# Strategic Deployment of Swarm of UAVs for Secure IoT Networks

X. A. Flores Cabezas, *Student Member, IEEE,* and D. P. Moya Osorio, *Senior Member, IEEE*

***Abstract*—Security provisioning for low-complex and constrained devices in the Internet of Things (IoT) is exacerbating the concerns for the design of future wireless networks. To unveil the full potential of the sixth generation (6G), it is becoming even more evident that security measurements should be considered at all layers of the network. This work aims to contribute in this direction by investigating the employment of unmanned aerial vehicles (UAVs) for providing secure transmissions in ground IoT networks. Toward this purpose, it is considered that a set of UAVs acting as aerial base stations provide secure connectivity between the network and multiple ground nodes. Then, the association of IoT nodes, the 3D positioning of the UAVs and the power allocation of the UAVs are obtained by leveraging game theoretic and convex optimization-based tools with the goal of increasing the amount of nodes that achieve perfect secrecy in the system. It is shown that the proposed framework obtains better and more efficient secrecy performance over an IoT network than state-of-the-art greedy algorithms for positioning and association.**

***Index Terms*—3D position control, IoT, node association, physical layer security, unmanned aerial vehicle.**

## I. Introduction

The fifth generation of wireless networks (5G) is envisioned to bring upon ubiquitous connectivity. Looking forward, beyond 5G, great advancements have been envisioned for the sixth generation of wireless networks (6G), which promises ubiquitous intelligence [1]. Toward that, many low-complexity wireless devices would be part of populated decentralized networks, where absolutely everything is connected in massive deployments of Internet of Things (IoT) networks, with applications in very different sectors, namely, industry, defense, healthcare, intelligent transportation systems, to name a few [2].

In such dense, heterogeneous networks, very sensitive information is transmitted over a shared medium, thus security and privacy issues become critical, and they cannot be handled independently of other parameters, i.e. energy consumption or latency [1]. While traditional cryptographic approaches have developed to be trustable solutions for preserving security in communications, the limitations and constraints of IoT devices and sensors, and the advancements in quantum computing render these approaches unfeasible or unreliable [2]. On the other hand, physical layer security (PLS) techniques, that explore the inherent properties of the noisy and random wireless channels to provide security to communications, has emerged as a promising and attractive security solution. Some well-known PLS techniques include artificial noise injection through friendly jamming, spatial diversity, beamforming design and relaying [1], [3], [4]. These techniques aim at designing the physical layer to provide an advantage of the legitimate link over the eavesdropping link with no assumption on the computing power of the attacker, thus providing information-theoretic security guarantees.

From other perspective, it is recognized that unmanned aerial vehicles (UAVs) will play an important role in IoT applications, specially to provide connectivity in remote areas, disaster zones, and harsh environments [5], [6]. Thanks to their flexible deployment, capability of providing strong line of sight (LoS) connectivity and, ease of maneuverability, UAVs open a new range of novel opportunities for wireless networks, but at the same time, novel threat vectors should be also considered [4]. Noting these advantageous properties, UAVs can also be exploited for the design of PLS techniques to safeguard UAV-assisted communications. For instance, the challenges and opportunities for preventing passive and active attacks in wireless networks have been recently discussed in [3].

Particularly, the introduction of UAV nodes acting as friendly jammers in order to improve the secrecy performance of wireless networks has recently risen special attention [7]. All in all, the integration of UAVs into the provisioning of security through PLS techniques provides novel opportunities for safeguarding 6G networks. Importantly, the use of learning methods would allow the UAVs not only to remain autonomous, but also to adapt to the complexity of PLS security provisioning under dynamic channels and complex IoT scenarios, which is the main focus of this work.

### *A. Related Work*

Recently, the flexibility of UAVs has risen attention for secure transmissions in wireless networks [8]–[14]. In particular, UAVs have been employed as friendly jammers to assist a legitimate transmission by introducing artificial noise in order to prevent leakage of information to possible eavesdroppers in the network [7], [15]–[23]. In [7], the optimal three-dimensional (3D) deployment and jamming power of a UAV-based jammer are investigated to improve the secrecy performance of a wireless network in terms of the outage probability and the intercept probability, by defining area-based metrics that ensure a given intercept probability threshold within a

X. A. Flores Cabezas is with the Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg (e-mail: alejandro.flores@uni.lu). He was previously with the Centre for Wireless Communications, University of Oulu, Oulu, Finland (e-mail: xavier.florescabezas@oulu.fi).

Diana Moya Osorio is with the Communication Systems Division, Department of Electrical Engineering, Linköping University, Linköping 581 83, Sweden (e-mail: diana.moya.osorio@liu.se). She was previously with the Centre for Wireless Communications, University of Oulu, Oulu 90014, Finland (e-mail: diana.moyaosorio@oulu.fi).

This research was supported by the Research Council of Finland (former Academy of Finland) 6G Flagship Programme (Grant Number: 346208), project FAITH (Grant Number: 334280), and by the Excellence Center at Linköping – Lund in Information Technology (ELLIIT).

certain area. In [15], a UAV friendly jammer scheme is introduced to enhance the secrecy rate of a wireless system, where the problem of trajectory optimization is investigated. In [16], a joint jamming scheme between the legitimate UAVs serving as multi-access edge computing (MEC) servers and the ground nodes is proposed to safeguard the legitimate transmission against malicious UAVs. Therein, the minimum secrecy capacity among system ground users (GUs) is maximized by jointly optimizing the position, jamming power, and the computing capacity of the legitimate UAV, as well as the offloading rate of the GUs to the UAV, the transmit power of the GUs, and the offloading GU association. Therein, it was demonstrated that the max-min secrecy capacity is improved over the benchmarks, specially for low offloading requirements, while existing a trade-off between security and latency. In [17], the secrecy outage probability (SOP) of a UAV-based millimeter wave (mmWave) relay network in the presence of multiple eavesdroppers is investigated, where the scenarios with and without cooperative jamming were contrasted. In [18], the existence of an optimal UAV jammer location on a network with multiple eavesdroppers was proven, and the impact of the density of eavesdroppers, the transmission power of the UAV jammer, and the density of UAV jammers on the optimal location was investigated. In [19], two area-based secrecy metrics, the jamming coverage (JC) and the jamming efficiency (JE), were proposed to evaluate the impact of jamming for secure wireless communications based on the SOP over an area, without knowledge of the position of the eavesdropper. Later, in [20], this idea was extended by introducing a hybrid secrecy metric, the so-called weighted secrecy coverage (WSC), that considers both coverage and efficiency of friendly jamming, simultaneously, in the context of UAV-based friendly jamming. Therein, the positioning of the UAV jammers to maximize the WSC is tackled. Further, in [21], a null-space precoding scheme is employed to eliminate the interference at the legitimate receiver. Under that scheme, a better performance was obtained in terms of the WSC. Further, in [22] and [23], the previous scenario was extended to include the 3D movement of the UAVs and the movement of the legitimate ground GU, respectively. These works consider the formulation of the problem of adaptive position control of the UAVs as a multi-armed bandit, and the results presented significant improvements of the secrecy of the system in terms of WSC. In [24], a system is considered where a UAV is serving a group of GUs via non-orthogonal multiple access (NOMA), while sending artificial noise to disrupt a passive eavesdropper in the system. The total jamming power and the rate at each GU are maximized by optimizing the UAV trajectory, the power allocation, and the GU scheduling. Such scheme was proven to outperform orthogonal multiple access schemes as well as non-jamming schemes in terms of the system sum-rate and of the eavesdropper data-rate. A summary of these works is depicted in Table 1, with the different aspects treated on them, contrasted to our work.

In recent years, the use of machine learning techniques has been increasingly considered to optimize the deployment of UAVs in wireless networks [25]–[29]. For instance, a novel federated learning-based framework for the distributed joint power allocation and scheduling of swarm of UAVs was proposed in [25]. The proposed framework significantly improves the convergence time of two baseline methods, namely optimized power-randomized scheduling and randomized power-optimized scheduling. In [26], an actor-critic deep reinforcement learning (RL) approach is proposed to find the optimal trajectory design and power allocation in UAV-assisted cellular networks, which achieves better network performance in terms of the average sum-rate of the system. In [27], game theory and RL are used to enhance the data offloading from UAVs to MEC servers in an IoT scenario. Therein, it was proven that the proposed methods converge to a Nash equilibrium of average offloaded data, whereas the RL approach ensures the convergence without exchange of information between UAVs. In [28], a deep Q-Learning-based scheduling approach is used to minimize the packet loss of IoT nodes in UAV-assisted wireless powered-IoT networks. The deep Q-Learning algorithm performs IoT node and modulation scheme selection for IoT nodes that wish to send information and wirelessly receive power from the UAVs. It was shown that the deep Q-Learning approach obtains much lesser packet loss than greedy or random scheduling approaches. In [29], the binary log-learning (BLLL) and greedy algorithms are proposed to maximize the total sum rate of the GUs throughout the network by optimizing the GU-UAV association and UAV position control in a UAV-assisted network. Therein, it was shown that greedy algorithms for UAV position control and GU-UAV association are sub-optimal and obtain a lower sum-rate than BLLL. However, the convergence of BLLL presents an exponential time, thus the greedy algorithms are preferable in this aspect.

Also, a deep Q-Network-based power allocation strategy was proposed in [30], to improve the secrecy rate of a legitimate communication between a UAV and a mobile GU in the presence of a malicious mobile GU and UAV. Therein, it is assumed that the attackers can choose between eavesdropping, spoofing and jamming attacks, and the results proved to overcome benchmarks based on Q-Learning and a win or learn faster-policy hill climbing (WoLF-PHC) approach. More recently, the optimization of the sum secrecy rate of a system with a single UAV acting as an aerial base station (ABS), that serves a group of ground nodes in the presence of UAVs acting as adaptive eavesdroppers or jammers, was proposed in [31]. Therein, a Stackelberg game was formulated considering two strategies, the ABS positioning to increase the sum secrecy rate of the system as the leader, and the cooperative attack of the adaptive eavesdroppers as the follower. Then, a spatial adaptive play learning algorithm is utilized to reach the equilibrium, which is shown to obtain a better sum secrecy rate than a random or ring deployment of the ABS.

