs rely on a hierarchical topology of compact, low power, low cost access points (APs). As a result, the user-centric clustering philosophy is emerging to allow the UEs to benefit from AP cooperation in UDNs [9] [10], which may substantially improve the throughput quality of service (TQoS) for each UE. However, in the presence of eavesdroppers, the secure transmission and the secrecy quality of service (SQoS) of each UE also has to be guaranteed. Although substantial research efforts have been invested into the PLS of wireless communications [11]–[15], the existing PLS policies cannot be directly applied to user-centric UDNs due to their high density and complex topology. **To the best of our knowledge, the PLS issues of user-centric UDNs constitute an open issue at the time of writing.**

Against the above backdrop, in this paper, we consider the PLS of UDNs in the presence of eavesdroppers. To be specific, for a given UE, the APs that are in its user-centric cluster may act as its cooperative serving APs for joint data transmission [16] [17], while those APs that are not in its user-centric cluster may be included to act as cooperative jammers for supporting secure transmission [18]–[22]. We refer to this strategy as *dedicated jamming*. Alternatively, the APs may jointly - rather than exclusively - perform serving and jamming. We refer to this strategy as *embedded jamming*. Secure transmission schemes differ substantially based on the availability of the eavesdropper's channel state information (CSI). Indeed, the eavesdropper may be active or passive (i.e. only listen but does not transmit) [23], hence its CSI may be known or unknown. In the case of unknown CSI, secure transmission can be achieved by the artificial noise aided technique of [24]. By contrast, in the case of known CSI, the legitimate transmitter can optimize its beamformer to enhance the data transmission rate for the intended UE for the sake of exceeding the eavesdropper's capacity. In this case, the transmitter can also combine the beamformer design with artificial noise genaration to degrade the overheard signals and to simultaneously enhance the legitimate UE's rate [25]. Naturally, having more serving APs and more dedicated jammers is capable of enhancing the UE's secrecy rate. However, when taking the energy consumption into account, which is also a critical issue in 5G [1], it is desirable to put some APs into sleep mode for energy savings. Hence, the intriguing research question becomes as how we can control the involvement of APs in the user-centric UDNs from the perspective of *secrecy-energy-efficiency*.

B. Related Contributions

Recently, user-centric UDNs have drawn substantial attention, thanks to their capability of satisfying each UE's TQoS in dense environments, regardless of its location. In particular, some research efforts have been focussed on the user-centric clustering design problem. For instance, Garcia *et al.* [26] designed a user-centric adaptive clustering method with the goal of maximizing each AP's normalized outage capacity. It was

The financial support of the European Research Council's Advanced Fellow Grant is gratefully acknowledged
IEEE JSAC 2018

shown that the user-centric adaptive clustering outperforms any fixed or predefined clustering by adapting its coordination to match each UE's specific conditions. As a further advance, Nie *et al.* [27] investigated both the spectral efficiency as well as the energy efficiency and proposed an energy-efficient user-centric cross-tier clustering solution, subject to a minimum spectral efficiency constraint. Another interesting proposal of Kang and Kim [28] was the dynamic clustering and inter-cluster coordination solution conceived for mitigating the interference imposed on cluster-edge UEs, which was shown to be particulaly efficient in overlapped clustering scenarios. As an extension, Huang *et al.* [29] proposed a clustering scheme with the aim of reducing the cluster update frequency. However, none of the above solutions have considered the security problems of user-centric UDNs in the presence of eavesdroppers.

Clearly, there is a paucity of literature on PLS solutions for UDNs. Wang *et al.* [6] introduced the PLS-oriented resource allocation problem in UDNs and presented their potential security challenges. As a further extension, Kamel *et al.* [7] evaluated the average secrecy rate of UDNs under Rician fading channels by employing stochastic geometry. However, the benefits of the user-centric clustering architecture have not been exploited to design any security policy for UDNs. Nevertheless, it is worth noting that neither [6] nor [7] considered the important security versus energy-efficiency trade-off, even though this design objective has been attracting increasing research attention [30]–[32] in conventional MIMO scenarios. Hence we extend this paramount trade-off to the user-centric UDNs considered in this paper. Finally, there are also contributions on various signal processing aspects of PLS [11]–[14].

C. Contributions and Organization

In this paper, we propose a novel secure user-centric clustering architecture and formulate its design for energy efficient UDNs, whilst relying both on the dedicated jamming strategy and on the embedded jamming strategy for maximizing the secrecy-energy-efficiency with the aid of various secure transmission schemes. To this end, we first have to establish a secure user-centric clustering architecture, and then elaborate on how to design the secure user-centric clustering problem based on different secure transmission schemes.

The main contributions of this paper are listed as follows:

1) A novel secure user-centric clustering architecture is proposed for enhancing the PLS of UDNs by introducing both the dedicated jamming strategy as well as the embedded jamming strategy, demonstrating the potential of the proposed architecture for improving the secrecy-energy-efficiency.
2) Based on this architecture, we consider secure transmissions for both the dedicated and the embedded jamming strategy, with both known and unknown eavesdropper CSI, relying on beamforming and artificial noise based jamming, respectively.
3) To maximize the secrecy-energy-efficiency, we formulate the design problem of secure user-centric clustering for energy efficient UDNs, while guaranteeing both the target TQoS and SQoS. A set of heuristic greedy algorithms are developed to efficiently solve the underlying NP-hard problem under different scenarios.
4) Numerically, our results reveal the benefits of the proposed secure user-centric clustering architecture and quantify the impact of the AP/UE/eavesdropper density and of the constraints on both the TQoS and SQoS. It is shown that the proposed dedicated jamming strategy has potential merits in terms of increasing the secrecy-energy-efficiency by exploiting the eavesdropper's CSI.

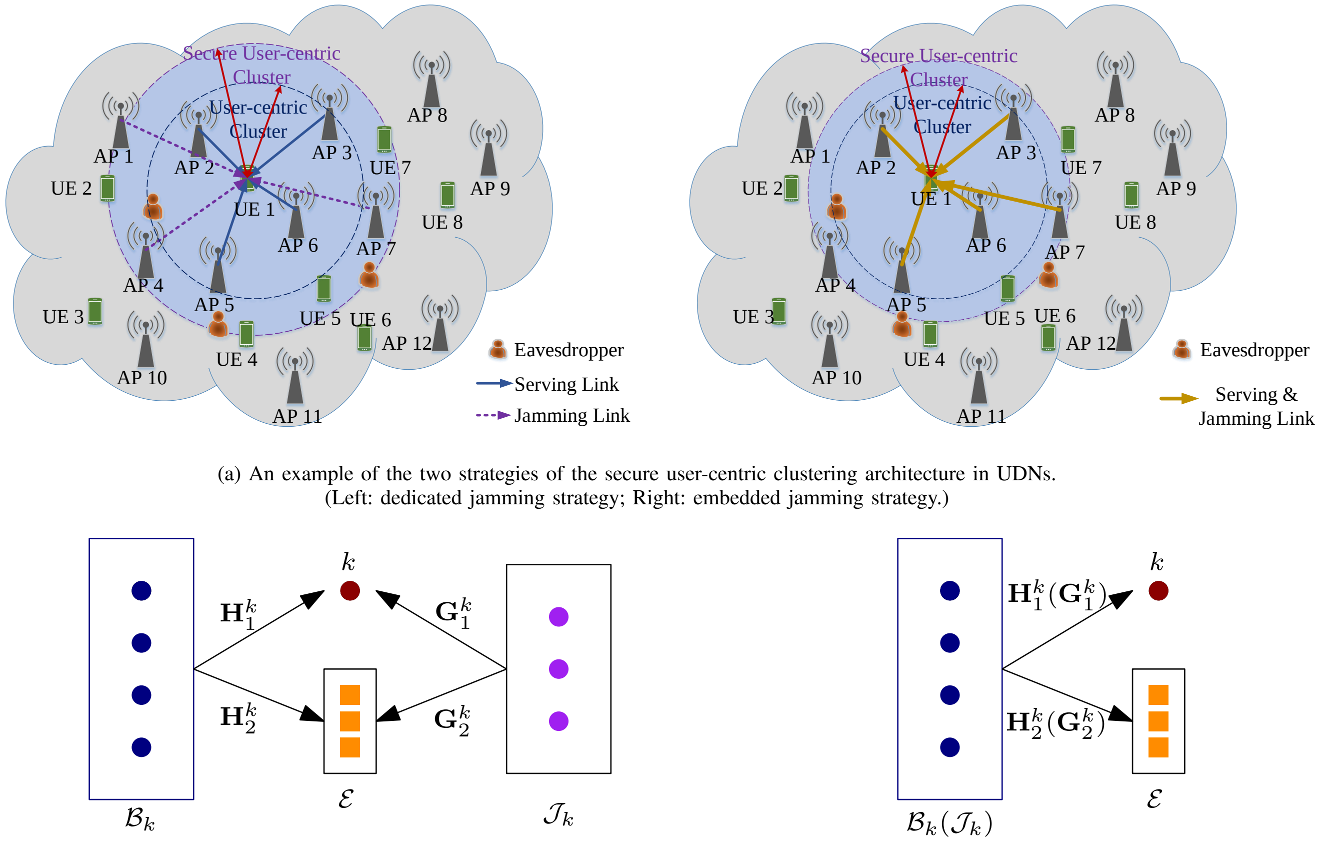
The rest of this paper is organized as follows. Section II describes the system model of user-centric UDNs and presents the proposed secure user-centric clustering architecture. Section III formulates the design problem of secure user-centric clustering and introduces the proposed solution framework. Then, Section IV focuses on various secure transmission schemes in different scenarios, while in Section V we propose the secure user-centric clustering algorithms for both strategies. Section VI presents our numerical results, and finally our conclusions are drawn in Section VII.

Notations: Matrices and vectors are expressed in italic bold capital letter and bold lower case letter respectively. Scalar variables are denoted by italic symbols. $|\mathcal{A}|$ denotes the cardinality of a set $\mathcal{A}$ and $|A|$ denotes the absolute value of a scalar A. $\mathbb{C}^{N\times M}$ denotes the space of all $N\times M$ matrices with complex entries. $\boldsymbol{I}_N$ denotes the N-dimensional unit matrix. Given a complex matrix, $(\cdot)^H$ and $Tr\{\cdot\}$ denote the conjugate transpose and trace, respectively. $(\cdot)^{-1}$ denotes the inverse of a square matrix. $\mathbb{E}\{\cdot\}$ denotes the expectation of a variable. $[x]^+$ denotes $\max\{0,x\}$. $\exp(\cdot)$ and $\mathrm{sgn}(\cdot)$ denote the exponential and sign function respectively. *Null*$\{\cdot\}$ denotes the nullspace of a matrix.

