UAV-assisted Secure Uplink Communications in Satellite-supported IoT: Secrecy Fairness Approach

Zhisheng Yin, *Member IEEE,* Nan Cheng, *Member IEEE*, Yunchao Song, *Member IEEE*, Yilong Hui, *Member IEEE*, Yunhan Li, Tom H. Luan, *Senior Member IEEE*, and Shui Yu, *Fellow IEEE*

***Abstract*—The escalating growth of the Internet of things (IoT) has intensified the demand for dependable and efficient communication networks to accommodate the massive data volumes produced by interconnected devices. Satellite networks have emerged as a promising alternative, particularly in remote and underserved regions where terrestrial communication infrastructures are inadequate. Nevertheless, guaranteeing secure uplink communications in satellite-based IoT networks is a daunting task due to similar satellite channels and limited resources at IoT nodes. In this paper, we explore the potential of unmanned aerial vehicle (UAV) to improve the secrecy performance of uplink transmissions in satellite-supported IoT networks. Specifically, we first introduce a framework for UAV-aided secure uplink communications, presuming a secure UAV-to-satellite connection. To mitigate the risks of ground eavesdroppers intercepting uplink transmissions, we develop a max-min secrecy rate optimization problem with uplink power constraints. To address this non-convex problem, a streamlined two-stage optimization approach is proposed. In inner stage, we combine uplink power allocation and UAV beamforming and propose a successive convex approximation (SCA) based joint optimization algorithm to address them. In outer stage, we propose an synergized bisection and coordinate descent algorithm to optimize UAV positioning. Convergence is attained by alternating iterations between these two stages. Particularly, the secrecy fairness among IoT users is reached by solving the max-min problem. Additionally, we offer a complexity analysis of the proposed algorithm and validate the efficacy of the presented approach through comprehensive simulation results.**

***Index Terms*—IoT, satellite, UAV, secure uplink, secrecy rate.**

I. INTRODUCTION

THe exponential growth of the Internet of Things (IoT) has resulted in the substantial rise in interconnected devices, producing vast amounts of data that necessitate efficient and dependable communication networks for their transmission [1], [2]. Satellite networks have surfaced as a feasible option for IoT implementations, particularly in remote and underserved regions where terrestrial communication infrastructures are insufficient or absent [3]–[5]. Satellite communication systems provide several essential advantages for IoT applications, such as extensive coverage, uninterrupted connectivity, and resilience to disasters and infrastructure breakdowns [6], [7].

Recently, Low Earth Orbit (LEO) satellite networks have gained significant interest in IoT domains due to their low latency and improved signal quality compared to Geostationary Earth Orbit (GEO) satellites [8]. The growing interest in LEO satellite networks is further fueled by the ongoing deployment of satellite constellations, e.g., SpaceX's Starlink and OneWeb etc., which aim to provide ubiquitous global connectivity [9]. However, the integration of satellite networks into the IoT ecosystem presents several challenges, particularly in terms of ensuring secure and reliable uplink communications [10]–[12].

Physical layer security plays a crucial role in protecting sensitive data transmitted by IoT devices from eavesdropping and other cyber threats [13], [14]. Whereas traditional cryptographic techniques depend on both key management and computational ability, and may not be suitable for resource-constrained IoT devices [15], [16]. Physical layer security techniques, as key-free security approaches, exploit the inherent characteristics of the wireless communication channels to ensure data confidentiality and integrity without relying on complex encryption algorithms [17], [18]. However, implementing secure communications in satellite-supported IoT networks is challenging due to the long propagation delays, high mobility, and varying channel conditions associated with satellite communications [19], [20]. Moreover, for the uplink transmission, the resource usage of individual nodes is subject to limitations, e.g., power and antennas. This factor complicates the deployment of intricate signal processing techniques. Consequently, this scenario poses substantial challenges towards establishing secure transmission. [21]

Unmanned aerial vehicles (UAVs), as the aerial reinforcement, have been the versatile and cost-effective tool to enhance wireless communication systems, including satellite-supported IoT networks [22], [23]. Their flexibility in deployment and ability to provide line-of-sight (LoS) connections make them well-suited for supporting secure uplink communications. By acting as aerial relay nodes, UAVs can enhance the physical layer security and extend the coverage of satellite communication systems, thereby improving the overall performance and robustness of IoT networks [24], [25]. However, the related work on secure uplink transmission is still relatively lacking. Considering the inherent mobility of UAVs, the resource limitations of IoT nodes, and the complexities arising from uplink

This work was supported in part by the National Natural Science Foundation of China (No. 62201432, 62071356, and 62101429), the National Natural Science Foundation of Shaanxi Province under Grant 2022JQ-602, and the Guangzhou Science and Technology Program under Grant 202201011732.