### B. Main Contributions

To contribute to the state-of-the-art, and different to the works cited, this work considers the association, power allocation, and position control of multiple UAVs serving as ABSs to a set of multiple ground IoT nodes through frequency division multiple access (FDMA), by focusing on the secrecy

| Ref. | Objective | Metric | Alice | Bob | Eve | Jammers | UAV position control | Power Allocation | Association | Method | A2G Channel |
|---|---|---|---|---|---|---|---|---|---|---|---|
| [7] | Maximize | IPSR | 1 GU | 1 GU | 1 GU | 1 UAV | 3D | Jam. | N/A | Friendly Jam. | Rayleigh |
| [15] | Maximize | Secrecy rate | 1 GU | 1 GU | 1 GU | 1 UAV | 2D | Tx. and Jam. | N/A | Friendly Jam. | Rayleigh |
| [16] | Max. min | Secrecy rate | Many GU | 1 UAV | Many UAVs | UAV & GU | 2D | Tx. and Jam. | Offloading | Cooperative Jam. | LoS |
| [17] | Analyze | SOP | 1 GU | 1 GU | Many GUs | 1 UAV | Fixed | Fixed | N/A | Cooperative Jam. | Nakagami-m |
| [18] | Analyze | Secrecy Transmission Probability | 1 GU | 1 GU | Many GUs | 1 UAV | Fixed | Fixed | N/A | Friendly Jam. | Nakagami-m |
| [19] | Analyze | JC / JE | 1 GU | 1 GU | 1 GU | 1-2 UAVs | Fixed | Fixed | N/A | Friendly Jam. | Rayleigh |
| [20] | Analyze | WSC | 1 GU | 1 GU | 1 GU | 2 UAVs | Fixed | Fixed | N/A | Friendly Jam. | LoS |
| [21] | Analyze | WSC | 1 GU | 1 GU | 1 GU | 2 UAVs | Fixed | Fixed | N/A | Friendly Jam.<br>NS precoding | LoS |
| [22] | Maximize | WSC | 1 GU | 1 GU | 1 GU | Many UAV | 2D | Jam. | N/A | Friendly Jam. | Rice |
| [23] | Maximize | WSC | 1 GU | 1 GU | 1 GU | Many UAV | 2D | Fixed | N/A | Friendly Jam.<br>NS precoding | LoS |
| [24] | Maximize | Jam. power + sum rate | 1 UAV | Many GUs | 1 GU | UAV | 2D | Tx. and Jam. | Scheduling | UAV as ABS and Jammer | LoS |
| * | Maximize | GUs with positive secrecy | Many UAVs | Many GUs | Many GUs | None | 3D | Tx. | Service | UAVs as ABSs | Rice |

TABLE I
Summary of UAV-aided secrecy-centric literature, compared to this work (*).

performance of the system assuming multiple eavesdroppers. Different from the approach in [29], in this work a measure of the number of nodes that achieve positive secrecy rate in the system is considered as the utility function, and the power allocation per node is also investigated. Moreover, different from the works in [16], [30], [31], inactive nodes in the system are treated as potential eavesdroppers, thus presenting a relatively high density of eavesdroppers in the system. For the user-UAV association and UAV positioning, the synchronous log-linear learning (SLLL) formulation is considered, which is a synchronous algorithm that offers faster convergence.

All in all, the main contributions of this paper are three-fold:

1) A three-stage block-coordinate ascend (BCA) framework is proposed where node association, UAV 3D position control, and power allocation are the blocks that are optimized iteratively by considering the other blocks fixed in order to increase nodes with positive secrecy in the proposed network.
2) Game-theoretic algorithms are proposed for node association and UAV position control to increase the nodes with positive secrecy of the system.
3) A convex optimization-based power allocation technique is developed to increase the minimum secrecy rate of IoT nodes that can achieve secrecy, while guaranteeing a level of service to all IoT nodes.

## II. System Model

This section introduces the system and channel models. For convenience, a list of the symbols used throughout this manuscript is presented in Table II.

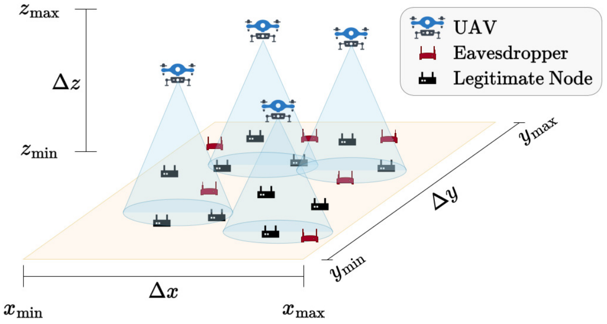

Fig. 1. System model.

Consider the system illustrated in Fig. 1, which consists of a set of $N$ IoT devices that are distributed following an uniform binomial point process over a rectangular region of dimensions $\Delta x = x_{\max} - x_{\min}$ and $\Delta y = y_{\max} - y_{\min}$, with the bi-dimensional position of the $n$th-IoT device (that can be a legitimate node or eavesdropper) denoted by $\mathbf{x}_l = (x_l, y_l)$. To provide connectivity to the IoT devices, a swarm of $M$ single-antenna UAVs, acting as ABSs is deployed over the region of interest at positions $\mathbf{x}_m = (x_m, y_m, z_m)$. These UAVs can move in three dimensions over the rectangular region, within a altitude range $\Delta z = z_{\max} - z_{\min}$. In this system, it is considered that, for a certain transmission process, only a fraction of IoT devices (randomly and independently selected according to a Bernoulli distribution of parameter $q$) are set on receiving mode (legitimate nodes), while the rest of the devices are assumed to be vulnerable to hijacking and are overhearing the channel, thus being considered as potential eavesdroppers.

| Symbol | Description |
|---|---|
| $h_{m,l}$ | Channel response between UAV $m$ and ground node $l$. |
| $g_{m,l}$ | Channel gain between UAV $m$ and ground node $l$. |
| $L_{m,l}$ | Average pathloss between UAV $m$ and ground node $l$. |
| $a_{l,m,c}$ | Association indicator of node $l$ to UAV $m$ through sub-channel $c$. |
| $p_m^c$ | Power employed by UAV through sub-channel $c$. |
| $r_l$ | Resource associated to node $l$. |
| $\gamma_m^c$ | Transmit SNR employed by UAV through sub-channel $c$. |
| $\gamma_{m,l}^c$ | SINR of node $l$, served by UAV $m$ through sub-channel $c$. |
| $\gamma_{m,e*}^c$ | SINR of strongest eavesdropper relative to node $l$, served by UAV $m$ through sub-channel $c$. |
| $\gamma_l$ | SINR of node $l$, over corresponding sub-channel served by the corresponding UAV. |
| $\gamma_{e*}$ | SINR of the corresponding strongest eavesdropper. |
| $I_{m,n}^c$ | Interference experienced by node $n \in \{l, e*\}$ served by UAV $m$ through sub-channel $c$. |
| $C_S$ | Secrecy capacity. |
| $\phi_l$ | Secrecy metric of node $l$. |
| $\mathbf{x}_m$ | Cartesian position of UAV $m$. |
| $\mathbf{x}_l$ | Cartesian position of node $l$. |
| $\mathbf{P}$ | Power allocation matrix of all UAVs. |
| $\mathbf{A}$ | Association array. |
| $C$ | Number of orthogonal sub-channels. |
| $BW$ | Total bandwidth per UAV. |
| $B$ | Bandwidth per node per UAV. |
| $N$ | Number of nodes in the system. |
| $M$ | Number of UAVs in the system. |
| $L$ | Number of legitimate nodes in the system. |
| $E$ | Number of eavesdroppers in the system. |

TABLE II
TABLE OF SYMBOLS

In this system, downlink transmissions from the UAVs to the IoT devices are based in frequency division multiple access (FDMA). Assuming that all UAVs have the same limited amount of bandwidth $BW$, each one divides its total bandwidth into $C$ orthogonal sub-channels of bandwidth $B = BW/C$. Additionally, let $\mathcal{N}$ be the set of ground nodes, while $\mathcal{L}$ and $\mathcal{E}$ are the sets of legitimate nodes and eavesdroppers, such that $|\mathcal{N}| = N$, $|\mathcal{L}| = L$ and $|\mathcal{E}| = E$, respectively. Additionally, $\mathcal{M}$ is the set of UAVs, such that $|\mathcal{M}| = M$ and $\mathcal{C}$ is the set of sub-channels available at each UAV, with $|\mathcal{C}| = C$. For simplicity purposes, the described sets are treated as their respective sets of indices as well.

Accordingly, each UAV can associate with up to $C$ ground nodes, with the power allocated by UAV $m \in \mathcal{M}$ to the sub-channel $c \in \mathcal{C}$ denoted as $p_m^c$, and the total power budget at each UAV is $P$. Then, the power allocation vector at UAV $m$ is given by $\mathbf{p}_m = (p_m^1, ..., p_m^C)^T$ and the power allocation matrix of the whole system is given by $\mathbf{P} \in \mathbb{R}^{C \times M}$ with $\mathbf{P} = [\mathbf{p}_1, ..., \mathbf{p}_M]$. Let $\mathbf{A} \in \mathbb{R}^{L \times M \times C}$ be the association array with elements $a_{l,m,c} \in \{0, 1\}$, where $a_{l,m,c} = 1$ if node $l$ is associated to UAV $m$ through sub-channel $c$, and 0 otherwise. Given that, at any time a certain sub-channel is either available or assigned to a single node, and that all legitimate nodes are associated to a single sub-channel, it holds that

$$\sum_{l \in \mathcal{L}} a_{l,m,c} \leq 1 \quad \forall m \in \mathcal{M}, \forall c \in \mathcal{C}, \tag{1}$$

$$\sum_{m \in \mathcal{M}} \sum_{c \in \mathcal{C}} a_{l,m,c} \leq 1 \quad \forall l \in \mathcal{L}. \tag{2}$$