II. System Model

A. Secure User-centric Clustering Architecture

We consider a user-centric UDN consisting of B APs and K UEs in the presence of E eavesdroppers, all of which are distributed independently according to homogeneous Poisson point processes (PPPs). All APs are assumed to be equipped with M_A antennas, while the UEs and eavesdroppers are assumed to be equipped with $M_U(< M_A)$ and $M_E(< M_A)$ antennas, respectively. The eavesdroppers may be active or passive, overhearing the information from all UEs. The CSI of UEs is assumed to be known to all APs. In order to achieve a high TQoS, each UE can be served simultaneously by multiple APs via AP cooperation, which constitutes the user-centric cluster supporting each UE. In this way, each AP may also simultaneously serve multiple UEs. In order to mitigate the inter-cluster interference, we employ orthogonal resource blocks (RBs) to separate the K independent user-centric clusters. Accordingly, in such a user-centric cluster, each UE is served by its serving AP set, but is also overheard by all eavesdroppers. To ensure an acceptable SQoS, we define the *secure user-centric cluster*. For the dedicated jamming strategy, the APs that are not in a given UE's user-centric cluster may be included to act as jammers to guarantee secure



(a) An example of the two strategies of the secure user-centric clustering architecture in UDNs.
(Left: dedicated jamming strategy; Right: embedded jamming strategy.)

(b) An illustration of the two strategies of the secure user-centric cluster.
(Left: dedicated jamming strategy; Right: embedded jamming strategy.)

Fig. 1: System Model

transmission. In this case, we refer to the AP as a *jamming AP* and the associated conventional AP as a *serving AP*. Then the secure user-centric cluster is defined by the union of the intended UE, its serving AP set and jamming AP set. By contrast, for the embedded jamming strategy, the APs within the secure user-centric cluster have the dual functionality of both serving and jamming. Hence, the serving AP set is identical to the jamming AP set. It is noteworthy that in this case, the coverage of the secure user-centric cluster may be the same as that of the user-centric cluster, or be larger than it, due to the TQoS and SQoS requirements.

Examples of both secure user-centric clustering architectures are depicted in Fig. 1(a), wherein the inner circle represents the user-centric cluster of UE 1 consisting of 4 serving APs to satisfy the target TQoS requirement. For the dedicated jamming strategy, UE 1 is guaranteed to have secure transmission with the aid of 3 other jammers (i.e. AP 1, AP 4, AP 7). By comparison, for the embedded jamming strategy, UE 1 is served by 5 embedded APs to satisfy both the TQoS and SQoS requirements by exploiting the dual functionality of serving and jamming. Both strategies of the corresponding secure user-centric clusters are illustrated in Fig. 1(b). In order to construct a unified model for both strategies, we define a series of sets and variables listed in TABLE I. Note that these definitions apply naturally to the dedicated jamming strategy, while for the embedded jamming strategy, $\mathcal{B}_k$ will be the same as $\mathcal{J}_k$ and $\boldsymbol{G}_1^k$ ($\boldsymbol{G}_2^k$) will be the same as $\boldsymbol{H}_1^k$ ($\boldsymbol{H}_2^k$).

TABLE I: NOTATION DEFINITIONS

$\mathcal{B}$	AP set of $\{1, ..., B\}$
$\mathcal{K}$	UE set of $\{1, ..., K\}$
$\mathcal{E}$	eavesdropper set of $\{1, ..., E\}$
$\mathcal{B}_k$	serving AP set of UE k
$\mathcal{J}_k$	jamming AP set of UE k
$\boldsymbol{H}_1^k$	$\in \mathbb{C}^{(\lvert\mathcal{B}_k\lvert M_A)\times M_U}$, the channel gains between $\mathcal{B}_k$ and UE k
$\boldsymbol{H}_2^{k,e}$	$\in \mathbb{C}^{(\lvert\mathcal{B}_k\lvert M_A)\times M_E}$, the channel gains between $\mathcal{B}_k$ and eavesdropper e
$\boldsymbol{H}_2^k$	$\{\boldsymbol{H}_2^{k,e}\}_{e\in\mathcal{E}}$, the channel gains between $\mathcal{B}_k$ and $\mathcal{E}$
$\boldsymbol{G}_1^k$	$\in \mathbb{C}^{(\lvert\mathcal{J}_k\lvert M_A)\times M_U}$, the channel gains between $\mathcal{J}_k$ and UE k
$\boldsymbol{G}_2^{k,e}$	$\in \mathbb{C}^{(\lvert\mathcal{J}_k\lvert M_A)\times M_E}$, the channel gains between $\mathcal{J}_k$ and eavesdropper e
$\boldsymbol{G}_2^k$	$\{\boldsymbol{G}_2^{k,e}\}_{e\in\mathcal{E}}$, the channel gains between $\mathcal{J}_k$ and $\mathcal{E}$

B. Wireless Channel Model

In general, the channel gains include the large-scale fading (path loss) and the small-scale fading. The small-scale fading coefficients are assumed to be identically and independently distributed (i.i.d.) zero-mean and unit-variance Rayleigh distributions. In UDNs, the standard path loss model is not capable of accurately capturing what happens as the networks densify [33] [34]. Hence, in this paper we follow the practical two-piece 3GPP Path Loss Model of [35], where the path loss includes both the line-of-sight (LoS) and non-line-of-sight (NLoS) transmissions with a certain probability. Let $d_{j,k}$ denote the two-dimensional distance (called distance hereafter) between AP j and UE k, while ψ denotes the absolute antenna height difference between any AP-UE pair. Then we consider the average path loss between AP j and UE k, which is based on the following function

$$\xi_{j,k} = \begin{cases} D_L z_{j,k}^{-\theta_L}, & \textit{LoS Prob: } Pr_L(z_{j,k}), \\ D_{NL} z_{j,k}^{-\theta_{NL}}, & \textit{NLoS Prob: } 1 - Pr_L(z_{j,k}). \end{cases} \tag{1}$$

Herein, $z_{j,k} = \sqrt{d_{j,k}^2 + \psi^2}$ denotes the three-dimensional distance between AP j and UE k, while D_L and D_{NL} denote the LoS and NLoS path losses at a unit reference distance, respectively. Furthermore, θ_L and θ_{NL} denote the LoS and NLoS path loss exponents, respectively. Besides, the LoS probability is segmented into two segments as follows

$$Pr_L(z_{j,k}) = \begin{cases} 1 - 5\exp(-\phi_1/z_{j,k}), & 0 < z_{j,k} \leq \overline{d}, \\ 5\exp(-z_{j,k}/\phi_2), & z_{j,k} > \overline{d}, \end{cases} \tag{2}$$

where ϕ_1, ϕ_2 and $\overline{d}$ are the shape parameters ensuring the continuity of $Pr_L(z_{j,k})$.

C. Downlink Transmission Model

Considering that there are two strategies to be discussed for the known and unknown eavesdropper CSI, in this paper we let $\alpha = \{0, 1\}$ and $\beta = \{0, 1\}$ indicate the CSI knowledge and the strategy adopted to unify the model, respectively. To be specific, $\alpha = 0$ (1) denotes the case of unknown (known) eavesdropper CSI, while $\beta = 0$ (1) represents adopting the embedded (dedicated) jamming strategy. Since the secure transmission scheme design is not the main focus of our paper, we choose two of the most popular methods to achieve secure transmission with the aid of the beamformer design for the known eavesdropper CSI and the artificial noise for the unknown eavesdropper CSI. In our hypothesis, the dedicated jammers adopt only jammer beamforming with known CSI for secure transmission, while adding an artificial noise for the unknown CSI scenario. As for the embedded jamming strategy, in order to achieve secure transmission, the embedded APs perform both transmit beamforming and jammer beamforming jointly with known CSI, while only adding an artificial noise source relying on a fraction $\gamma \in [0, 1)$ of the embedded AP's transmit power to contaminate the overheard signals, when the CSI is unknown. Finally, the transmit power of the APs involved in the secure user-centric cluster is assumed to be same, which is denoted as p_t.

Accordingly, the downlink signal received by UE k and the signal overheard by the eavesdropper e in the secure user-centric cluster of UE k may be, respectively, written as

$$\boldsymbol{y}_U^k = \sqrt{p_t} \boldsymbol{H}_1^{k^H} \boldsymbol{s}_B^k + \sum_{e \in \mathcal{E}} \sqrt{p_t} \boldsymbol{G}_1^{k^H} \boldsymbol{s}_J^{k,e} + \boldsymbol{n}_U^k \tag{3}$$

$$\boldsymbol{y}_E^{k,e} \quad = \sqrt{p_t} \boldsymbol{H}_2^{k,e^H} \boldsymbol{s}_B^k + \sqrt{p_t} \boldsymbol{G}_2^{k,e^H} \boldsymbol{s}_J^{k,e} + \boldsymbol{n}_E^{k,e}, \tag{4}$$

where the elements in $\boldsymbol{n}_U^k$ and $\boldsymbol{n}_E^{k,e}$ are the additive white Gaussian noise (AWGN) samples with variance σ^2, while $\boldsymbol{s}_B^k$ and $\boldsymbol{s}_J^{k,e}$ are respectively given by

$$\boldsymbol{s}_B^k \quad = \sqrt{1 - \bar{\gamma}} \boldsymbol{W}_B^k \boldsymbol{u}_B^k + \sqrt{\bar{\gamma}} \boldsymbol{v}_B^k \tag{5}$$

$$\boldsymbol{s}_J^{k,e} \quad = \alpha\beta \boldsymbol{W}_J^{k,e} \boldsymbol{u}_J^{k,e} + (1 - \alpha)\beta \boldsymbol{v}_J^k, \tag{6}$$