Z. Yin, N. Cheng, Y. Hui and Tom H. Luan are with State Key Lab. of ISN, Xidian University, 710071, Xi'an, Shaanxi, China (e-mail: {zsyin, tom.luan, ylhui}@xidian.edu.cn, dr.nan.cheng@ieee.org).

Y. Song is with the College of Electronic and Optical Engineering, Nanjing University of Posts and Telecommunications, 210003, Nanjing, Jiangsu, China (e-mail: songyc@njupt.edu.cn).

Y. Li is with the Shaanxi Transportation Holding Group Co., Ltd., 710065, Xi'an, Shaanxi, China. (e-mail: lyh199433@126.com).

S. Yu is with the School of Computer Science, University of Technology Sydney, Australia. E-mail: Shui.Yu@uts.edu.au.

Corresponding author: Nan Cheng.

interference, achieving secure uplink transmission presents significant challenges in the wireless security domain. These pressing concerns have served as the catalyst for the rigorous and scholarly investigation conducted in this paper.

Departing from existing researches on uplink physical layer secure transmission, this study does not consider methods reliant on interference machinery or relay selection [21], [26], [27]. Instead, we utilize a lower-cost approach, taking into account the similarity of line-of-sight channels in satellite-to-ground and air-to-ground scenarios. The primary issue addressed here is secure uplink transmission under extremely harsh conditions, focusing on low energy consumption and cost-effectiveness for physical network nodes. Additionally, the problem of fairness among uplink nodes is also considered. Particularly, the potential of UAV-assisted secure uplink communications in satellite-supported IoT networks is studied. We propose a novel framework that leverages the inherent advantages of UAV to realize the secure transmissions in the uplink of from IoT users to LEO satellite. To combat the interception of uplink signals from IoT users by ground-based eavesdropper (Eve), we employ a UAV to securely relay the uplink transmissions. A max-min optimization problem is formulated to improve the secrecy rate performance among IoT data uplinks, considering the energy constraints of IoT users by incorporating uplink power as a limiting factor. Then the max-min secrecy fairness is realized among uplink transmissions through joint optimization of UAV placement, uplink power allocation of IoT users, and UAV beamforming. In addition, main contributions of this work are as follows:

- We establish a framework for secure uplink transmissions in satellite-supported IoT networks using UAV-assisted communication, assuming a secure UAV-to-satellite link. To tackle challenges arising from potential ground Eve intercepting uplink transmissions of IoT users, we formulate a max-min secrecy rate optimization problem, aiming to improve the overall secrecy performance among simultaneous secure uplink transmissions while constraining the uplink transmission power.
- To tackle the non-convex max-min uplink secrecy rate problem, we introduce a streamlined two-stage optimization approach. In the inner stage, we mathematically consolidate uplink power allocation and UAV beamforming, and propose an SCA-based algorithm for their joint optimization. In the outer stage, we propose the synergized bisection and coordinate descent algorithm to optimize UAV placement. Ultimately, convergence is achieved through alternating iterations between these two stages.
- The impact of uplink transmission power from IoT users on secrecy rate is analyzed, and it is revealed that the max-min problem attains its solution when the secrecy fairness among uplink transmissions is realized. Also we provide complexity analysis of proposed algorithms. Moreover, effectiveness of the proposed approach is substantiated through extensive simulation results.

The remainder of this paper is organized as follows. In Section II, we provide an overview of the satellite networks for IoT applications and discuss the challenges and opportunities associated with implementing secure uplink transmissions in satellite-supported IoT networks. We also introduce the concept of UAV-assisted secure uplink communications and explain its potential benefits for IoT networks. Section III presents system model and formulates the max-min problem by comprehensive considering the uplink power allocation, UAV beamforming, and UAV placement. In Section IV, we propose the algorithm of joint optimization of UAV placement, UAV beamforming, and uplink power allocation to solve the max-min problem and provide some discussions. Section V presents the simulation results and performance evaluation, followed by the conclusion and future research directions in Section VI.

II. Related Work

In this section, we discuss the current research progress in secure uplink communication for satellite-supported IoT networks. Satellite networks have attracted growing interest due to their potential for IoT communication, particularly in remote and underserved areas where terrestrial communication infrastructures are insufficient [28]. Various aspects of satellite-based IoT networks, including network architecture, resource allocation, and protocol design, have been explored by researchers [28], [29]. Among these aspects, the security of data transmission has become a vital concern. Recent research has emphasized cryptographic techniques, key management, and secure routing to protect the confidentiality and integrity of data transmitted over satellite networks [29], [30]. However, physical layer security, especially in uplink communication, has not been extensively investigated and remains a relatively unexplored area.