The air-to-ground (A2G) channel between UAV $m$, at altitude $z_m$, and a ground node $l$ is modeled as $h_{m,l} = (\sqrt{L_{m,l}})^{-1} \hat{h}_{m,l}$, where $L_{m,l}$ is the average pathloss of the link and $\hat{h}_{m,l}$ is the small-scale fading component. Here, $\hat{h}_{m,l}$ is modeled as Rician fading as in [32], given by

$$\hat{h}_{m,l} = \sqrt{\frac{K_{m,l}}{1 + K_{m,l}}} \hat{h}_{m,l}^{\text{LoS}} + \sqrt{\frac{1}{1 + K_{m,l}}} \hat{h}_{m,l}^{\text{NLoS}}, \tag{3}$$

where $\hat{h}_{m,l}^{\text{LoS}}$ is the line of sight component with $|\hat{h}_{m,l}^{\text{LoS}}| = 1$, $\hat{h}_{m,l}^{\text{NLoS}}$ contains the contribution of the NLoS components, and is modeled as a circularly symmetric complex Gaussian random variable as $\hat{h}_{m,l}^{\text{NLoS}} \sim \mathcal{CN}(0, 1)$, and $K_{m,l}$ is the Rician factor of the channel, which depends on the elevation angle from UAV $m$ to node $l$ [32]. The average pathloss for the A2G links is modeled as in [7], with $P_{\text{LoS}}$ and $P_{\text{NLoS}}$ probabilities of LoS and NLoS connection being, respectively, given by [7]

$$P_{\text{LoS}} = \frac{1}{1 + \psi \exp\left(-\omega \left[\frac{180}{\pi} \tan^{-1}\left(\frac{z_m}{r_{m,l}}\right) - \psi\right]\right)} \tag{4}$$

and $P_{\text{NLoS}} = 1 - P_{\text{LoS}}$, with $\psi$ and $\omega$ being environmental constants [33], [34], and $r_{m,l}$ is the distance from node $l$ and the projection on the ground of UAV $m$. Then, the average pathloss of the links is given by

$$L_{m,l} = \left(z_m^2 + r_{m,l}^2\right)^{\alpha_J} \left(P_{\text{LoS}} \eta_{\text{LoS}} + P_{\text{NLoS}} \eta_{\text{NLoS}}\right), \tag{5}$$

where $\alpha_J$ is the pathloss exponent for the A2G links, and $\eta_{\text{LoS}}$ and $\eta_{\text{NLoS}}$ are the attenuation factors for the LoS and the NLoS links, respectively. Also, the channel gain $g_{m,l}$ is given by $g_{m,l} = |h_{m,l}|^2$.

Let $s_m^c$ be the unit-power symbol sent by UAV $m$ to node $l$ through its sub-channel $c$ with power $p_m^c$. Then, the received signal $y_l^c$ at node $l$ is given by

$$y_l^c = h_{m,l} \sqrt{p_m^c} s_m^c + \sum_{\substack{k \in \mathcal{M} \\ k \neq m}} h_{k,l} \sqrt{p_k^c} s_k^c + w, \tag{6}$$

where $w$ is the additive white Gaussian noise (AWGN) of power $N_0$. Then, the received signal-to-interference-plus-noise ratio (SINR) at node $l$ from UAV $m$ through channel $c$ is given by

$$\gamma_{m,l}^c = \frac{a_{l,m,c} \gamma_m^c g_{m,l}}{\sum\limits_{\substack{k \in \mathcal{M} \\ k \neq m}} \gamma_k^c g_{k,l} + 1}, \tag{7}$$

where $\gamma_m^c = \frac{p_m^c}{N_0}$ is the transmit signal-to-noise ratio (SNR) at UAV $m$ in sub-channel $c$. Furthermore, no cooperation is considered among eavesdroppers, i.e. they are non-colluding, thus the eavesdropping risk is dominated by the eavesdropper with the strongest received SINR given by

$$\gamma^c_{m,e*} = \frac{\gamma^c_m g_{m,e*}}{\sum\limits_{\substack{k\in\mathcal{M}\\ k\neq m}} \gamma^c_k g_{k,e*} + 1}, \tag{8}$$

$$e* = \underset{e\in\mathcal{E}}{\operatorname{argmax}} \left\{ \frac{\gamma^c_m g_{m,e}}{\sum\limits_{\substack{k\in\mathcal{M}\\ k\neq m}} \gamma^c_k g_{k,e} + 1} \right\}. \tag{9}$$

For ease of notation, $\gamma^c_{m,l}$ will be written as $\gamma_l$ when $a_{l,m,c} = 1$, and its corresponding $\gamma^c_{m,e*}$ will be written as $\gamma_{e*}$.

The secrecy capacity $C_S$ of the wiretap channel [35], which is the maximum achievable secrecy rate for a wiretap channel, is defined as $C_S = [C_\mathrm{M} - C_\mathrm{W}]^+$ [36] with $[X]^+ = \max[X, 0]$. Here $C_\mathrm{M}$ is the main channel capacity between the legitimate receiver and the legitimate transmitter, and $C_\mathrm{W}$ is the wiretap channel capacity between the eavesdropper and the legitimate transmitter. Then, the secrecy capacity for the downlink communication of the corresponding UAV to node $l$, considering Gaussian channels, is given as

$$C_S = \left[\log_2\left(\frac{1+\gamma_l}{1+\gamma_{e*}}\right)\right]^+. \tag{10}$$

## III. Maximization of Nodes with Positive Secrecy

In this section, the optimal node association, the 3D-deployment of UAVs, and the power allocation are obtained to maximize the amount of IoT nodes that achieve positive secrecy rate.

A positive secrecy capacity indicates that a node is able to transmit confidential messages at a secrecy rate lower than the secrecy capacity. Considering the achievable secrecy rate for the node $l$ given by (10), the condition for node $l$ to achieve positive secrecy rate is

$$\frac{g_{m,l}}{I^c_{m,l} + 1} > \frac{g_{m,e*}}{I^c_{m,e*} + 1}, \tag{11}$$

with the interference terms defined as

$$I^c_{m,n} = \sum_{\substack{k\in\mathcal{M}\\ k\neq m}} \gamma^c_k g_{k,n}, \qquad n \in \{l, e*\}, \tag{12}$$

which shows the impact of the node association, UAV deployment, and power allocation on the number of nodes that can achieve positive secrecy. The derivation of (11) is detailed in Appendix A.

The condition for positive secrecy given by equation (11) can be re-written as

$$\frac{\frac{g_{m,l}}{I^c_{m,l}+1}}{\frac{g_{m,e*}}{I^c_{m,e*}+1}} > 1. \tag{13}$$

By defining variable $\phi_l$ as

$$\phi_l \triangleq \log_2\left(\frac{\frac{g_{m,l}}{I^c_{m,l}+1}}{\frac{g_{m,e*}}{I^c_{m,e*}+1}}\right) > 0, \tag{14}$$

$\phi_l$ can be used to measure whether a node achieves positive secrecy or not. Particularly, $\phi_l > 0$ if node $l$ achieves positive secrecy, and $\phi_l \leq 0$, otherwise.

Note that, due to the high density of eavesdroppers and legitimate nodes, as well as the geometry of the system, not every node will be able to obtain a positive secrecy rate. Then, the objective of this study is to maximize the number of nodes that transmit in secrecy, and the optimization problem can be formulated as

$$\begin{aligned}
\mathcal{P}: \quad & \max_{\mathbf{A}, \{\mathbf{x}_m\}_{m\in\mathcal{M}}, \mathbf{P}} \sum_{l\in\mathcal{L}} \phi_l && && \text{(15a)}\\
\text{s.t.} \quad & (1), (2), && && \\
& a_{l,m,c} \in \{0,1\}, && \forall a_{l,m,c} \in \mathbf{A} && \text{(15b)}\\
& x_{\min} \leq x_m \leq x_{\max}, && \forall m \in \mathcal{M} && \text{(15c)}\\
& y_{\min} \leq y_m \leq y_{\max}, && \forall m \in \mathcal{M} && \text{(15d)}\\
& z_{\min} \leq z_m \leq z_{\max}, && \forall m \in \mathcal{M} && \text{(15e)}\\
& \sum_{c\in\mathcal{C}} p^c_m \leq P, && \forall m \in \mathcal{M}. && \text{(15f)}
\end{aligned}$$

The objective function (15a) is a non convex function, and (15b) is a mixed-integer constraint, thus problem $\mathcal{P}$ is an intricate non-convex combinatorial optimization problem. Alternatively, a block coordinate ascend (BCA) algorithm is proposed to optimize the node association, UAV positioning, and power allocation, each block optimized by considering the other blocks fixed. The proposed secure BCA framework is described next, where each block is optimized at a time while maintaining the others fixed. Note that this optimization is performed over a snapshot of the network with fixed node positions, and would be performed on-demand for different transmission blocks.

### A. Node Association

The first stage consists of solving the optimal association of legitimate IoT nodes to the UAVs. Thus, the goal of this stage is to solve the following optimization sub-problem

$$\begin{aligned}
\mathcal{P}1: \quad & \max_{\mathbf{A}} \quad \sum_{l\in\mathcal{L}} \phi_l \\
& \text{s.t.} \quad (1),\ (2),\ (15\text{b}).
\end{aligned} \tag{16}$$

Note that the power allocated by the UAVs to their subchannels is not considered for the optimization at this stage, thus allowing users to associate based on the channels that offer better secrecy performance.

To solve $\mathcal{P}1$, a potential game is formulated as described next.

*1) Potential Game:* According to this game, a fixed number of resources $r_l$, i.e. sub-channels, are available at each UAV. By associating to a given resource, a node $l$ will obtain a certain $\phi_l(r_l)$ value, and the goal is to get the highest possible value. However, resources are limited, and if a given resource is already occupied, it cannot be assigned to another node. Therefore, there exists a competition among nodes for a given resource in order to obtain the best local secrecy performance. This game considers the following elements:

- **Players:** Are the legitimate nodes $l \in \mathcal{L}$.
- **Actions:** Are the resources to associate with, i.e. the pairs $r_l = (m, c)$, with $m \in \mathcal{M}$ and $c \in \mathcal{C}$.
- **Payoffs:** Are the values $f_l(r_l) = \phi_l(r_l)$ obtained after performing an association.