wherein $\bar{\gamma} = \gamma(1 - \alpha)(1 - \beta)$ denotes the unified expression relying on a specific fraction of the serving AP's transmit power assigned to the artificial noise, which is actually only activated in the embedded strategy associated with unknown CSI. Furthermore, $\boldsymbol{u}_B^k$ is the Gaussian distributed information bearing signal vector satisfying $\mathbb{E}\{\boldsymbol{u}_B^k \boldsymbol{u}_B^{k^H}\} = \boldsymbol{I}_{M_U}$, and $\boldsymbol{u}_J^{k,e}$ is transmitted by the dedicated jammers $\mathcal{J}_k$ satisfying $\mathbb{E}\{\boldsymbol{u}_J^{k,e} \boldsymbol{u}_J^{k,e^H}\} = \boldsymbol{I}_{M_E}$, while $\boldsymbol{W}_B^k \in \mathbb{C}^{(|\mathcal{B}_k| M_A) \times M_U}$ and $\boldsymbol{W}_J^{k,e} \in \mathbb{C}^{(|\mathcal{J}_k| M_A) \times M_E}$ are the normalized beamformers transmitting from the serving APs/embedded APs and from the dedicated jamming APs, respectively. Finally, $\boldsymbol{v}_B^k \in \mathbb{C}^{(|\mathcal{B}_k| M_A) \times 1}$ and $\boldsymbol{v}_J^k \in \mathbb{C}^{(|\mathcal{J}_k| M_A) \times 1}$ are the normalized independently distributed artificial noise vectors imposed on the embedded APs and the dedicated jamming APs, respectively, which follow the complex Gaussian distributions, i.e. $\boldsymbol{v}_B^k \sim \mathbb{CN}(\boldsymbol{0}, \boldsymbol{\Sigma}_B^k)$ and $\boldsymbol{v}_J^k \sim \mathbb{CN}(\boldsymbol{0}, \boldsymbol{\Sigma}_J^k)$. Herein, we have assumed $\text{Tr}\{\boldsymbol{\Sigma}_B^k\} = 1$ and $\text{Tr}\{\boldsymbol{\Sigma}_J^k\} = 1$.

In order to determine the involvement of APs, let us define $\boldsymbol{X} = [x_{j,k}]$ having a matrix of $(B \times K)$ elements represent the involvement status of AP j for a given UE k. For the dedicated jamming strategy, the variable is given by

$$x_{j,k} = \begin{cases} 1, & \textit{serving}, \\ -1, & \textit{jamming}, \\ 0, & \textit{otherwise}. \end{cases} \tag{7}$$

Accordingly, we have $\mathcal{B}_k = \{j | x_{j,k} = 1, j \in \mathcal{B}\}$, $\mathcal{J}_k = \{j | x_{j,k} = -1, j \in \mathcal{B}\}$. By contrast, for the embedded jamming strategy, the variable is given by

$$x_{j,k} = \begin{cases} 1, & \textit{serving \& jamming}, \\ 0, & \textit{otherwise}. \end{cases} \tag{8}$$

In this strategy, we have $\mathcal{B}_k = \mathcal{J}_k = \{j | x_{j,k} = 1, j \in \mathcal{B}\}$.

For convenience, we define $\boldsymbol{X}^k = \{x_{j,k}\}_{j \in \mathcal{B}}$, $\boldsymbol{W}_J^k = \{\boldsymbol{W}_J^{k,e}\}_{e \in \mathcal{E}}$, $\boldsymbol{W}^k = \{\boldsymbol{W}_B^k, \boldsymbol{W}_J^k\}$ and $\boldsymbol{v}^k = \{\boldsymbol{v}_B^k, \boldsymbol{v}_J^k\}$. Therefore, by substituting (5) and (6) into (3) and (4), the instantaneous achievable rate of UE k and of independent eavesdropper e in the secure user-centric cluster of UE k can be obtained as follows, respectively

$$R_k(\boldsymbol{X}^k, \boldsymbol{W}^k, \boldsymbol{v}^k) = \log \left| \boldsymbol{I}_{M_U} + \frac{(1-\bar{\gamma})p_t \boldsymbol{H}_1^{k^H} \boldsymbol{W}_B^k \boldsymbol{W}_B^{k^H} \boldsymbol{H}_1^k}{\boldsymbol{F}_k + \sigma^2 \boldsymbol{I}_{M_U}} \right|, \tag{9}$$

$$LR_{k,e}(\boldsymbol{X}^k, \boldsymbol{W}^k, \boldsymbol{v}^k) = \log \left| \boldsymbol{I}_{M_E} + \frac{(1-\bar{\gamma})p_t \boldsymbol{H}_2^{k,e^H} \boldsymbol{W}_B^k \boldsymbol{W}_B^{k^H} \boldsymbol{H}_2^{k,e}}{\boldsymbol{SF}_{k,e} + \sigma^2 \boldsymbol{I}_{M_E}} \right|, \tag{10}$$

where

$$\boldsymbol{F}_k = \begin{cases} \gamma p_t \boldsymbol{H}_1^{k^H} \boldsymbol{\Sigma}_B^k \boldsymbol{H}_1^k, & \textit{if} \;\; \alpha = 0, \beta = 0, \\ \sum_{e \in \mathcal{E}} p_t \boldsymbol{G}_1^{k^H} \boldsymbol{\Sigma}_J^k \boldsymbol{G}_1^k, & \textit{if} \;\; \alpha = 0, \beta = 1, \\ \boldsymbol{0}, & \textit{if} \;\; \alpha = 1, \beta = 0, \\ \sum_{e \in \mathcal{E}} p_t \boldsymbol{G}_1^{k^H} \boldsymbol{W}_J^{k,e} \boldsymbol{W}_J^{k.e^H} \boldsymbol{G}_1^k, & \textit{if} \;\; \alpha = 1, \beta = 1, \end{cases} \tag{11}$$

and

$$\boldsymbol{SF}_{k,e} = \begin{cases} \gamma p_t \boldsymbol{H}_2^{k,e^H} \boldsymbol{\Sigma}_B^k \boldsymbol{H}_2^{k,e}, & \textit{if} \;\; \alpha = 0, \beta = 0, \\ p_t \boldsymbol{G}_2^{k,e^H} \boldsymbol{\Sigma}_J^k \boldsymbol{G}_2^{k,e}, & \textit{if} \;\; \alpha = 0, \beta = 1, \\ \boldsymbol{0}, & \textit{if} \;\; \alpha = 1, \beta = 0, \\ p_t \boldsymbol{G}_2^{k,e^H} \boldsymbol{W}_J^{k,e} \boldsymbol{W}_J^{k,e^H} \boldsymbol{G}_2^{k,e}, & \textit{if} \;\; \alpha = 1, \beta = 1. \end{cases} \tag{12}$$

In order not to interfere with the useful signal, $\boldsymbol{W}_J^k$ and $\boldsymbol{v}^k$ have to be designed to let $\boldsymbol{F}_k = \boldsymbol{0}$ and maximize $\boldsymbol{SF}_{k,e}$ for the above scenarios. Since the eavesdroppers are independent of each other in overhearing the data transmission of the UEs, according to [36], the instantaneous achievable secrecy rate of UE k is formulated as

$$SR_k(\boldsymbol{X}^k, \boldsymbol{W}^k, \boldsymbol{v}^k) = \Bigg[R_k(\boldsymbol{X}^k, \boldsymbol{W}^k, \boldsymbol{v}^k) - \max_{e \in \mathcal{E}} LR_{k,e}(\boldsymbol{X}^k, \boldsymbol{W}^k, \boldsymbol{v}^k) \Bigg]^+ . \tag{13}$$

Naturally, both the rate and the secrecy rate are related not only to the value of the variable $\boldsymbol{X}^k$, but also to the choice of $\boldsymbol{W}^k$ and $\boldsymbol{v}^k$.

D. Power Consumption Model

From a secrecy-energy-efficiency[1] perspective, it is desirable to put the AP into the *sleep* mode when it is neither a serving AP nor a jamming AP for any UE, otherwise into the *awake* state. Hence, we can let $\text{sgn}\left(\sum_k |x_{j,k}|\right)$ denote the state of AP j, and then the number of awake APs is represented as $\sum_j \text{sgn}\left(\sum_k |x_{j,k}|\right)$. As far as the total power consumption is concerned, it is constitued by the total transmit power and the total static power. According to [37] [38], the power consumption of AP j can be modelled as

$$P_j = \begin{cases} \sum_k |x_{j,k}| \Delta_p p_t + M_A P_W, & \textit{if} \; \text{sgn}(\sum_k |x_{j,k}|) = 1, \\ M_A P_S, & \textit{if} \; \text{sgn}(\sum_k |x_{j,k}|) = 0, \end{cases} \tag{14}$$

where P_W and P_S are the static power consumption per antenna in the awake state and the asleep state, respectively, while Δ_p is the slope of the load-dependent power consumption. Therefore, the total power consumption (i.e. $\sum_j P_j$) can be represented as

$$P_T(\boldsymbol{X}) = \sum_{j \in \mathcal{B}} \sum_{k \in \mathcal{K}} |x_{j,k}| \Delta_p p_t + \sum_{j \in \mathcal{B}} \text{sgn}(\sum_{k \in \mathcal{K}} |x_{j,k}|) \times M_A P_W + \left(B - \sum_{j \in \mathcal{B}} \text{sgn}(\sum_{k \in \mathcal{K}} |x_{j,k}|) \right) M_A P_S, \tag{15}$$

which is related to the involvement state of APs in each secure user-centric cluster. In the following section, we will formulate our design problem and introduce the proposed solution framework.