The incorporation of UAVs into satellite-supported IoT networks has shown promising results in enhancing the security of satellite-to-ground communication [31]. Stochastic analysis has been utilized to examine cooperative satellite-UAV communications, considering aerial relays to ensure a secure satellite-UAV link [32]. In [33], a two-layer Stackelberg game model has been suggested to counter full-duplex (FD) eavesdropping and jamming attacks, where malicious eavesdropping attacks are resisted by an optimal cooperative UAV transmits jamming signals. Muli-beam satellite is considered in [18] which addresses the challenge of enhancing the legitimate user's secrecy rate within a designated beam while ensuring the common communication performance for users in surrounding beams. Besides, a UAV is introduced to leveraged to act as the relay to reinforce secure satellite beam and to serve as a jammer that purposefully creates artificial noise (AN) to thwart eavesdropping attempts. Considering energy consumption limitations at UAV, analysis of ergodic capacity and achievable secrecy rate have been given in [34] for the downlink of satellite-terrestrial communications, with the UAV employing maximum-ratio combining (MRC) to receive satellite signals and enhance transmission capacity while simultaneously combating eavesdropping.

Considering computation capability and secure transmission, a double-edge secure offloading approach has been

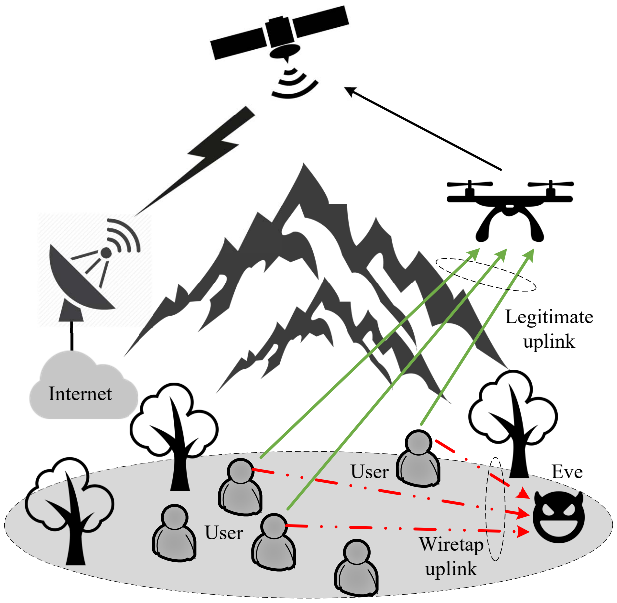


Fig. 1. UAV-assisted secure uplink communications in satellite-supported IoT.

presented in [35] for space-air-aqua integrated networks. This scheme involves UAVs securely relaying offloading for maritime mobile users and deploying jamming UAVs to protect the offloading process by determining transmit power and UAV trajectories. For power-limited or battery-free IoT devices, a secure structure has been proposed in [36] to support UAV-assisted IoT networks. This strategy includes trajectory planning for UAVs to minimize energy consumption across multiple clusters to maximize secrecy performance. In scenarios where confidential messages are transmitted to a mobile user by a UAV and AN is emitted by a cooperative UAV to deter eavesdroppers, the challenge of maximizing secrecy rates is tackled in [37]. A joint design for UAVs' 3D trajectories and time allocation is employed, taking into account practical constraints such as speed, collision avoidance, positioning error, and energy harvesting. To maximize average secrecy rates for both uplink and downlink in air-to-ground transmissions, a joint optimization framework is proposed in [38], incorporating the UAV trajectory and the transmission power of legitimate user. Besides, to maximize the average worst-case secrecy rate among UAV downlink transmissions, a joint optimization of the UAV trajectory, beamforming of intelligent reflective surface, and transmission power of legitimate users, is proposed in [39]. By employing the UAV as a relay between cluster users and terrestrial base stations, the secrecy energy efficiency is maximized by jointly adjusting the uplink transmission powers and the UAV's position [40].

Notations: $\mathrm{Tr}\left(\cdot\right)$ denotes the trace of a matrix. $rank\left(\cdot\right)$ denotes the rank of a matrix. $\triangleq$ means the redefinition. $\mathbb{C}^{a\times b}$ denotes a complex space of $a\times b$. $(\cdot)^{\dagger}$ denotes the Hermitian transpose. $\mathcal{N}\left(\mu,\delta^2\right)$ denotes the normal distribution with mean μ and variance δ^2. $\|\cdot\|$ stands for the Euclidean norm of a vector. Other notations can be found in Table I.