Once the goal is to maximize the nodes with positive secrecy, the overall utility can be represented as a function of the actions of every node in the system. Then, the utility can be expressed as

$$F(\mathbf{r}) = F(r_l, \mathbf{r}_{-l}) = \sum_{\substack{n \in \mathcal{L} \\ n \neq l}} f_n(r_n) + f_l(r_l). \tag{17}$$

In (17), $r_l$ represents the current strategy of node $l$, and $r_l'$ represents a potential new strategy to be adopted, such that the change in payoff for the node $l$ is given by $f_l(r_l') - f_l(r_l)$. By assuming constant power over the association phase, the choice of resource of a given node during this phase does not consider the signal or interference levels at the other nodes, thus $f_n(r_n)$ remains constant under a change of strategy of node $l \neq n$, and then

$$\begin{aligned} & F(r_l', \mathbf{r}_{-l}) - F(r_l, \mathbf{r}_{-l}) \\ & = \left( \sum_{\substack{n \in \mathcal{L} \\ n \neq l}} f_n(r_n) + f_l(r_l') \right) - \left( \sum_{\substack{n \in \mathcal{L} \\ n \neq l}} f_n(r_n) + f_l(r_l) \right) \\ & = f_l(r_l') - f_l(r_l). \end{aligned} \tag{18}$$

This indicates that this is a potential game with the potential function being the overall utility of the system $F(\cdot)$. Therefore, the best response dynamics can be used to reach a pure Nash equilibrium. Furthermore, given that every node can be considered an independent entity, the overall game is a simultaneous move game, where every node chooses its next strategy independently.

Under these considerations, two conflicts may arise. Particularly, it is possible for more than one node to choose the same resource at a certain moment, and it is also possible for a node to choose an already occupied resource at a certain moment. To address these conflicts, a protocol is proposed to be followed by each UAV. For the first conflict, UAVs will be programmed to allocate the resource to the contending node with the highest $\phi_l$, and if there are two or more nodes with the same value of $\phi_l$, the UAV will associate to one of them arbitrarily. To address the second conflict, nodes are only allowed to choose resources that are not currently occupied. It can be seen as the UAVs advertising only their available sub-channels to the legitimate nodes.

Apart from best response dynamics, a potential game is guaranteed to reach a pure Nash equilibrium under a synchronous log-linear learning (SLLL) algorithm [37], which is described next.

*2) Synchronous Log Linear Learning:* In this algorithm, it is considered that the gain in payoff, obtained by performing an action, changes with respect to the current action (marginal payoff), which is given by

$$f_l(r_l') = \phi_l(r_l') - \phi_l(r_l). \tag{19}$$

Therefore, the gain in payoff obtained by remaining in the current strategy is 0 and the potential game modeling holds.

The SLLL algorithm is considered for the potential game with (19) as the payoff function. Under the SLLL algorithm, a legitimate node chooses an action from their available actions following the smooth best response (SBR) mixed strategy [38] given by

$$\pi_l(r_l) = \frac{e^{f_l(r_l)}}{\sum\limits_{z_l \in \mathcal{A}_l} e^{f_l(z_l)}}. \tag{20}$$

After each legitimate node has chosen an action, if two or more nodes choose the same resource, UAVs apply the protocol to solve conflicts, then all the legitimate nodes choose their next strategy. This goes on until no legitimate nodes have available strategies, i.e., until no node has an incentive to change strategies (i.e., they are already in their best response strategy), which constitutes a pure Nash equilibrium. Algorithm 1 describes the operation of this algorithm.

**Algorithm 1:** SLLL for node association algorithm

```
counter $\leftarrow$ 0;
while $counter < n\_iter$ do
    conv_flag $\leftarrow$ 1 ;
    $\mathbf{x}[l] \leftarrow -1 \;\forall l \in \mathcal{L}$;
    for $l \in \mathcal{L}$ do
        $\mathcal{A}_l \leftarrow \{r = (m,c),\; s.t.\; (m,c) \in \mathcal{M} \times \mathcal{C}\}$;
        $\mathcal{A}_l \leftarrow \mathcal{A}_l \setminus \{r = (m,c),\; s.t.\; \sum_{n \in \mathcal{L}} a_{n,m,c} > 0\}$;
        $f_l(r) \leftarrow$ compute as in (19) $\forall r \in \mathcal{A}_l$;
        $\mathcal{A}_l \leftarrow \mathcal{A}_l \setminus \{r = (m,c)\; s.t.\; f_l(r) \leq 0\}$ ;
        if $\mathcal{A}_n \neq \emptyset$ then
            $\Pr[X_l = r] \leftarrow$ compute as in (20) $\forall r \in \mathcal{A}_l$;
            $x_l \leftarrow$ choose from $r \in \mathcal{A}_l$ according to $\Pr[X_l = r]$;
            $\mathbf{x}[l] \leftarrow x_l$;
            conv_flag $\leftarrow$ 0 ;
    end
    if $conv\_flag == 1$ then
        Stop the association process;
    for $m \in \mathcal{M}$ do
        for $c \in \{c \in \mathcal{C}\; s.t. \sum_{n \in \mathcal{L}} a_{n,m,c} = 0\}$ do
            $\mathcal{N}_{m,c} \leftarrow \{l\; s.t.\; \mathbf{x}[l] = (m,c)\}$;
            if $|\mathcal{N}_{m,c}| > 0$ then
                $f_l(m,c) \leftarrow$ compute as in (19) $\forall l \in \mathcal{N}_{m,c}$;
                $f_{l,\max} \leftarrow \max_{l \in \mathcal{N}_{m,c}} f_l(m,c)$ ;
                $\mathcal{N}_{m,c,\max} \leftarrow \{l \in \mathcal{N}_{m,c}\; s.t.\; f_l(m,c) = f_{l,\max}\}$;
                $l^* \leftarrow$ choose from $l \in \mathcal{N}_{m,c,\max}$ randomly;
                $(m_{\text{prev}}, c_{\text{prev}}) \leftarrow (m,c)\; s.t.\; a_{l^*,m,c} = 1$;
                $a_{l^*,m_{\text{prev}},c_{\text{prev}}} \leftarrow 0$;
                $a_{l^*,m,c} \leftarrow 1$;
        end
    end
    counter $\leftarrow$ counter + 1;
end
```

### *B. UAV Position Control*

The second stage in the framework consists of the 3D positioning of the UAVs within region $S$ based on the sum secrecy obtained by each UAV, having $\mathcal{L}_m$ be the set of legitimate nodes associated to UAV $m$.

For the UAV positioning, the following optimization subproblem is formulated

$$\mathcal{P}2: \quad \max_{\mathbf{A},\{\mathbf{x}_m\}_{m\in\mathcal{M}}} \quad \Phi = \sum_{l\in\mathcal{L}} \phi_l \tag{21a}$$

$$\text{s.t.} \quad (15c), (15d), (15e). \tag{21b}$$

The positioning of the UAVs, unlike the association of the nodes, is performed over a continuous domain which is the entire region, with a continuous altitude range, for all of the UAVs. Heuristic methods have shown to work well over a continuous space, such as particle swarm optimization [39] and genetic algorithm [40]. However, these methods require increased complexity, continuous coordination between the agents, and longer convergence time. While the outcomes from these continuous-domain algorithms are close to optimum values, discrete-domain algorithms may provide simpler and satisfactory solutions, which is beneficial when considering resource-limited IoT nodes.

Thus, a two-stage positioning protocol is proposed, where a global 2D $M$-centroid clustering is solved as the first stage, then an individual altitude selection is performed over the altitude range $\Delta z$ discretized over $N_z$ altitude levels. The set of discretized altitude levels is denoted as $\mathcal{Z}$, with $|\mathcal{Z}| = N_z$. The two stages of this protocol are described in the following.

*1) 2D Clustering:* For the 2D positioning, we aim at finding the 2D points with the highest concentration of legitimate nodes, or barycenters of the concentrations of nodes, which will privilege the best secrecy coverage. For this purpose, the unsupervised learning algorithm k-means clustering [41] is applied, which returns the centroids of the clusters (points in the area) and the members of each cluster. A diagram of this algorithm can be seen in Fig. 2.

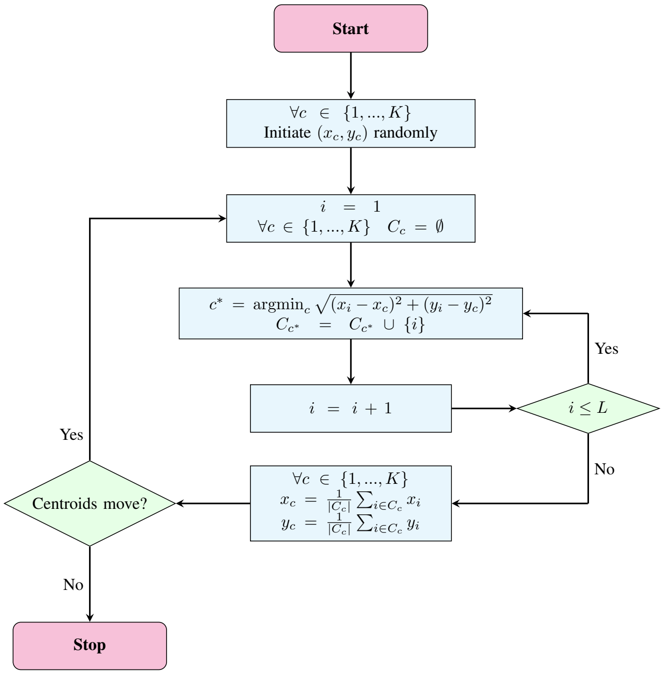
Start
$\forall c \in \{1,...,K\}$ Initiate $(x_c, y_c)$ randomly
$i = 1$ $\forall c \in \{1,...,K\}$ $C_c = \emptyset$
$c^* = \text{argmin}_c \sqrt{(x_i - x_c)^2 + (y_i - y_c)^2}$ $C_{c^*} = C_{c^*} \cup \{i\}$
Yes
$i = i + 1$
$i \leq L$
Yes
No
$\forall c \in \{1,...,K\}$ $x_c = \frac{1}{|C_c|}\sum_{i\in C_c} x_i$ $y_c = \frac{1}{|C_c|}\sum_{i\in C_c} y_i$
Centroids move?
No
Stop

Fig. 2. K-means algorithm flowchart

The k-means algorithm requires the knowledge of the position of the legitimate nodes of the system. Then, the algorithm is run at some central unit (one of the UAVs) only once for the real positions of the nodes.

*2) Best Response Dynamics:* Once the UAV 2D positioning is solved, the UAV altitude selection problem can be formulated as a game consisting of

- **Players:** UAVs $m \in \mathcal{M}$.
- **Actions:** discrete altitude levels $r_m = z_m \in \mathcal{Z}$.
- **Payoffs:** the sum secrecy metric obtained by their associated nodes $f_m(r_m) = \Phi_m(r_m) = \sum_{l\in\mathcal{L}_m} \phi_l$.