III. Problem Formulation and Proposed Framework

This paper aims for designing and optimizing the secure user-centric clustering in UDNs from the perspective of secrecy-energy-efficiency. Although having more serving/jamming APs in both strategies will potentially enhance both the user-rate and the secrecy rate, the energy consumption of the system may also be increased due to the increased number of awake APs. The system-wide overall secrecy-energy-efficiency of the system, which is defined formally as the aggregated secrecy rate over the total power consumption, given by

$$SEE = \frac{\sum_{k \in \mathcal{K}} SR_k(\boldsymbol{X}^k, \boldsymbol{W}^k, \boldsymbol{v}^k)}{P_T(\boldsymbol{X})}. \tag{16}$$

In other words, the goal of our paper is to maximize the secrecy-energy-efficiency by jointly designing the secure transmission scheme and the secure user-centric clustering, while satisfying both the TQoS constraint and the SQoS constraint. Accordingly, our problem can be formulated as

$$\boldsymbol{\mathcal{P}0}: \max_{\boldsymbol{X}, \{\boldsymbol{W}^k\}_{k \in \mathcal{K}}, \{\boldsymbol{v}^k\}_{k \in \mathcal{K}}} \frac{\sum_{k \in \mathcal{K}} SR_k(\boldsymbol{X}^k, \boldsymbol{W}^k, \boldsymbol{v}^k)}{P_T(\boldsymbol{X})} \tag{17a}$$

$$\text{s.t.} \;\; R_k(\boldsymbol{X}^k, \boldsymbol{W}^k, \boldsymbol{v}^k) \geq \overline{R}_k, \; \forall k, \tag{17b}$$

$$SR_k(\boldsymbol{X}^k, \boldsymbol{W}^k, \boldsymbol{v}^k) \geq \overline{SR}_k, \; \forall k, \tag{17c}$$

$$(7) \text{ or } (8). \tag{17d}$$

where $\overline{R}_k$ and $\overline{SR}_k$ are the minimum TQoS and SQoS requirements of UE k, respectively. To elaborate a litter further, the third constraint is (7), if $\beta = 1$ and it is (8), if $\beta = 0$. It can be observed that problem $\boldsymbol{\mathcal{P}0}$ is actually an NP-hard mixed integer non-linear programming problem, which consists of the integer variable $\boldsymbol{X}$ and continuous variable sets $\{\boldsymbol{W}^k\}_{k \in \mathcal{K}}$, $\{\boldsymbol{v}^k\}_{k \in \mathcal{K}}$. Owing to the fact that this objective is too complex to be described by a closed-form expression of $\boldsymbol{X}$, seeking an optimum solution is infeasible. Therefore, our proposed framework independently considers the two problems: *the secure transmission* and *the secure user-centric clustering*.

To elaborate, we first have to design different feasible secure transmission schemes according to the availability or absence of the eavesdropper CSI, relying on the beamforming and on the artificial noise based approaches, respectively. Next,

[1] This is defined as the aggregated secrecy rate normalized by the total power consumption.

given these secure transmission schemes, we consider how to construct the secure user-centric clusters. In other words, our target is to find each UE's serving AP set and jamming AP set with the goal of maximizing the secrecy-energy-efficiency, while satisfying the minimum TQoS and SQoS constraints. Nevertheless, the exhaustive search for the optimum solution remains infeasible due to the high density of the network. Fortunately, we notice that the constraints (17b) and (17c) can be decoupled for each UE. Thus, we can construct the secure user-centric clusters in a distributed way, which is capable of reducing the computational complexity. The basic idea is that we first select some APs acting as serving and/or jamming APs for satisfying the TQoS and SQoS, and then determine the remaining AP's involvement according to the secrecy-energy-efficiency metric, which may be viewed as a greedy heuristic algorithm. The proposed secure transmission schemes and secure user-centric clustering solutions will be detailed in the following sections, respectively.

IV. Secure Transmission Schemes Design

In this section, we consider our secure transmission schemes based on both strategies both with and without known CSI of the eavesdroppers, respectively. Since power allocation is not considered in this context, the formulated problem $\boldsymbol{\mathcal{P}0}$ can be transformed and decoupled into K subproblems of maximizing the secrecy rate by designing $\boldsymbol{W}^k$ and $\boldsymbol{v}^k$ in (13). Then the k-th subproblem designed for the secure user-centric cluster of UE k can be represented as

$$\boldsymbol{\mathcal{P}1}: \arg \max_{\boldsymbol{W}^k, \boldsymbol{v}^k} \{SR_k(\boldsymbol{W}^k, \boldsymbol{v}^k)\}. \tag{18}$$

A. With Unknown Eavesdropper CSI ($\alpha = 0$)

In this case, the signals of the serving APs/embedded APs and dedicated jamming APs are $\boldsymbol{s}_B^k = \sqrt{1-\bar{\gamma}}\boldsymbol{W}_B^k\boldsymbol{u}_B^k + \sqrt{\bar{\gamma}}\boldsymbol{v}_B^k$ and $\boldsymbol{s}_J^{k,e} = \beta\boldsymbol{v}_J^k$, respectively. Thus, the problem becomes the design of the beamformer $\boldsymbol{W}_B^k$ and of the artificial noise $\boldsymbol{v}_B^k$ or $\boldsymbol{v}_J^k$. In this paper, for simplicity, we opt for the maximum-ratio-transmission (MRT) based beamformer [39], i.e. $\boldsymbol{W}_B^k = \boldsymbol{H}_1^k/\sqrt{Tr\{\boldsymbol{H}_1^k{\boldsymbol{H}_1^k}^H\}}$, so as to maximize the rate. Furthermore, the artificial noise at the dedicated jamming APs $\boldsymbol{v}_J^k$ or at the embedded APs $\boldsymbol{v}_B^k$ is designed for degrading the eavesdroppers' channel, without affecting the channel of intended UE k, thus allowing perfectly secure communication.

Consider the dedicated jamming strategy as an example. According to [24], $\boldsymbol{v}_J^k$ is chosen for ensuring that $\boldsymbol{v}_J^k$ lies in the null space of ${\boldsymbol{G}_1^k}^H$, i.e. satisfying ${\boldsymbol{G}_1^k}^H\boldsymbol{v}_J^k = \boldsymbol{0}, \forall k$. In order to maximize the secrecy rate expressed in (18), $\boldsymbol{v}_J^k$ is chosen to be i.i.d. Gaussian random vectors in the null space of ${\boldsymbol{G}_1^k}^H$, given by

$$\boldsymbol{v}_J^k = \boldsymbol{\Gamma}_J^k\boldsymbol{t}_J^k, \tag{19}$$

where $\boldsymbol{\Gamma}_J^k = Null\{{\boldsymbol{G}_1^k}^H\}$ and the elements of $\boldsymbol{t}_J^k$ are i.i.d. Gaussian with zero mean and unit variance. Note that the power of artificial noise is normalized, hence we formulate the normalized artificial noise of dedicated jamming APs as $\boldsymbol{v}_J^k = \boldsymbol{\Gamma}_J^k\boldsymbol{t}_J^k/\sqrt{Tr\{\boldsymbol{\Gamma}_J^k{\boldsymbol{\Gamma}_J^k}^H\}}$. Similarly, we define $\boldsymbol{\Gamma}_B^k = Null\{{\boldsymbol{H}_1^k}^H\}$ and the elements of $\boldsymbol{t}_B^k$ are i.i.d. Gaussian with zero-mean and unit-variance, while the artificial noise of embedded APs is denoted by $\boldsymbol{v}_B^k = \boldsymbol{\Gamma}_B^k\boldsymbol{t}_B^k/\sqrt{Tr\{\boldsymbol{\Gamma}_B^k{\boldsymbol{\Gamma}_B^k}^H\}}$.

Accordingly, the rate and the secrecy rate of UE k are given by

$$R_k = \log\left|\boldsymbol{I}_{M_U} + \frac{(1-\bar{\gamma})p_t{\boldsymbol{H}_1^k}^H\boldsymbol{W}_B^k{\boldsymbol{W}_B^k}^H\boldsymbol{H}_1^k}{\sigma^2\boldsymbol{I}_{M_U}}\right|, \tag{20}$$

$$\begin{aligned} SR_k = [R_k - \\ \max_{e\in\mathcal{E}}\log\left|\boldsymbol{I}_{M_E} + \frac{(1-\bar{\gamma})p_t{\boldsymbol{H}_2^{k,e}}^H\boldsymbol{W}_B^k{\boldsymbol{W}_B^k}^H\boldsymbol{H}_2^{k,e}}{\boldsymbol{SF}_{k,e} + \sigma^2\boldsymbol{I}_{M_E}}\right|]^+,\end{aligned} \tag{21}$$

where

$$\boldsymbol{SF}_{k,e} = \begin{cases} \gamma p_t{\boldsymbol{H}_2^{k,e}}^H\boldsymbol{\Gamma}_B^k{\boldsymbol{\Gamma}_B^k}^H\boldsymbol{H}_2^{k,e}/\mathrm{Tr}\{\boldsymbol{\Gamma}_B^k{\boldsymbol{\Gamma}_B^k}^H\}, \\ \qquad\qquad \textit{if} \;\; \alpha = 0, \beta = 0, \\ p_t{\boldsymbol{G}_2^{k,e}}^H\boldsymbol{\Gamma}_J^k{\boldsymbol{\Gamma}_J^k}^H\boldsymbol{G}_2^{k,e}/\mathrm{Tr}\{\boldsymbol{\Gamma}_J^k{\boldsymbol{\Gamma}_J^k}^H\}, \\ \qquad\qquad \textit{if} \;\; \alpha = 0, \beta = 1. \end{cases} \tag{22}$$

B. With Known Eavesdropper CSI ($\alpha = 1$)

With known CSI of the eavesdroppers, the dedicated jamming APs or embedded APs can configure their beamformer for suppressing or eliminating eavesdropper's signal, relying on both the CSI of the intended UE, i.e. $\boldsymbol{G}_1^k$, and of the eavesdroppers, i.e. $\boldsymbol{G}_2^k$. Then we have $\boldsymbol{s}_B^k = \boldsymbol{W}_B^k\boldsymbol{u}_B^k$ and $\boldsymbol{s}_J^{k,e} = \beta\boldsymbol{W}_J^{k,e}\boldsymbol{u}_J^{k,e}$, depending on the strategy selection, and hence the problem becomes how to design $\boldsymbol{W}_B^k$ and $\boldsymbol{W}_J^{k,e}$. Nevertheless, the targets of dedicated jamming beamformer and embedded beamformer are different, hence leading to different designs.