We utilize a best response algorithm to solve the positioning problem with a modified payoff into the marginal gain payoff of UAV $m$ for choosing altitude $r'_m$:

$$f_m(r'_m) = \Phi_m(r'_m) - \Phi_m(r_m). \tag{22}$$

where $r_m$ is the current position of UAV $m$. Then this algorithm considers the simple action selection per UAV, i.e. $r_m = \text{argmax}_{z_m\in\mathcal{Z}}\, z_m$, which is performed simultaneously and independently at each UAV. This algorithm is described at Algorithm 2.

**Algorithm 2:** Best response for UAV altitude positioning algorithm

```
counter ← 0;
while counter < n_iter do
    conv_flag ← 1 ;
    for $m \in \mathcal{M}$ do
        $\mathcal{A}_m \leftarrow \mathcal{Z}$;
        $f_m(r) \leftarrow$ compute as in (22) $\forall r \in \mathcal{A}_m$;
        $\mathcal{A}_m \leftarrow \mathcal{A}_m \setminus \{r \in \mathcal{A}_m \;\; s.t. \;\; f_m(r) \leq 0\}$ ;
        if $\mathcal{A}_m \neq \emptyset$ then
            $f_{m,\max} \leftarrow \max_{r\in\mathcal{A}_m} f_m(r)$ ;
            $\mathcal{A}_{m,\max} \leftarrow \{r \in \mathcal{A}_m \;\; s.t. \;\; f_m(r) = f_{m,\max}\}$;
            $z_m \leftarrow$ choose from $r \in \mathcal{A}_{m,\max}$ randomly;
            conv_flag ← 0 ;
            Make UAV $m$ assume altitude $z_m$;
    end
    if conv_flag == 1 then
        Stop the positioning process ;
    counter ← counter + 1;
end
```

The information required for Algorithm 2 is local to each UAV, disregarding the strategy taken by other UAVs or their exact positions. This algorithm is fast compared to exhaustive search, and it usually converges within two or three iterations.

## C. Secure Power Allocation

In the third and final stage, each UAV allocates its available power to the nodes associated to them. To this end, the following convex optimization problem is addressed

$$\mathcal{P}3: \quad \max_{\mathbf{P}} \quad \sum_{l\in\mathcal{L}} \phi_l \tag{23a}$$

$$\text{s.t.} \quad (15f).$$

In $\mathcal{P}3$, the objective (23a) is non-convex on $\mathbf{P}$, so this problem cannot be directly solved. Moreover, the condition for secrecy for a user is given by (11), which cannot be guaranteed to all nodes. In that case, the power optimization formulation as expressed in $\mathcal{P}3$ will allocate all the power budget only to the nodes that can achieve secrecy, leaving without power to those that cannot, which is not desirable. Alternatively, a consideration is added to the original problem in order to guarantee a minimum SINR requirement to every node in the system. To that purpose, the set $\mathcal{L}_m^S$ is introduced as the set of nodes associated to UAV $m$ that can be guaranteed secrecy, that is to say, for which (11) holds. Afterwards, the proposed optimization problem is a max-min secrecy rate problem for the nodes in $\mathcal{L}_m^S$, performed locally at each UAV, expressed as

$$\max_{\mathbf{p}_m} \min_{l\in\mathcal{L}_m^S} \quad \log_2\left(\frac{1+\gamma_l}{1+\gamma_{e*}}\right) \tag{24a}$$
$$\text{s.t.} \quad \gamma_l > \gamma_0 \qquad \forall l \in \mathcal{L}_m \tag{24b}$$
$$\sum_{c\in\mathcal{C}} p_m^c \leq P, \tag{24c}$$

An equivalent optimization problem can be formulated as

$$\mathcal{P}3' : \quad \max_{\mathbf{p}_m} \quad R_S \tag{25a}$$
$$\text{s.t.} \quad \gamma_l > \gamma_0 \qquad \forall l \in \mathcal{L}_m \tag{25b}$$
$$\log_2\left(\frac{1+\gamma_l}{1+\gamma_{e*}}\right) > R_S \quad \forall l \in \mathcal{L}_m^S \tag{25c}$$
$$\sum_{c\in\mathcal{C}} p_m^c \leq P, \tag{25d}$$

In this formulation, the interference perceived at each node is assumed constant over the optimization process, and an iterative optimization scheme can be applied. Thus, the interference at its associated nodes are computed at each UAV, and problem $\mathcal{P}3'$ is solved in parallel in all UAVs. Then the updated interference terms are computed, and the process is repeated until convergence or for a number of iterations.

Once $\mathcal{P}3'$ is convex, it can be split into two subproblems, $\mathcal{P}3'$a and $\mathcal{P}3'$b, as

$$\mathcal{P}3'\text{a} : \quad \min_{\mathbf{p}_m^{(a)}} \quad P_{NS} \tag{26a}$$
$$\text{s.t.} \quad \gamma_l > \gamma_0 \quad \forall l \in \mathcal{L}_m. \tag{26b}$$

$$\mathcal{P}3'\text{b} : \quad \max_{\mathbf{p}_m^{(b)}} \quad R_S \tag{27a}$$
$$\text{s.t.} \quad \log_2\left(\frac{1+\gamma_l}{1+\gamma_{e*}}\right) > R_S \quad \forall l \in \mathcal{L}_m^S \tag{27b}$$
$$\sum_{c\in\mathcal{C}} p_m^{c,(b)} \leq P_S, \tag{27c}$$

where $\mathbf{p}_m^{(a)}$ is the power profile for the minimum SINR requirement, and $\mathbf{p}_m^{(b)}$ is the power profile for the max-min secrecy rate optimization, such that $\mathbf{p}_m = \mathbf{p}_m^{(a)} + \mathbf{p}_m^{(b)}$, $P_{NS}$ is the power used to meet the minimum SINR requirement, and $P_S = [P - P_{NS}]^+$ is the power available for max-min secrecy rate optimization.

First, problem $\mathcal{P}3'$a is solved for the power profile $\mathbf{p}_m^{(a)}$ and power $P_{NS}$ is found, which is power required to guarantee the minimum SINR $\gamma_0$ for all associated nodes. If $P_{NS} \geq P$, there is not enough power to meet the SINR constraint, then the overall local power profile is taken as $\mathbf{p}_m = \mathbf{p}_m^{(a)}(P/P_{NS})$, and the local power allocation process ends. If $P_{NS} < P$, then the available power for the max-min secrecy rate problem is assumed as $P_S = P - P_{NS}$, and the problem $\mathcal{P}3'$b is solved by obtaining the power profile $\mathbf{p}_m^{(b)}$, and the overall local power profile is given as $\mathbf{p}_m = \mathbf{p}_m^{(a)} + \mathbf{p}_m^{(b)}$.

The closed form solution for problem $\mathcal{P}3'$a is given as

$$p_m^{c,(a)} = \gamma_0 \left(\frac{I_{m,l}^c + 1}{g_{m,l}}\right) \quad \forall l \in \mathcal{L}_m \tag{28}$$

Problem $\mathcal{P}3'$b can be solved by bisection over the following minimum power optimization problem

$$\mathcal{P}3'\text{b}' : \quad \min_{\mathbf{p}_m^{(b)}} \quad P_S \tag{29a}$$
$$\text{s.t.} \quad \frac{1+\gamma_l}{1+\gamma_{e*}} > \gamma_S \quad \forall l \in \mathcal{L}_m^S. \tag{29b}$$

where $\gamma_S = 2^{R_S}$. This problem has the following closed-form solution

$$p_m^{c,(b)} = \left[\frac{\gamma_S - 1}{\frac{g_{m,l}}{I_{m,l}^c+1} - \gamma_S\left(\frac{g_{m,e*}}{I_{m,e*}^c+1}\right)}\right]^+ \quad \forall m \in \mathcal{L}_m. \tag{30}$$

Considering that this problem is solved for nodes that can achieve secrecy, and assuring that $p_m^{c,(b)}$ is non-zero, the bounds for $\gamma_S$ are

$$1 < \gamma_S < \min_{l\in\mathcal{L}_m^S}\left\{\frac{\frac{g_{m,l}}{I_{m,l}^c+1}}{\frac{g_{m,e*}}{I_{m,e*}^c+1}}\right\} \tag{31}$$

All in all, to solve problem $\mathcal{P}3'$b, bisection is performed on problem $\mathcal{P}3'$b$'$ with closed form solution (30), over $\gamma_S$, whose initial minimum and maximum values are given by the bounds in (31). The power allocation algorithm is described in Algorithm 3.

## IV. Results and Discussion

In this section, the performance of the proposed framework is evaluated through Monte Carlo simulations. For that purpose, unless otherwise stated, the adopted simulation parameters are presented in Table III. Therein, $\gamma_P = P/N_0$ is the total transmit SNR of each UAV, and $N_{it}$ is the number of iterations for a given realization of the system. The number of UAVs $M$ to be deployed is chosen such that $(M-1)C < L \leq MC$.

Unless otherwise stated, for each realization the following steps are taken

1) The $N$ nodes are distributed over the region following a binomial point process.
2) Legitimate nodes are selected following a Bernoulli distribution of parameter $q$.
3) The association, positioning and power allocation processes are performed subsequently a number $N_{it}$ of iterations.

### A. Association and Positioning Benchmarks

Two association and positioning benchmarks are presented for the sake of comparison:

1) **Greedy Association [29]:** Framework with greedy association algorithm from [29]. This approach iteratively

**Algorithm 3:** Secure power allocation algorithm

```
while $counter < n\_iter\_pow$ do
    for $m \in \mathcal{M}$ do
        for $l \in \mathcal{L}_m$ do
            $I_{m,l} \leftarrow$ compute as in (12);
            $I_{m,e*} \leftarrow$ compute as in (12);
        end
    end
    for $m \in \mathcal{M}$ do
        $\mathcal{L}_m^S \leftarrow \{\}$;
        for $l \in \mathcal{L}_m$ do
            if (11) holds then
                $\mathcal{L}_m^S \leftarrow \mathcal{L}_m^S \cup \{l\}$;
        end
        for $l \in \mathcal{L}_m$ do
            $p_m^{c,(a)} \leftarrow$ compute as in (28);
        end
        $P_{NS} \leftarrow \sum_{l \in \mathcal{L}_m} p_m^{c,(a)}$;
        if $P_{NS} \geq P$ OR $\mathcal{L}_m^S$ is empty then
            for $l \in \mathcal{L}_m$ do
                $p_m^c \leftarrow p_m^{c,(a)}(P/P_{NS})$ ;
            end
            continue;
        $P_S \leftarrow P - P_{NS}$;
        $\gamma_{\min}, \gamma_{\max} \leftarrow$ set according to (31);
        while $counter\_bis < n\_iter\_bis$ do
            $\gamma_S \leftarrow \frac{1}{2}(\gamma_{\min} + \gamma_{\max})$;
            for $l \in \mathcal{L}_m^S$ do
                $p_m^{c,(a)} \leftarrow$ compute as in (30);
            end
            if $\sum_{l \in \mathcal{L}_m} p_m^{c,(b)} > P_S$ then
                $\gamma_{\max} \leftarrow \gamma_S$;
            if $\sum_{l \in \mathcal{L}_m} p_m^{c,(b)} < P_S$ then
                $\gamma_{\min} \leftarrow \gamma_S$;
        end
        for $l \in \mathcal{L}_m^S$ do
            $p_m^c \leftarrow p_m^{c,(a)} + p_m^{c,(b)}$;
        end
    end
    counter $\leftarrow$ counter + 1;
end
```

| Parameter | Value | Parameter | Value |
|---|---|---|---|
| $N_{it}$ | 5 | $\gamma_P$ | 20 $dB$ |
| $x_{\min}$ | 0 m | $q$ | 0.5 |
| $x_{\max}$ | 1000 m | $\psi$ (Urban) | 9.61 |
| $y_{\min}$ | 0 m | $\omega$ (Urban) | 0.16 |
| $y_{\max}$ | 1000 m | $\eta_{\text{LoS}}$ (Urban) | 1.0 |
| $z_{\min}$ | 20 m | $\eta_{\text{NLoS}}$ (Urban) | 20 |
| $z_{\max}$ | 300 m | $\alpha_G$ (Urban) | 0.3 |
| $C$ | 8 | $\alpha_J$ (Urban) | 0.3 |
| $BW$ | 20 MHz | $N$ | 80 |
| $f_c$ | 2 GHz | $N_z$ | 8 |

TABLE III
MONTE CARLO SIMULATIONS COMMON PARAMETERS.

associates the best node-UAV pair through the system in terms of SINR, until all nodes are associated.

2) **Adapted Greedy [29]:** Framework with adapted greedy algorithm for association and positioning from [29]. This approach positions each UAV one by one, and associates to it the nodes that present the best secrecy, until all UAVs are positioned, and all nodes associated.

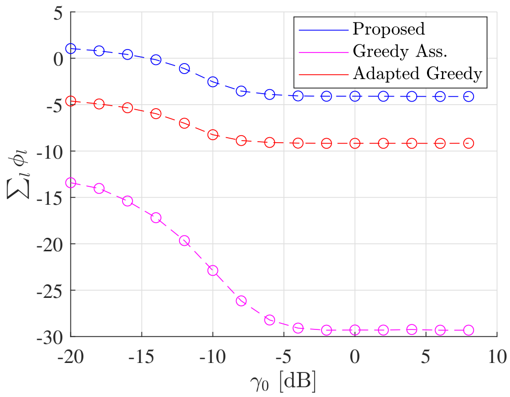

Fig. 3. Average sum secrecy metric vs. minimum SINR constraint $\gamma_0$ obtained by different frameworks.

Fig. 3 shows the sum secrecy of the system versus $\gamma_0$ for the proposed secure power allocation scheme, and results are compared to the benchmarks described above. It can be seen that, the proposed framework vastly outperforms the benchmarks. Particularly, for smaller $\gamma_0$ values more power is allocated for the max-min secrecy rate subproblem by reducing the constraint on the communication quality of service (QoS). Thus, the curves present higher sum secrecy metric for low $\gamma_0$. Moreover, although the optimization problem was performed for the secrecy metric $\phi_l$, the initial objective is to increase the proportional number of nodes with positive secrecy in the system, as illustrated in the following figure.

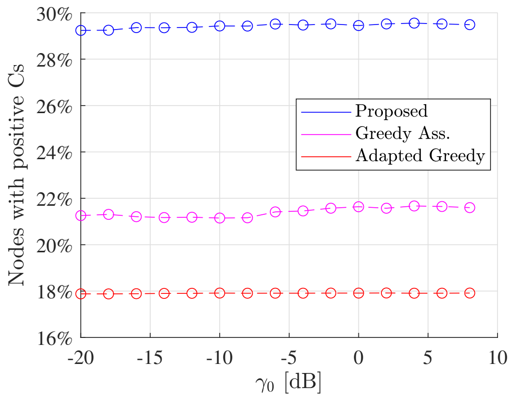

Fig. 4. Average percentage of legitimate nodes with positive secrecy rate vs. minimum SINR constraint $\gamma_0$ obtained by different frameworks.

Fig. 4 shows the percentage of legitimate nodes with positive secrecy rate versus $\gamma_0$. A small fluctuation can be appreciated for varying values of $\gamma_0$, where the proposed scheme greatly outperforms the benchmarks.

Fig. 5 shows the percentage of legitimate nodes with positive secrecy rate versus the rate of activation of the IoT nodes $q$. It can be seen that the proposed scheme outperforms the benchmarks for any value of $q$ between 0.1 and 0.9. However, as $q$ decreases, the proposed secure scheme approaches the level of the benchmarks, with a small proportion of nodes achieving positive secrecy. This occurs because if $q$ is small, then a small proportion of the IoT nodes are legitimate nodes, while the rest are considered as eavesdroppers. Then, due to

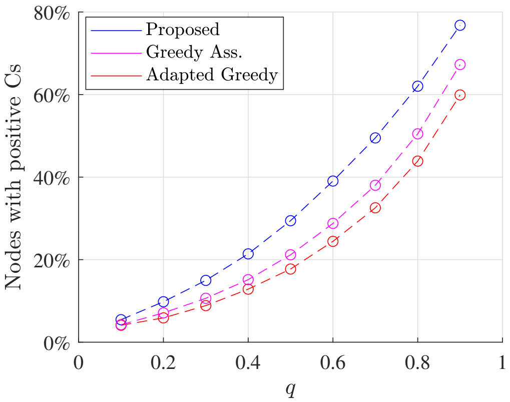

Fig. 5. Average percentage of legitimate nodes with positive secrecy rate vs. node activation rate $q$.

the relative large amount of eavesdroppers, it becomes less likely for the legitimate nodes to be able to obtain positive secrecy.

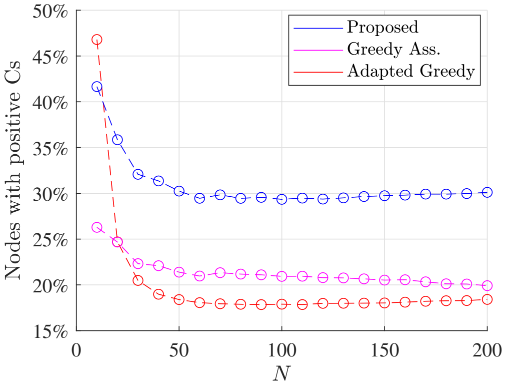

Fig. 6. Average percentage of legitimate nodes with positive secrecy rate vs. number of IoT nodes in the system $N$, obtained by different frameworks.

Fig. 6 shows the percentage of legitimate nodes that achieve positive secrecy rate versus the number of nodes in the system $N$, with $\gamma_0 = -10$dB and $M$ chosen such that $(M-1)C < L \leq MC$. The proposed framework clearly outperforms the benchmarks for $N > 10$. Moreover, note that there is an initial drop in the percentage of users with positive secrecy for small $N$ values due to the added interference of an increasing number of UAVs. However, after the point around $N = 50$, the percentage of users with positive secrecy in the system remains steady, since the amount of interference is proportional to the number of nodes in the system.

### B. Convergence Analysis

Consider the objective function of optimization problem $\mathcal{P}$, which is $\Phi$, as formulated in (21a). Then, let $\Phi_o(t)$ be the value of $\Phi$ at the beginning of iteration $t$. Likewise, let $\Phi_a(t)$, $\Phi_{m1}(t)$, $\Phi_{m2}(t)$ and $\Phi_p(t)$ be the value of $\Phi$ after association, horizontal positioning, vertical positioning, and power allocation respectively, such that $\Phi_o(t+1) = \Phi_p(t)$.

Let us consider any iteration $t$ such that $t > 1$, i.e. the first iteration has already been performed. We have that $\Phi_o(t) = \Phi_p(t-1)$. For the association stage at iteration $t$, all of the nodes are already associated from the result of the association stage at iteration $t-1$. Note that, in Algorithm 1, the nodes will only choose to change their current resource if it is not occupied by another node, and if this change leads to an increment in the current payoff. This, together with the conflict resolution mechanisms guarantees that the resulting $\Phi$ value of the association will not be lower than the initial condition at time $t$, so that $\Phi_a(t) \geq \Phi_o(t)$.

The horizontal positionining is obtained by executing a k-means algorithm over the positions of the IoT nodes. Thus, given that this algorithm already ran in the previous iteration, and that the position of the IoT nodes has not changed, it follows that $\Phi_{m1}(t) = \Phi_a(t)$. Next, the vertical positioning of the UAVs follows a similar logic to the association game, in which the UAVs will choose a different altitude only if it increases their current local $\Phi_m$ value. Thus, it follows that $\Phi_{m2}(t) \geq \Phi_{m1}(t)$.

By sequentially improving the value of $\Phi$, the association and positioning stages eventually converge to an optimal $\Phi$ value. Regarding power allocation, first, let us note that the optimization problem $\mathcal{P}3'$ changes its objective function to guarantee the fairness of secrecy rate across nodes that do achieve secrecy, while providing a minimum of service to all nodes. By constraint (25c) of problem $\mathcal{P}3'$, it is guaranteed that the number of nodes that can achieve secrecy is not decreased. Thus, it follows that

$$\sum_{l\in\mathcal{L}} \mathbb{1}_{\phi_l>0,m2} \geq \sum_{l\in\mathcal{L}} \mathbb{1}_{\phi_l>0,p}, \tag{32}$$

where $\mathbb{1}_{\phi_l>0,m2}$ and $\mathbb{1}_{\phi_l>0,p}$ are indicator functions before and after power allocation, respectively. Correspondingly, they equal 1 if $\phi_l > 0$ and 0 otherwise. With this in mind, after power allocation the number of users with positive secrecy is not decreased, eventually converging to an optimum. To further illustrate the convergence of the BCA algorithm consider Fig. 7.