1) Dedicated Jamming Strategy ($\beta = 1$): The beamformer optimization of the dedicated jamming APs has the following two goals: i) the received signal power of the intended UE is zero; ii) the interference imposed on the eavesdroppers is maximized. For the sake of fairness, we also opt for the MRT beamformer for serving the APs, i.e. we have $\boldsymbol{W}_B^k = \boldsymbol{H}_1^k/\sqrt{Tr\{\boldsymbol{H}_1^k{\boldsymbol{H}_1^k}^H\}}$. Accordingly, the k-th subproblem $\boldsymbol{\mathcal{P}1}$ derived for eavesdropper e can be represented as

$$\max_{\boldsymbol{W}_J^{k,e}} \;\; {\boldsymbol{G}_2^{k,e}}^H\boldsymbol{W}_J^{k,e}{\boldsymbol{W}_J^{k,e}}^H\boldsymbol{G}_2^{k,e} \tag{23a}$$

$$\text{s.t.} \;\; {\boldsymbol{G}_1^k}^H\boldsymbol{W}_J^{k,e} = \boldsymbol{0}. \tag{23b}$$

It has been found that the optimal solution $\boldsymbol{W}_J^{k,e}$ is the null-steering beamforming [40], which is based on the orthogonal projection of $\boldsymbol{G}_2^{k,e}$ onto the null space of $\boldsymbol{G}_1^k$, given by[2]

$$\boldsymbol{W}_J^{k,e} = \frac{\left[\boldsymbol{I} - \Pi_{\boldsymbol{G}_1^k}\right]\boldsymbol{G}_2^{k,e}}{\sqrt{Tr\{\left[\boldsymbol{I} - \Pi_{\boldsymbol{G}_1^k}\right]\boldsymbol{G}_2^{k,e}{\boldsymbol{G}_2^{k,e}}^H\left[\boldsymbol{I} - \Pi_{\boldsymbol{G}_1^k}\right]^H\}}}. \tag{24}$$

[2] Throughout, $\Pi_{\boldsymbol{A}} = \boldsymbol{A}(\boldsymbol{A}^H\boldsymbol{A})^{-1}\boldsymbol{A}^H$ denotes the orthogonal projection matrix onto the subspace spanned by the columns of $\boldsymbol{A}$.

Thereby, the rate and the secrecy rate of UE k are given by

$$R_k = \log\left|\boldsymbol{I}_{M_U} + \frac{p_t {\boldsymbol{H}_1^k}^H \boldsymbol{W}_B^k {\boldsymbol{W}_B^k}^H \boldsymbol{H}_1^k}{\sigma^2 \boldsymbol{I}_{M_U}}\right|, \tag{25}$$

$$SR_k = \Bigg[R_k - \max_{e\in\mathcal{E}} \log\left|\boldsymbol{I}_{M_E} + \frac{p_t {\boldsymbol{H}_2^{k,e}}^H \boldsymbol{W}_B^k {\boldsymbol{W}_B^k}^H \boldsymbol{H}_2^{k,e}}{p_t {\boldsymbol{G}_2^{k,e}}^H \boldsymbol{W}_J^{k,e} {\boldsymbol{W}_J^{k,e}}^H \boldsymbol{G}_2^{k,e} + \sigma^2 \boldsymbol{I}_{M_E}}\right|\Bigg]^+. \tag{26}$$

2) Embedded Jamming Strategy ($\beta = 0$): In contrast to the dedicated jamming strategy, the beamformer of embedded APs is designed in order to simultaneously achieve a pair of goals: i) the received signal power of the intended UE is maximized; ii) the leakage to the eavesdroppers is zero. In this case, we only have to optimize $\boldsymbol{W}_B^k$ as a result of the dual functionality of the embedded APs. Hence, the k-th subproblem $\boldsymbol{\mathcal{P}1}$ can be rewritten as

$$\max_{\boldsymbol{W}_B^k} \quad {\boldsymbol{H}_1^k}^H \boldsymbol{W}_B^k {\boldsymbol{W}_B^k}^H \boldsymbol{H}_1^k \tag{27a}$$

$$\text{s.t.} \quad {\boldsymbol{H}_2^k}^H \boldsymbol{W}_B^k = \boldsymbol{0}. \tag{27b}$$

Note that although we have $\boldsymbol{H}_1^k = \boldsymbol{G}_1^k$ in this strategy, this problem is completely different from the problem in (23). However, we can still adopt the null-steering beamforming, but it is an orthogonal projection of $\boldsymbol{H}_1^k$ onto the null space of $\boldsymbol{H}_2^k$, given by

$$\boldsymbol{W}_B^k = \frac{\left[\boldsymbol{I} - \Pi_{\boldsymbol{H}_2^k}\right] \boldsymbol{H}_1^k}{\sqrt{Tr\{\left[\boldsymbol{I} - \Pi_{\boldsymbol{H}_2^k}\right] \boldsymbol{H}_1^k {\boldsymbol{H}_1^k}^H \left[\boldsymbol{I} - \Pi_{\boldsymbol{H}_2^k}\right]^H\}}}. \tag{28}$$

Thus, the eavesdropper's signal is completely eliminated, and then the rate as well as the secrecy rate of UE k are given by

$$R_k = SR_k = \log\left|\boldsymbol{I}_{M_U} + \frac{p_t {\boldsymbol{H}_1^k}^H \boldsymbol{W}_B^k {\boldsymbol{W}_B^k}^H \boldsymbol{H}_1^k}{\sigma^2 \boldsymbol{I}_{M_U}}\right|. \tag{29}$$

Given these secure transmission schemes, the secure user-centric clustering problem is discussed in the next section.

V. Secure User-centric Clustering Design

The goal of this section is to design secure user-centric clustering, i.e. to determine the involvement of APs for each UE, relying on the previously mentioned secure transmission schemes. With the objective of maximizing the secrecy-energy-efficiency, the secure user-centric clustering problem can be formulated as

$$\boldsymbol{\mathcal{P}2}: \max_{\boldsymbol{X}} \quad \frac{\sum_{k\in\mathcal{K}} SR_k(\boldsymbol{X}^k)}{P_T(\boldsymbol{X})} \tag{30a}$$

$$\text{s.t.} \quad R_k(\boldsymbol{X}^k) \geq \overline{R}_k,\ \forall k, \tag{30b}$$

$$SR_k(\boldsymbol{X}^k) \geq \overline{SR}_k,\ \forall k, \tag{30c}$$

$$(7) \text{ or } (8). \tag{30d}$$

where the constraint (30d) depends on the specific strategy adopted. It can be observed that problem (30) is a combinatorial optimization problem and the exhaustive search is infeasible due to the excessive computational complexity. At the time of writing, we have no existing algorithms to solve this kind of NP-hard problem, even if the discrete variables are relaxed to be continuous variables. This is due to the fact that the objective function (30a) is an extremely complex function of the variable $\boldsymbol{X}$, which cannot be expressed in closed-form. Nevertheless, as mentioned above, we notice that the constraints (30b) and (30c) can be decoupled for each UE. Motivated by this, we can construct our secure user-centric clusters in a distributed way.

Note that, we differentiate the expression of SR_k with/without the eavesdropper's CSI. For the former case, the secrecy rate is still formulated as (13). For the latter case, we consider the secure user-centric clustering design based on the maximum ergodic rate of the eavesdroppers over their average CSI. Then, the minimum ergodic secrecy rate of UE k is given by (31).

Before introducing the detailed algorithms, the involvement of APs can be naturally determined according to the coverage distance, which is a clean and direct criterion. In general, the cooperation of close-by serving APs contributes to the UE's increased rate. Hence, in this paper we adopt the coverage distance as the criterion of selecting APs, so as to maximize the benefits of AP cooperation, and then determine the involvement of the selected APs for a given UE according to the rate/secrecy rate/secrecy-energy-efficiency metrics. From a practical point of view, we also assume that each AP can only serve those UEs roaming within the coverage distance threshold d_t from the UEs. Owing to the fact that the algorithm of our embedded jamming strategy is simpler than that of the dedicated jamming strategy, next we introduce the former one first.

A. Embedded Jamming Strategy

In the embedded jamming strategy, the secure user-centric clustering problem becomes identical to determine the involvement of embedded APs. We conceive a greedy algorithm for our embedded jamming strategy, where each UE first attempts to involve its nearest embedded APs to satisfy the constraints of both (30b) and (30c), and then exhaustively searches through the remaining embedded APs within d_t to judge whether it does or does not contribute to the overall secrecy-energy-efficiency. To be specific, the greedy algorithm consists of a pair of search processes:

i) Firstly, for any given UE k, if the rate R_k does not satisfy (30b) and the nearest uninvolved AP j^* within d_t contributes to the rate, then AP j^* will be incorporated into the serving AP set $\mathcal{B}_k$, i.e. $\mathcal{B}_k = \mathcal{B}_k \cap j^*$. If the rate R_k satisfies (30b) but the secrecy rate SR_k does not satisfy (30c), the nearest uninvolved AP j^* within d_t will be judged whether it does or does not contribute to the secrecy rate as well as satisfy (30b). If it does, AP j^* above will be incorporated into the serving AP set $\mathcal{B}_k$. The first search process will stop, when all UEs achieve

$$SR_k=\left\{R_k-\max_{e\in\mathcal{E}}\mathbb{E}_{\boldsymbol{H}_2^{k,e},\boldsymbol{G}_2^{k,e}}\left[\log\left|\boldsymbol{I}_{M_E}+\frac{(1-\bar{\gamma})p_t{\boldsymbol{H}_2^{k,e}}^H\boldsymbol{W}_B^k{\boldsymbol{W}_B^k}^H\boldsymbol{H}_2^{k,e}}{\boldsymbol{SF}_{k,e}+\sigma^2\boldsymbol{I}_{M_E}}\right|\right]\right\}^+. \tag{31}$$

the TQoS and SQoS target, or all embedded APs within d_t of each UE are already in its serving AP set.

ii) Secondly, if there exists any remaining embedded AP j^* within d_t, which is not yet connected to the given UE k, i.e. $x_{j^*,k}=0$, UE k continues to search the nearest embedded AP within d_t and judges whether it does or does not contribute to the secrecy-energy-efficiency, while still meeting both the requirements of TQoS and SQoS. If it does, it is incorporated into $\mathcal{B}_k$, otherwise it is not. The second search process will stop, when all embedded APs within d_t of all UEs have been considered.

We summarize the above greedy search in Algorithm 1.