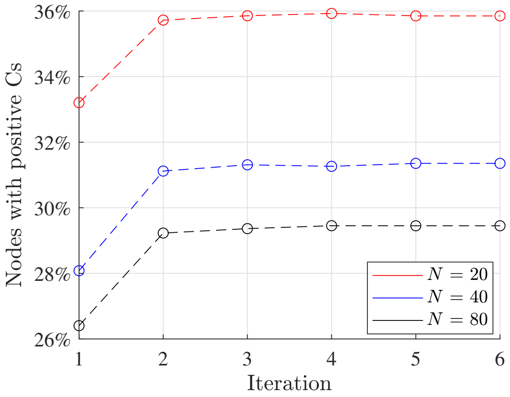

Fig. 7. Average percentage of legitimate nodes with positive secrecy rate vs. number of iterations of BCA algorithm for different values of $N$.

In Fig. 7, it is illustrated the average percentage of legitimate nodes that achieve positive secrecy rate at every step of the iterative algorithm. It can be observed that the algorithm converges, on average, within two iterations, and that it converges faster for a system with lower number of nodes.

This is expected, as fewer nodes in the system reduce the chances of leakage, thus increasing the opportunities of secret transmissions among all nodes. The small fluctuations in the curves can be explained by the different instances of fading in the communication channels from one iteration to the next.

To emphasize the advantage of our proposal, in Table IV the time complexity of our algorithm is compared to the greedy association and adapted greedy benchmarks in terms of convergence time for $N = 80$. Note that the increased complexity of the benchmarks in their executions require more coordination, and take a longer time to converge. As an illustrative example of time complexity, let $T_{\text{ass}}$, $T_{\text{pos}}$ and $T_{\text{pow}}$ be the running times for a round of association, positioning and power allocation iterations. Then, note that, for $N = 80$, the node association process in the proposed framework converges in less than 10 iterations, the UAV positioning converges in less than 3 iterations, and the overall framework converges in less than 3 iterations.

| Framework | Convergence Time |
|---|---|
| Proposed | $3(10T_{\text{ass}} + 2T_{\text{pos}} + T_{\text{pow}})$ |
| Greedy Ass. | $3(NT_{\text{ass}} + 2T_{\text{pos}} + T_{\text{pow}})$ |
| Adapted Greedy | $(N_zT_{\text{ass}} + N_zT_{\text{pos}})M + +T_{\text{pow}}$ |

TABLE IV
CONVERGENCE TIMES.

Therefore, the proposed framework presents much faster convergence times than the greedy algorithms presented in [29].

### C. Complexity Analysis

For the association Algorithm 1, consider that the processing is done locally at each IoT node. In the worst-case scenario, they have to compute the metric of interest for every subchannel in every UAV and repeat this until convergence, while also every node chooses the same resource at each iteration but only one is assigned to it. Considering this, Algorithm 1 presents a complexity of $\mathcal{O}(NMC)$. For the positioning Algorithm 2, the processing is done locally at each UAV for every permitted altitude, and this process continues until convergence, or until a fixed maximum number of iterations $n\_iter$, thus its complexity is of $\mathcal{O}(N_z)$. Finally, for the power allocation in Algorithm 3, the algorithm is executed locally at each UAV for a number of $n\_iter\_pow$ iterations. Therefore, problem $\mathcal{P}3'$ is solved by solving problems $\mathcal{P}3'a$ and $\mathcal{P}3'b$, sequentially. To solve $\mathcal{P}3'a$, each UAV computes (28) for every user associated to it, which is upper bounded by the amount of subchannels supported by the UAV, which is $C$. On the other hand, $\mathcal{P}3'b$ is solved through bisection by iterating over $\mathcal{P}3'b'$ a maximum of $n\_iter\_bis$ times, and (30) is computed for every user associated to it that achieves secrecy, upper bounded by $C$. Thus, the number of computations is given by $n\_iter\_pow(C + C(n\_iter\_bis))$. Assuming a fixed number of maximum iterations, the complexity is given by $\mathcal{O}(C)$. Thus, the complexity of the proposed framework is given by $\mathcal{O}(NMC + N_z)$.

### D. Power Allocation Benchmarks

To compare the proposed secure power allocation strategy, the following power allocation benchmarks are considered

1) **Max. Min SINR:** An iterative local max-min SINR power allocation per UAV. It solves the following optimization problem

$$\max_{\mathbf{p}_m} \min_{l \in \mathcal{L}_m} \quad \gamma_l \tag{33a}$$
$$\text{s.t.} \quad \gamma_l > \gamma_0 \qquad \forall l \in \mathcal{L}_m \tag{33b}$$
$$\sum_{c \in \mathcal{C}} p_m^c \leq P, \tag{33c}$$

This power allocation scheme targets to guarantee the same SINR to all the nodes served by a given UAV.

2) **Max. Sum-Rate:** An iterative local sum-rate maximization power allocation per UAV. It solves the following optimization problem

$$\max_{\mathbf{p}_m} \quad \sum_{l \in \mathcal{L}_m} \log_2(1 + \gamma_l) \tag{34a}$$
$$\text{s.t.} \quad \sum_{c \in \mathcal{C}} p_m^c \leq P, \tag{34b}$$

This power allocation scheme seeks to maximize the sum-rate across all of the nodes served by a UAV. By doing so, it may cause some nodes to have no power allocated to them.

The proposed power allocation strategy as well as the power allocation benchmarks are performed with the secure association and positioning phases proposed.

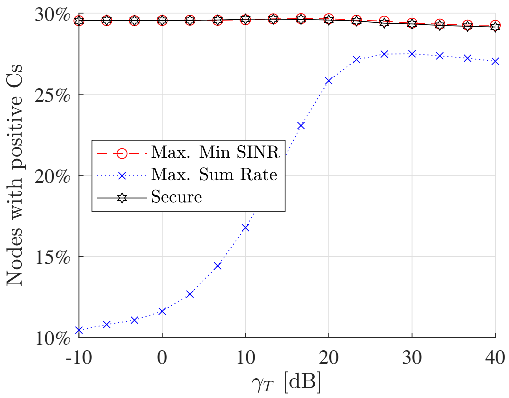

Fig. 8. Average percentage of legitimate nodes with positive secrecy rate vs.transmit SNR available to UAVs, obtained by the different power allocation schemes.

Fig. 8 shows the percentage of legitimate nodes that are able to achieve positive secrecy rate versus $\gamma_T$, for the proposed secure power allocation scheme compared to the benchmarks and $\gamma_0 = -10$dB. Note that the proposed secure power allocation scheme presents a similar behavior compared to the max-min SINR benchmark. However, it can be seen that the max. sum-rate benchmark presents a significant smaller number of users that can achieve secrecy in the system due to all the power being allocated only to the users with strongest channels. Even for high $\gamma_T$ values, the performance of max. sum-rate benchmark is still worse than the proposed secure power allocation in terms of users that achieve positive secrecy rates in the system. While the secure power allocation scheme achieves similar performance to the max-min SINR power allocation scheme, it is worth noting that it has a gain over the latter in terms of secrecy rate, as is displayed in the next figure.

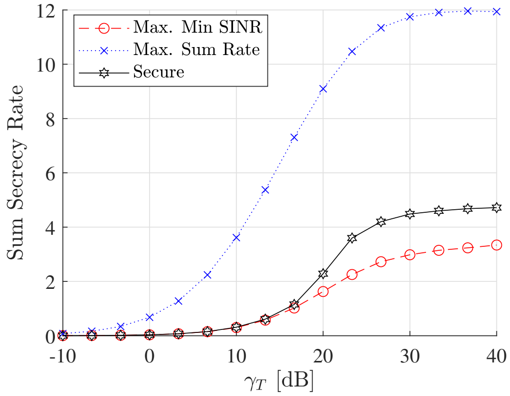

Fig. 9. Average sum secrecy rate vs. transmit SNR available to UAVs, obtained by the different power allocation schemes.

Fig. 9 shows the sum secrecy rate of the system versus $\gamma_T$ for the proposed secure power allocation scheme compared to the benchmarks with $\gamma_0 = -10$dB. It can be seen that for smaller transmit SNR values, the proposed power allocation scheme matches with the max-min benchmark. This behavior occurs because, at these ranges of $\gamma_T$, there is not enough transmit SNR to satisfy the minimum SINR requirement, so no power is allocated for $P_S$. At higher $\gamma_T$ values, the proposed scheme outperforms the max-min benchmark, as power is allocated for secrecy improvement after fulfilling the minimum SINR requirements for all nodes. On the other hand, the max. sum-rate benchmark outperforms the proposed secure power allocation scheme in terms of sum secrecy rate. However, the max. sum-rate scheme allocates all the power of a given UAV to the nodes with the strongest channel to it. This causes the nodes with weaker channels to their serving UAV to receive no power from it, effectively disconnecting a large number of nodes from the network.

## V. Conclusions

In this work, an IoT scenario was investigated, where a swarm of UAVs, acting as ABSs, provide coverage to a group of ground nodes, while considering all nodes that do not participate of the communication process as eavesdroppers. In this scenario, the maximization of the number of nodes with positive secrecy is addressed by proposing a BCA secure framework consisting of the association of the ground nodes, the 3D positioning of the UAVs, and the power allocation for the associated nodes. Different approaches based on game theory and optimization-based techniques were employed. Extensive simulations were performed, for which the proposed framework achieved enhanced secrecy performance while maintaining low complexity, compared to greedy association and positioning, as well as best response dynamics benchmarks.

## Appendix A

Considering that the achievable secrecy rate for the node $l$ is given by (10) and the interference terms as in (12). Then, the condition for positive secrecy, i.e. $C_S > 0$, is obtained as

$$\left[\log_2\left(\frac{1+\frac{a_{l,m,c}\gamma_m^c g_{m,l}}{I_{m,l}^c+1}}{1+\frac{\gamma_m^c g_{m,e*}}{I_{m,e^*}^c+1}}\right)\right]^+ > 0 \tag{35}$$

$$1+\frac{a_{l,m,c}\gamma_m^c g_{m,l}}{I_{m,l}^c+1} > 1+\frac{\gamma_m^c g_{m,e*}}{I_{m,e^*}^c+1} \tag{36}$$

then, assuming $a_{l,m,c} = 1$, (36) can be expressed as

$$1+\frac{\gamma_m^c g_{m,l}}{I_{m,l}^c+1} > 1+\frac{\gamma_m^c g_{m,e*}}{I_{m,e^*}^c+1} \tag{37}$$

$$\frac{g_{m,l}}{I_{m,l}^c+1} > \frac{g_{m,e*}}{I_{m,e^*}^c+1} \tag{38}$$

## References

[1] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6G security and privacy," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1094–1122, 2021.