Algorithm 1 A greedy algorithm for secure user-centric clustering under embedded jamming strategy

```
Initialize: $\boldsymbol{X}=\mathbf{0}$, $\mathcal{B}_k=\emptyset$ $(\forall k)$;
Calculate $\{d_{j,k}\}$ $(\forall j,\forall k)$;
for all $k\in\mathcal{K}$ do
    Set $\mathcal{L}_k=\{j|\ d_{j,k}\le d_t,\ j\in\mathcal{L}\}$;
    repeat
        Find $j^*=\arg\min_{j\in\mathcal{L}_k}\{d_{j,k}\}$ satisfying $x_{j^*,k}=0$;
        if $R_k<\overline{R}_k$ & &$R_k(\mathcal{B}_k\cap j^*)>R_k(\mathcal{B}_k)$ then
            $\mathcal{B}_k\leftarrow\mathcal{B}_k\cap j^*$, $x_{j^*,k}\leftarrow 1$, $\mathcal{L}_k\leftarrow\mathcal{L}_k\setminus j^*$;
        else if $SR_k<\overline{SR}_k$&&$SR_k(\mathcal{B}_k\cap j^*)>SR_k(\mathcal{B}_k)$& &$R_k(\mathcal{B}_k\cap j^*)\ge\overline{R}_k$ then
            $\mathcal{B}_k\leftarrow\mathcal{B}_k\cap j^*$, $x_{j^*,k}\leftarrow 1$, $\mathcal{L}_k\leftarrow\mathcal{L}_k\setminus j^*$;
        end if
    until $(R_k\ge\overline{R}_k\ \ \&\&\ SR_k\ge\overline{SR}_k)\ ||\ \mathcal{L}_k==\emptyset$
end for
for all $k\in\mathcal{K}$ do
    repeat
        Find $j^*=\arg\min_{j\in\mathcal{L}_k}\{d_{j,k}\}$ satisfying $x_{j^*,k}=0$;
        if $SEE(\mathcal{B}_k\cap j^*)>SEE(\mathcal{B}_k)$ & &$R_k(\mathcal{B}_k\cap j^*)\ge\overline{R}_k$ & &$SR_k(\mathcal{B}_k\cap j^*)\ge\overline{SR}_k$ then
            $\mathcal{B}_k\leftarrow\mathcal{B}_k\cap j^*$, $x_{j^*,k}\leftarrow 1$;
        end if
        $\mathcal{L}_k\leftarrow\mathcal{L}_k\setminus j^*$;
    until $\mathcal{L}_k==\emptyset$
end for
Output: $\boldsymbol{X}$
```

B. Dedicated Jamming Strategy

In the dedicated jamming strategy, the secure user-centric clustering problem turns into that of selecting each UE's distinctive serving AP set and jamming AP set. Similarly, we can also construct the secure user-centric clusters in a distributed way. Our basic principle is that the close-by APs in the secure user-centric cluster act as serving APs to satisfy the TQoS, while the farther APs in the secure user-centric cluster serve as jamming APs to maintain the SQoS. This may be referred to as the 'rate-first principle'. As for the involvement of serving APs, their increased number is capable of contributing to a higher user rate, due to the user-centric design. However, the secrecy rate may be deteriorated with the involvement of jamming APs according to the locations of the eavesdroppers. We also propose a greedy algorithm, which consists of two search processes. The procedure of the algorithm is described as follows:

Algorithm 2 A greedy algorithm for secure user-centric clustering under dedicated jamming strategy

```
Initialize: $\boldsymbol{X}=\mathbf{0}$, $\mathcal{B}_k=\emptyset(\forall k)$, $\mathcal{J}_k=\emptyset(\forall k)$;
Calculate $\{d_{j,k}\}$, $(\forall j,\forall k)$;
for all $k\in\mathcal{K}$ do
    Set $\mathcal{L}_k=\{j|\ d_{j,k}\le d_t,\ j\in\mathcal{L}\}$;
    repeat
        Find $j^*=\arg\min_{j\in\mathcal{L}_k}\{d_{j,k}\}$ satisfying $x_{j^*,k}=0$;
        if $R(k)<\overline{R}_k$ then
            $\mathcal{B}_k\leftarrow\mathcal{B}_k\cap j^*,\ \ x_{j^*,k}\leftarrow 1$, $\mathcal{L}_k\leftarrow\mathcal{L}_k\setminus j^*$;
        else if $SR_k<\overline{SR}_k$ & &$SR_k(\mathcal{J}_k\cap j^*)>SR_k(\mathcal{J}_k)$ then
            $\mathcal{J}_k\leftarrow\mathcal{J}_k\cap j^*,\ \ x_{j^*,k}\leftarrow -1$, $\mathcal{L}_k\leftarrow\mathcal{L}_k\setminus j^*$;
        end if
    until $(R_k\ge\overline{R}_k\ \ \&\&\ SR_k\ge\overline{SR}_k)\ ||\ \mathcal{L}_k==\emptyset$
end for
for all $k\in\mathcal{K}$ do
    repeat
        Find $j^*=\arg\min_{j\in\mathcal{L}_k}\{d_{j,k}\}$ satisfying $x_{j^*,k}=0$;
        if $\max\{SEE(\mathcal{B}_k\ \cap\ j^*),SEE(\mathcal{J}_k\ \cap\ j^*)\}\ >\ SEE(\mathcal{B}_k,\mathcal{J}_k)$ then
            if $SEE(\mathcal{B}_k\cap j^*)\ge SEE(\mathcal{J}_k\cap j^*)$&&$SR_k(\mathcal{B}_k\cap j^*)\ge\overline{SR}_k$ then
                $\mathcal{B}_k\leftarrow\mathcal{B}_k\cap j^*$, $x_{j^*,k}\leftarrow 1$;
            else if $SEE(\mathcal{J}_k\cap j^*)\ >\ SEE(\mathcal{B}_k\cap j^*)$ & &$SR_k(\mathcal{J}_k\cap j^*)\ge\overline{SR}_k$ then
                $\mathcal{J}_k\leftarrow\mathcal{J}_k\cap j^*$, $x_{j^*,k}\leftarrow -1$;
            end if
        end if
        $\mathcal{L}_k\leftarrow\mathcal{L}_k\setminus j^*$;
    until $\mathcal{L}_k==\emptyset$
end for
Output: $\boldsymbol{X}$
```

i) Firstly, for any given UE k, if the rate R_k does not satisfy (30b), the nearest uninvolved AP j^* within d_t will be incorporated acting as the serving AP, i.e. we have $\mathcal{B}_k=\mathcal{B}_k\cap j^*$. If the rate satisfies (30b) but the secrecy rate does not satisfy (30c), the nearest uninvolved AP j^* within d_t will be judged depending on whether contributes to the secrecy rate. If it does, AP j^* above will join the jamming

AP set, i.e. we have $\mathcal{J}_k = \mathcal{J}_k \cap j^*$. This search process will be repeated until all UEs achieved both the target TQoS and SQoS, or all APs within d_t of each UE are already in its serving AP set or jamming AP set.

ii) Secondly, if there are any remaining uninvolved APs j^* within d_t for a given UE k satisfying $x_{j^*,k} = 0$, UE k continues to judge the associated contribution to the secrecy-energy-efficiency assuming that it is acting as the serving AP or the jamming AP. If AP j^* above to be included in the serving AP set will actually obtain a higher secrecy-energy-efficiency than upon being included in the jamming AP set, while still satisfying the SQoS target, it is selected as a serving AP, and vice versa. If the current secrecy-energy-efficiency remains at its maximum value during the search, the serving AP set and jamming AP set remain unchanged. This search process will be repeated until all APs within d_t have been considered by all UEs.

We summarize the above search process of our greedy technique in Algorithm 2.

VI. Numerical Results

In this section, we characterize the performance of our secure user-centric clustering designed for energy efficient UDNs under the above scenarios by our numerical results. For simplicity but without loss of generality, we focus our attention on a squared area of S [km^2], wherein the locations of APs, UEs and eavesdroppers are generated independently by homogeneous PPPs, each having a density of λ_A [APs/km^2], λ_U [UEs/km^2] and λ_E [eavesdroppers/km^2], respectively. The default simulation parameters are listed in TABLE II and 10 000 Monte Carlo drops are generated for recording all results.

We validate the efficiency of our proposed secure user-centric clustering architecture by simulations, and evaluate the performance of our proposed secure user-centric clustering algorithms, both with (w) and without (w/o) the eavesdropper CSI, which are denoted by the legends of 'Embedded-w/o CSI (hexagon)', 'Embedded-w CSI (circle)', 'Dedicated-w/o CSI (diamond)' and 'Dedicated-w CSI (square)', respectively. As far as the performance metric is concerned, in this paper, we define the per UE average rate (PAR) as[3] $\sum_{k\in\mathcal{K}} R_k/|\mathcal{K}|$, and per UE average secrecy rate (PASR) as $\sum_{k\in\mathcal{K}} SR_k/|\mathcal{K}|$. Additionally, we also compare the total power consumption and the secrecy-energy-efficiency, which are defined in (15) and (16), respectively.

TABLE II: Simulation Parameters

Area Coverage Area	$S = 0.2$ km $\times$ 0.2 km
AP Coverage Area Threshold	$d_t = 0.05$ km
RB Bandwidth	180kHz
Path Loss Model [35]	$\theta_L = 2.09$, $\theta_{NL} = 3.75$, $D_L = 10^{-10.38}$, $D_{NL} = 10^{-14.54}$, $\phi_1 = 0.156$ km, $\phi_2 = 0.03$ km, $\overline{d} = \phi_1/\ln(10)$, $\psi = 0.0085$ km
Noise Power Density (5 dB figure)	-174 dBm/Hz
AP Transmit Power Density	-40 dBm/Hz
Power Consumption Model [38]	$\Delta_p = 4$, $P_W = 6.8$ w, $P_S = 4.3$ w
Fraction of Transmit Power for Artificial Noise	$\gamma = 0.5$
Number of Antennas	$M_A = 8$, $M_U = 2$, $M_E = 2$
Density	$\lambda_A = 5 \times 10^3/\text{km}^2$, $\lambda_U = 3 \times 10^3/\text{km}^2$, $\lambda_E = 300/\text{km}^2$
TQoS constraint	$\overline{R}_k = 45$ b/s/Hz, $\forall k$
SQoS constraint	$\overline{SR}_k = 40$ b/s/Hz, $\forall k$

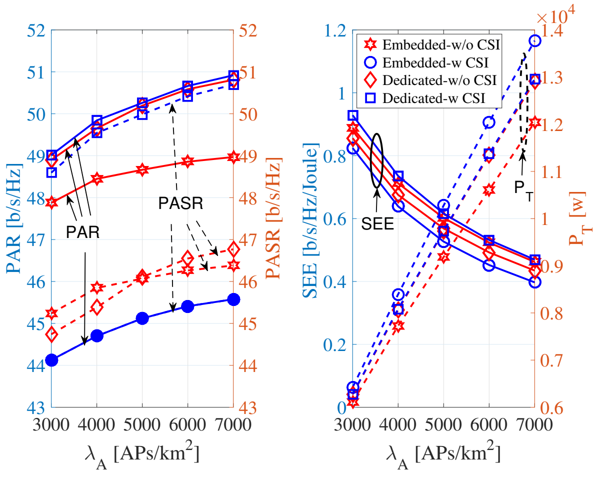


Fig. 2: Impact of AP density λ_A on the performance. (The filled marker indicates that the PAR and PASR performance curves coincide with each other.)

A. Impact of AP density on the performance

Fig. 2 shows the impact of AP density on the various performance metrics. Firstly, observe at the left of Fig. 2, that the PARs of all the solutions increase gradually, when the AP density is increased. This is due to the fact that denser APs may have more and nearer APs with better channel quality to be involved as serving APs both for satisfying the TQoS constraint and for maximizing the secrecy-energy-efficiency. The PASR follows a similar increasing trend to that of the corresponding PAR for all the solutions. The underlying reason is that denser APs increase the PAR and their jamming capability can cope better with the increased information leakage to the eavesdroppers. Specifically, although the leakage of information may be increased upon increasing the PAR, the jamming capability of the increased number of embedded APs involved is also improved, whilst the dedicated jammers enlisted for

[3] Herein, $\mathcal{K}$ is the actual UE set generated by PPP.

imposing interference on the eavesdroppers are capable of satisfying the minimum SQoS requirement. Additionally, it is worth noting that the PAR and the PASR of the embedded jamming strategy relying on the CSI are identical, since only this strategy is capable of completely avoiding any leakage of the desired signals via our beamformer design. Having said that, this can only be achieved at the expense of a lower PAR and PASR.

Next, we compare these solutions at the left of Fig. 2. Firstly, we observe that the pair of dedicated jamming strategy based solutions outperform both embedded jamming strategy based solutions in terms of their PAR. The underlying reason for this is that the embedded APs have to dedicate a certain fraction of their transmit power to guarantee secure transmission. This specific fraction is fixed in the scenario operating without CSI knowledge, while it depends on the CSI of the eavesdroppers in the scenario relying on it, so as to completely eliminate any information leakage. Secondly, it can be seen that the 'Dedicated- w CSI (square)' solution achieves the highest PASR amongst all the solutions, which is an explicit benefit of the PAR performance and of the jamming capability relying on the CSI knowledge.

Observe at the right of Fig. 2 that there is a significant increase in total power consumption as the AP density increases, mainly because of the increased total static power consumption of the asleep APs. This rate of increase is much faster than the potentially increased aggregated secrecy rate, hence the secrecy-energy-efficiency is significantly reduced for all the solutions, when the APs become denser. However, it is noteworthy that in the scenario operating without the CSI, the embedded jamming strategy exhibits a higher secrecy-energy-efficiency than the dedicated jamming strategy. The underlying reason behind this trend is that the number of awake APs in the 'Dedicated-w/o CSI (diamond)' is higher than that of the 'Embedded-w/o CSI (hexagon)' solution, which leads to a higher total power consumption and hence to a reduced secrecy-energy-efficiency. By contrast, in the scenario exploiting the CSI, the dedicated jamming strategy outperforms the embedded jamming strategy in terms of its secrecy-energy-efficiency. This is due to the fact that the dedicated jamming strategy allows the UE to involve the serving APs of other user-centric clusters for acting as its dedicated jammers for achieving energy savings. As a benefit of the above PAR and PASR trends, the superiority of the dedicated jamming strategy in the scenario relying on the CSI becomes plausible.

B. Impact of UE density on the performance

Fig. 3 plots the performance with regard to various UE densities. We first observe from the left illustration of Fig. 3 that upon increasing the UE density, all the solutions have an either near-constant or slightly increased PAR and PASR, which confirms the efficiency of our proposed secure user-centric clustering architecture to guarantee both the target TQoS and SQoS for each UE. Furthermore, we can see that the PAR and PASR superiority of the 'Dedicated-w CSI (square)' solution has been maintained, regardless of the UE density.

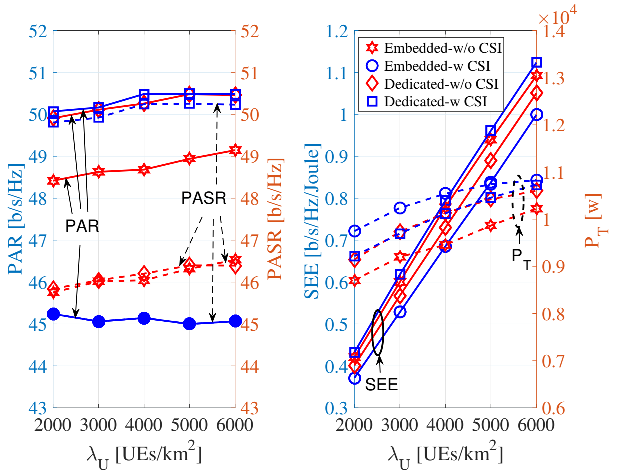


Fig. 3: Impact of UE density λ_U on the performance. (The filled marker indicates that the PAR and PASR performance curves coincide with each other.)

At the right of Fig. 3, we observe that the overall secrecy-energy-efficiency exhibits an increasing trend upon increasing the UE density. This is due to the fact that the PASR remains either near-constant or slightly increase upon increasing the UE density, hence the higher the number of UEs, the higher the aggregated secure rate becomes. This increase is much faster than the increased power consumption, when involving more awake APs for satisfying the increased number of UEs. Furthermore, it is seen again that the embedded jamming strategy operating without the CSI exhibits a higher secrecy-energy-efficiency than the dedicated jamming strategy operating without the CSI, whilst the dedicated jamming strategy relying on the CSI is capable of achieving a higher secrecy-energy-efficiency to that of the embedded jamming strategy having access to the CSI.

C. Impact of the eavesdropper density on the performance

The performance is further investigated in Fig. 4 as a function of the eavesdropper density. First of all, we observe in terms of the PAR that the 'Embedded-w CSI (circle)' solution exhibits a different trend from the other three solutions, when the density of eavesdroppers increases. This is because an increased fraction of transmit power is used for completely avoiding any information leakage to all eavesdroppers upon increasing the eavesdropper density. Hence the received signal power of the intended UE is reduced, and it fails to meet the TQoS requirement. (In this case, the maximum achievable performance is shown.) By contrast, the other three solutions have a fixed fraction of transmit power assigned for signal transmission, regardless of the eavesdropper density. Secondly, as far as the PASR is concerned, the trends of all the solutions coincide with the corresponding PAR, when the density of eavesdroppers is increased. To be specific, the embedded jamming strategy in the scenario relying on the CSI exhibits a significant reduction as a result of completely avoiding any information leakage to all eavesdroppers, while the PASR

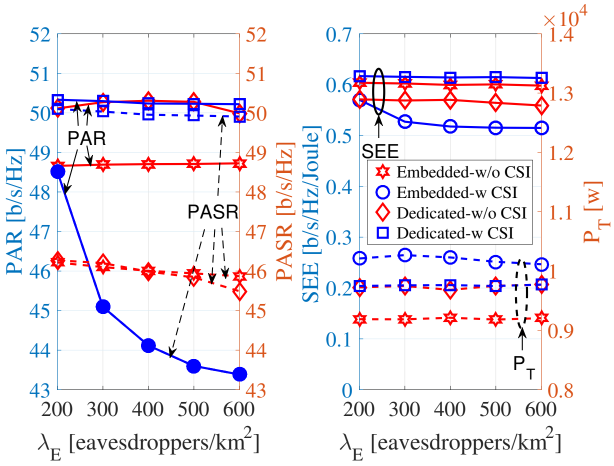


Fig. 4: Impact of the eavesdropper density λ_E on the performance. (The filled marker indicates that the PAR and PASR performance curves coincide with each other.)

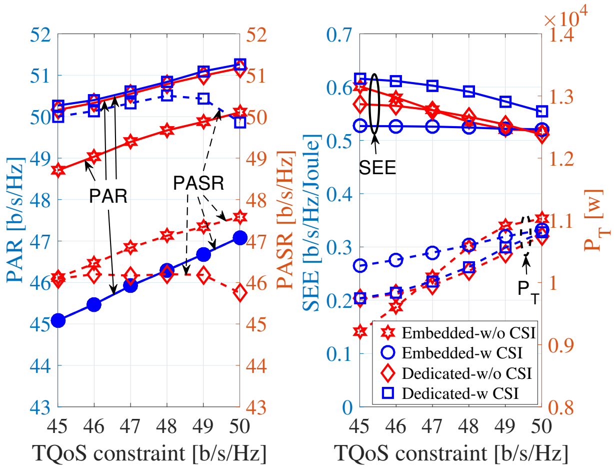


Fig. 5: Impact of TQoS constraint on the performance. (The filled marker indicates that the PAR and PASR performance curves coincide with each other.)

of the other three solutions is related to the eavesdropper's maximum rate, rather than to the eavesdropper density.

It can be observed at the right of Fig. 4 that the total transmit power consumption of all the solutions remains near-constant, as eavesdroppers become denser. Except for the 'Embedded-w CSI (circle)' solution, this trend is indeed expected for the other three solutions, since the performance is unrelated to the density of the eavesdroppers. However, for the 'Embedded-w CSI (circle)' solution, all available APs are relied upon for satisfying the current TQoS requirement, as well as for completely eliminating any information leakage to all eavesdroppers at any given eavesdropper density. Finally, the secrecy-energy-efficiency of the 'Embedded-w CSI (circle)' solution decays upon increasing the density of the eavesdroppers, whilst that of the other three solutions remains near-constant, due to the near-constant trends in terms of their PASR and P_T.

D. Impact of TQoS constraint on the performance

As a further step, the secrecy-energy-efficiency performance versus the TQoS constraint is studied. The left of Fig. 5 shows that as the TQoS constraint increases, as expected, all the solutions aim for involving more APs acting as serving APs to satisfy the TQoS constraint. As a consequence, the PASR of the embedded jamming strategy is also increased with the improved jamming capability. However, for the dedicated jamming strategy, the number of APs available as dedicated jammers for improving the secrecy-energy-efficiency may be reduced upon increasing the TQoS constraint. Hence the PASR may be reduced, albeit still satisfying the SQoS constraint. Observe at the right of Fig. 5 that the total power consumption of all the solutions increases due to the increased number of awake APs, when aiming for satisfying the TQoS constraint. Consequently, the secrecy-energy-efficiency trends of all the solutions tend to decay with various slopes, which is a consequence of having different trends in terms of their PASR and P_T.