[2] D. P. M. Osorio, E. E. B. Olivo, H. Alves, and M. Latva-Aho, "Safeguarding MTC at the physical layer: Potentials and challenges," *IEEE Access*, vol. 8, pp. 101 437–101 447, 2020.

[3] X. Sun *et al.*, "Physical layer security in UAV systems: Challenges and opportunities," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 40–47, 2019.

[4] D. P. Moya Osorio, I. Ahmad, J. D. V. Sánchez, A. Gurtov, J. Scholliers, M. Kutila, and P. Porambage, "Towards 6G-enabled internet of vehicles: Security and privacy," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 82–105, 2022.

[5] O. M. Bushnaq, A. Chaaban, and T. Y. Al-Naffouri, "The role of UAV-IoT networks in future wildfire detection," *IEEE Internet of Things Journal*, vol. 8, no. 23, pp. 16 984–16 999, 2021.

[6] R. La Scalea *et al.*, "Opportunities for autonomous UAV in harsh environments," in *2019 16th International Symposium on Wireless Communication Systems (ISWCS)*, 2019, pp. 227–232.

[7] Y. Zhou *et al.*, "Improving physical layer security via a UAV friendly jammer for unknown eavesdropper location," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 11 280–11 284, 2018.

[8] W. Wei, X. Pang, J. Tang, N. Zhao, X. Wang, and A. Nallanathan, "Secure transmission design for aerial IRS assisted wireless networks," *IEEE Transactions on Communications*, vol. 71, no. 6, pp. 3528–3540, 2023.

[9] S. Yoo, S. Jeong, and J. Kang, "Hybrid UAV-enabled secure offloading via deep reinforcement learning," *IEEE Wireless Communications Letters*, vol. 12, no. 6, pp. 972–976, 2023.

[10] P. Chen, X. Luo, D. Guo, Y. Sun, J. Xie, Y. Zhao, and R. Zhou, "Secure task offloading for MEC-aided-UAV system," *IEEE Transactions on Intelligent Vehicles*, vol. 8, no. 5, pp. 3444–3457, 2023.

[11] H. Lu, Z. Shi, N. Zhao, A. Nallanathan, and X. Wang, "Secrecy analysis of control information for UAV," *IEEE Transactions on Vehicular Technology*, pp. 1–6, 2023.

[12] A. A. Salem, M. H. Ismail, and A. S. Ibrahim, "Active reconfigurable intelligent surface-assisted MISO integrated sensing and communication systems for secure operation," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 4, pp. 4919–4931, 2023.

[13] R. Dong, B. Wang, J. Tian, T. Cheng, and D. Diao, "Deep reinforcement learning based UAV for securing mmWave communications," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 4, pp. 5429–5434, 2023.

[14] E. Illi, M. Qaraqe, F. E. Bouanani, and S. Al-Kuwari, "On the physical-layer security of a dual-hop UAV-based network in the presence of per-hop eavesdropping and imperfect CSI," *IEEE Internet of Things Journal*, vol. 10, no. 9, pp. 7850–7867, 2023.

[15] A. Li, Q. Wu, and R. Zhang, "UAV-enabled cooperative jamming for improving secrecy of ground wiretap channel," *IEEE Wireless Communications Letters*, vol. 8, no. 1, pp. 181–184, 2019.

[16] Y. Zhou *et al.*, "Secure communications for UAV-enabled mobile edge computing systems," *IEEE Transactions on Communications*, vol. 68, no. 1, pp. 376–388, 2020.

[17] X. Pang *et al.*, "Secrecy analysis of UAV-based mmWave relaying networks," *IEEE Transactions on Wireless Communications*, vol. 20, no. 8, pp. 4990–5002, 2021.

[18] M. Kim, S. Kim, and J. Lee, "Securing communications with friendly unmanned aerial vehicle jammers," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1972–1977, 2021.

[19] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 256–266, 2011.

[20] X. A. F. Cabezas, D. P. M. Osorio, and M. Latva-aho, "Weighted secrecy coverage analysis and the impact of friendly jamming over UAV-enabled networks," in *2021 Joint European Conference on Networks and Communications 6G Summit (EuCNC/6G Summit)*, 2021, pp. 124–129.

[21] X. A. Flores Cabezas, D. P. M. Osorio, and M. Latva-Aho, "Distributed UAV-enabled zero-forcing cooperative jamming scheme for safeguarding future wireless networks," in *2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2021, pp. 739–744.

[22] X. A. Flores Cabezas, D. P. Moya Osorio, and M. Latva-aho, "Positioning and power optimisation for UAV-assisted networks in the presence of eavesdroppers: A multi-armed bandit approach," *EURASIP Journal on Wireless Communications and Networking*, 09 2022.

[23] X. A. F. Cabezas, D. P. M. Osorio, and M. Juntti, "A multi-armed bandit framework for efficient UAV-based cooperative jamming coverage," *IEEE Transactions on Vehicular Technology*, pp. 1–6, 2023.

[24] Y. Li, W. Wang, M. Liu, N. Zhao, X. Jiang, Y. Chen, and X. Wang, "Joint trajectory and power optimization for jamming-aided noma-UAV secure networks," *IEEE Systems Journal*, vol. 17, no. 1, pp. 732–743, 2023.

[25] T. Zeng, O. Semiari, M. Mozaffari, M. Chen, W. Saad, and M. Bennis, "Federated learning in the sky: Joint power allocation and scheduling with UAV swarms," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–6.

[26] N. Zhao, Y. Cheng, Y. Pei, Y.-C. Liang, and D. Niyato, "Deep reinforcement learning for trajectory design and power allocation in UAV networks," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–6.

[27] G. Fragkos, N. Kemp, E. E. Tsiropoulou, and S. Papavassiliou, "Artificial intelligence empowered UAV data offloading in mobile edge computing," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–7.

[28] K. Li, W. Ni, E. Tovar, and A. Jamalipour, "Deep Q-Learning based resource management in UAV-assisted wireless powered IoT networks," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–6.

[29] H. E. Hammouti, D. Hamza, B. Shihada, M.-S. Alouini, and J. S. Shamma, "The optimal and the greedy: Drone association and positioning schemes for internet of UAVs," *IEEE Internet of Things Journal*, vol. 8, no. 18, pp. 14 066–14 079, 2021.

[30] L. Xiao, C. Xie, M. Min, and W. Zhuang, "User-centric view of unmanned aerial vehicle transmission against smart attacks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 4, pp. 3420–3430, 2018.

[31] J. Liu and W. Yang, "Secure UAV communication against cooperative adaptive eavesdroppers," *Wireless Networks*, vol. 28, no. 3, pp. 1113–1128, 2022. [Online]. Available: www.scopus.com

[32] C. You and R. Zhang, "3D trajectory optimization in rician fading for UAV-enabled data harvesting," *IEEE Transactions on Wireless Communications*, vol. 18, no. 6, pp. 3192–3207, 2019.

[33] V. Dao, H. Tran, S. Girs, and E. Uhlemann, "Reliability and fairness for UAV communication based on non-orthogonal multiple access," in *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2019, pp. 1–6.

[34] A. Al-Hourani, S. Kandeepan, and S. Lardner, "Optimal LAP altitude for maximum coverage," *IEEE Wireless Communications Letters*, vol. 3, no. 6, pp. 569–572, 2014.

[35] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[36] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[37] J. R. Marden and J. S. Shamma, "Revisiting log-linear learning: Asynchrony, completeness and payoff-based implementation," *Games and Economic Behavior*, vol. 75, no. 2, pp. 788–808, 2012. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0899825612000462

[38] M. Hasanbeig and L. Pavel, "From game-theoretic multi-agent log linear learning to reinforcement learning," *ArXiv*, vol. abs/1802.02277, 2018.

[39] M. R. Bonyadi and Z. Michalewicz, "Particle Swarm Optimization for Single Objective Continuous Space Problems: A Review," *Evolutionary Computation*, vol. 25, no. 1, pp. 1–54, 03 2017. [Online]. Available: https://doi.org/10.1162/EVCO_r_00180

[40] M. Mitchell, *An Introduction to Genetic Algorithms*. Cambridge, MA, USA: MIT Press, 1998.

[41] M. Ahmed, R. Seraj, and S. M. S. Islam, "The k-means algorithm: A comprehensive survey and performance evaluation," *Electronics*, vol. 9, no. 8, 2020. [Online]. Available: https://www.mdpi.com/2079-9292/9/8/1295

**Xavier Alejandro Flores Cabezas** is currently a Doctoral Candidate at Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg. He worked as a Doctoral Researcher and obtained his M.Sc. degree in wireless communications engineering from University of Oulu, Finland, during which he published several conference and journal papers, and won the student best paper award in the 2021 Joint EuCNC & 6G Summit. He has served as reviewer for several journals and conferences. His research interests include resource allocation in non-terrestrial networks, unmanned aerial vehicles for wireless communications, integrated sensing and communications and physical-layer security.

**Diana Pamela Moya Osorio** (M'16, SM'23) is currently Associate Professor at the Communication Systems Division, Department of Electrical Engineering, Linköping University, Sweden, and an ELLIIT recruited faculty. Previously, she was Senior Research Fellow and Adjunct Professor at the Centre for Wireless Communications, University of Oulu, Finland. She received the B.Sc. degree in electronics and telecommunications engineering from the Armed Forces University, Ecuador, in 2008, and the M.Sc. and D.Sc. degrees in electrical engineering with emphasis on telecommunications and telematics from the University of Campinas, Brazil, in 2011 and 2015, respectively. From 2015 to 2022, she was an Assistant Professor with the Department of Electrical Engineering, Federal University of São Carlos, Brazil. From 2020 to 2023, she was also a Postdoctoral Researcher for the Academy of Finland. She has served as TPC and reviewer for several journals and conferences. Currently, she is Associate Editor of IEEE Wireless Communications Letters and IEEE Transactions on Information Forensics & Security. She also serves as working group leader for Trustworthy 6G at the Cost Action 6G-PHYSEC. Her research interests include wireless communications in general, signal processing for wireless communications, physical layer security, and integrated sensing and communications.