E. Impact of SQoS constraint on the performance

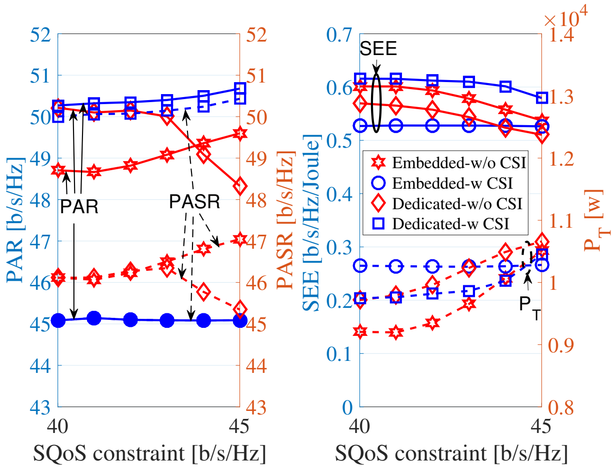


Fig. 6: Impact of SQoS constraint on the performance. (The filled marker indicates that the PAR and PASR performance curves coincide with each other.)

The performance is investigated in Fig.6 with regard to the various SQoS constraints. The first point to observe is that upon increasing the SQoS constraint, the trends of all the solutions become quite different. To be specific, for the embedded jamming strategy, the scenario operating without CSI exhibits a gradual increase in terms of both PAR and PASR, because an increased number of embedded APs is invoked for satisfying the increasing minimum SQoS target, while the scenario relying on the CSI remains unchanged, which is an explicit benefit of its perfect jamming capability. By contrast, as for the dedicated jamming strategy, the scenario operating without the CSI experiences a decaying PAR and PASR trend, while the scenario exploiting the CSI exhibits a slightly increased trend, due to the change in the number of dedicated jammers invoked for satisfying the minimum SQoS constraint, as well as due to the increased number of serving APs that contribute to improving the secrecy-energy-efficiency. Therefore, in the right of Fig. 6 we observe the corresponding total power consumption trends of these solutions, which reflect the increasing number of awake APs. Finally, we observe in Fig. 6 in terms of the secrecy-energy-efficiency trends that except for the 'Embedded-w CSI (circle)' solution - which remains unchanged upon increasing the SQoS constraint, - the other three solutions sacrifice their secrecy-energy-efficiency for satisfying the increased minimum SQoS requirement.

VII. Conclusions

In this paper, we considered the intriguing problem of designing secure and energy efficient user-centric UDNs. Novel secure user-centric clustering architectures were proposed along with a pair of carefully designed transmission strategies, corresponding to operating either with or without the eavesdropper's CSI knowledge. We proposed a sophisticated decoupled heuristics based technique for solving the optimization problem, in order to circumvent its computational intractability. Our numerical results characterized various performance metrics of our designs under diverse network settings. Explicitly, we characterized the security versus the energy-efficiency of user-centric UDNs, which is the first attempt in the literature. Our future work includes the consideration of the challenging case of mobile UEs.

References

[1] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, June 2014.

[2] X. Ge, S. Tu, G. Mao, C. X. Wang, and T. Han, "5G ultra-dense cellular networks," *IEEE Wireless Commun.*, vol. 23, no. 1, pp. 72–79, February 2016.

[3] M. Kamel, W. Hamouda, and A. Youssef, "Ultra-dense networks: A survey," *IEEE Commun.& Surveys Tuts.*, vol. 18, no. 4, pp. 2522–2545, 2016.

[4] A. Gotsis, S. Stefanatos, and A. Alexiou, "Ultra dense networks: The new wireless frontier for enabling 5G access," *IEEE Veh. Technol. Mag.*, vol. 11, no. 2, pp. 71–78, June 2016.

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

[6] Y. Wang, Z. Miao, and L. Jiao, "Safeguarding the ultra-dense networks with the aid of physical layer security: A review and a case study," *IEEE Access*, vol. 4, pp. 9082–9092, 2016.

[7] M. Kamel, W. Hamouda, and A. Youssef, "Physical layer security in ultra-dense networks," *IEEE Wireless Commun. Lett.*, vol. PP, no. 99, pp. 1–1, 2017.

[8] The 5G Infrastructure Public Private Partnership, *5G PPP Use Cases and Performance Evaluation Models*, April.25, 2016.

[9] J. Kim, H. W. Lee, and S. Chong, "Virtual cell beamforming in cooperative networks," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1126–1138, June 2014.

[10] S. Chen, F. Qin, B. Hu, X. Li, and Z. Chen, "User-centric ultra-dense networks for 5G: challenges, methodologies, and directions," *IEEE Wireless Commun.*, vol. 23, no. 2, pp. 78–85, April 2016.

[11] Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. H. Huang, and H. H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, April 2011.

[12] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, Third 2014.

[13] 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, Firstquarter 2017.

[14] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sept 2016.

[15] Y. Zou, B. Champagne, W. P. Zhu, and L. Hanzo, "Relay-selection improves the security-reliability trade-off in cognitive radio systems," *IEEE Trans. on Commun.*, vol. 63, no. 1, pp. 215–228, Jan 2015.

[16] G. Nigam, P. Minero, and M. Haenggi, "Coordinated multipoint joint transmission in heterogeneous networks," *IEEE Trans. on Commun.*, vol. 62, no. 11, pp. 4134–4146, Nov 2014.

[17] M. Kamel, W. Hamouda, and A. Youssef, "Performance analysis of multiple association in ultra-dense networks," *IEEE Trans. on Commun.*, vol. PP, no. 99, pp. 1–1, 2017.

[18] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. on Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct 2011.

[19] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. on Inf. Forensics and Security*, vol. 7, no. 1, pp. 310–320, Feb 2012.

[20] G. Zheng, L. C. Choo, and K. K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. on Signal Process.*, vol. 59, no. 3, pp. 1317–1322, March 2011.

[21] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. R. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 16–28, Sept 2013.

[22] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Y. Le Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Trans. on Veh. Technol.*, vol. 64, no. 5, pp. 1833–1847, May 2015.

[23] A. Chorti, S. M. Perlaza, Z. Han, and H. V. Poor, "Physical layer security in wireless networks with passive and active eavesdroppers," in *Proc. IEEE Global Telecommun. Conf. (Globecom)*, Dec 2012, pp. 4868–4873.

[24] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. on Wireless Commun.*, vol. 7, no. 6, 2008.

[25] W. C. Liao, T. H. Chang, W. K. Ma, and C. Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. on Signal Process*, vol. 59, no. 3, pp. 1202–1216, March 2011.

[26] V. Garcia, Y. Zhou, and J. Shi, "Coordinated multipoint transmission in dense cellular networks with user-centric adaptive clustering," *IEEE Trans. on Wireless Commun.*, vol. 13, no. 8, pp. 4297–4308, Aug 2014.

[27] W. Nie, F. C. Zheng, X. Wang, W. Zhang, and S. Jin, "User-centric cross-tier base station clustering and cooperation in heterogeneous networks: Rate improvement and energy saving," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 5, pp. 1192–1206, May 2016.

[28] H. S. Kang and D. K. Kim, "User-centric overlapped clustering based on anchor-based precoding in cellular networks," *IEEE Commun. Lett.*, vol. 20, no. 3, pp. 542–545, March 2016.

[29] Z. Huang, H. Tian, C. Qin, S. Fan, and X. Zhang, "A social-energy based cluster management scheme for user-centric ultra-dense networks," *IEEE Access*, vol. 5, pp. 10 769–10 781, 2017.

[30] A. Zappone, P. H. Lin, and E. Jorswieck, "Energy efficiency of confidential multi-antenna systems with artificial noise and statistical CSI," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1462–1477, Dec 2016.

[31] A. Kalantari, S. Maleki, S. Chatzinotas, and B. Ottersten, "Secrecy energy efficiency optimization for MISO and SISO communication networks," in *Proc. IEEE Int. Workshop on Signal Process. Advances in Wireless Commun. (SPAWC)*, June 2015, pp. 21–25.

[32] H. Ta and S. W. Kim, "Adapting rate and power for maximizing secrecy energy efficiency," *IEEE Commun. Lett.*, vol. PP, no. 99, pp. 1–1, 2017.

[33] X. Zhang and J. G. Andrews, "Downlink cellular network analysis with multi-slope path loss models," *IEEE Trans. on Commun.*, vol. 63, no. 5, pp. 1881–1894, May 2015.

[34] M. Ding, P. Wang, D. López-Pérez, G. Mao, and Z. Lin, "Performance impact of LoS and NLoS transmissions in dense cellular networks," *IEEE Trans. on Wireless Commun.*, vol. 15, no. 3, pp. 2365–2380, March 2016.

[35] M. Ding and D. López-Pérez, "On the performance of practical ultra-dense networks: The major and minor factors," in *IEEE Int. Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt)*, May 2017, pp. 1–8.

[36] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, “Compound wiretap channels,” *EURASIP J. on Wireless Commun. and Networking*, vol. 2009, p. 5, 2009.

[37] G. Auer, V. Giannini, C. Desset, I. Godor, P. Skillermark, M. Olsson, M. A. Imran, D. Sabella, M. J. Gonzalez, O. Blume, and A. Fehske, “How much energy is needed to run a wireless network?” *IEEE Wireless Commun.*, vol. 18, no. 5, pp. 40–49, October 2011.

[38] G. Auer, O. Blume, V. Giannini, I. Godor, M. Imran, Y. Jading, E. Katranaras, M. Olsson, D. Sabella, P. Skillermark, and W. Wajda, “D2.3: Energy efficiency analysis of the reference systems, areas of improvements and target breakdown,” *INFSO-ICT- 247733 EARTH (Energy Aware Radio NeTw. TecHnol.)*, November 2010.

[39] T. K. Y. Lo, “Maximum ratio transmission,” *IEEE Trans. on Commun.*, vol. 47, no. 10, pp. 1458–1461, Oct 1999.

[40] K. Zarifi, S. Affes, and A. Ghrayeb, “Collaborative null-steering beamforming for uniformly distributed wireless sensor networks,” *IEEE Trans. on Signal Process.*, vol. 58, no. 3, pp. 1889–1903, March 2010.