TABLE I
NOTATIONS AND DEFINITIONS

Notation	Definition
M	Number of IoT users within the UVA's coverage area
$\mathcal{M}$	Set of IoT user index
IU_m	The m^{th} IoT user within the UAV coverage
$\mathbf{g}_{m,u}^{\dagger}\in\mathbb{C}^{1\times N}$	The legitimate wiretap channel from IU_m to UAV
$\mathbf{g}_{m,e}^{\dagger}\in\mathbb{C}^{1\times N}$	The wiretap channel from IU_m to UAV
p_m	The transmission power of IU_m
$D_{m\to u}$	The distance from IU_m to UAV
$\mathbf{w}_m\in\mathbb{C}^{N\times 1}$	The beamforming vector at UAV receiver
R_m	The secrecy rate of transmission from IU_m to UAV
$\gamma_{m,u}$	The received SINR of transmission from IU_m to UAV
$\gamma_{e,m}$	The received SINR at for wiretapping IU_m
p_{Los}	The LoS probability
p_{NLos}	The non-LoS probability
(x_u,y_u,h_u)	The 3D coordinates of UAV
(x_m,y_m)	The 2D horizontal coordinates of IoT user
$\mathbf{g}_{\mathrm{LoS}}\in\mathbb{C}^{N\times 1}$	The LoS component of ground-to-UAV channel
$\mathbf{g}_{\mathrm{Ray}}\in\mathbb{C}^{N\times 1}$	The NLoS Rayleigh fading component
$\mathbf{W}_m$	UAV beamforming matrix ($\mathbf{W}_m=\mathbf{w}_m^{\dagger}\mathbf{w}_m$)

III. System Model and Problem Formulation

We investigate UAV-assisted secure uplink communications in satellite-supported IoT networks, as illustrated in Fig. 1. We focus on a remote area where multiple IoT devices are located within the coverage of a satellite communication, which provides backhaul connectivity to the Internet. In the uplink, IoT devices transmit confidential information to the satellite, which subsequently relays the data to Internet servers via the backhaul. To enhance the secrecy performance of uplink transmissions from IoT devices to the satellite, we propose utilizing a UAV as an aerial relay to assist the implement of physical layer security. Within the UAV's coverage area, we assume that M IoT devices are distributed following a 2D Poisson Point Process (PPP) with intensity λ_b and are denoted by the set Φ_b [41]. These IoT devices are subject to random activation, while an eavesdropper (Eve) within the same coverage area which aims to intercept the uplink transmissions. The proposed UAV-assisted secure uplink communication system seeks to protect the data transmitted by IoT devices from being compromised by the eavesdropper. By leveraging the inherent advantages of the UAV in terms of mobility and line-of-sight (LoS) connections, the system aims to improve the physical layer security of uplink communications, ensuring data confidentiality and integrity for IoT devices in satellite-supported networks.

A. Channel Models

In this paper, we follow the empirical uplink channel of satellite [42], [43], and the channel power gain at satellite is modeled as

$$H=\beta_{EIRP}l_{air}C_l\zeta, \tag{1}$$

where the β_{EIRP} is the uplink EIRP, l_{air} denotes the air absorption attenuation induced by the resonance of gas and water vapor in satellite-to-ground links, and l denotes the free-space path gain which is calculated as

$$l\left(\theta\right)=\frac{l_0}{d^2}=\frac{l_0}{r^2+\left(r+h^{so}\right)^2-2r\left(r+h^{so}\right)\cos\theta}, \quad (2)$$

where $l_0=c^2/\left(4\pi f\right)^2$ denotes the path gain with c being the speed of light and f being the center carrier frequency. Besides, ζ denotes small-scale fading which experiences a mixed Gaussian distribution, which is written as

$$\zeta\left[\mathrm{dB}\right]\sim p_{Los}\mathcal{N}\left(-\mu_{Los},\delta_{Los}^2\right)+p_{NLos}\mathcal{N}\left(-\mu_{NLos},\delta_{NLos}^2\right), \quad (3)$$

where p_{Los} and p_{NLos} are the LoS and non-LoS probabilities respectively, and $\mathcal{N}\left(-\mu_{Los},\delta_{Los}^2\right)$ and $\mathcal{N}\left(-\mu_{NLos},\delta_{NLos}^2\right)$ are normal distributions with mean μ_{Los}, μ_{NLos} and variance δ_{Los}^2, δ_{NLos}^2, respectively. Particularly, $p_{Los}+p_{NLos}=1$ and the probability of the LoS in (3) can be calculated as

$$p_{Los}=\exp\left(-\ell\cot\phi\right)=\exp\left(-\frac{\ell\sin\theta}{\cos\theta-\theta'}\right), \quad (4)$$

where ℓ denotes the propagation environment parameter and ϕ is the elevation angle between satellite and user.

We focus primarily on the secure transmission from IoT nodes to the UAV relay in the uplink. Additionally, we assume that the security of the link between the UAV relay and the satellite, which is responsible for forwarding secure information, can be guaranteed. Particularly, the channel from IoT user m (IU$_m$) to the UAV can be modeled as [44]

$$\mathbf{g}_m=\frac{\sqrt{g_0}}{D_{m\to u}}\left(\sqrt{\frac{K}{K+1}}\mathbf{g}_{\mathrm{LoS}}+\sqrt{\frac{1}{K+1}}\mathbf{g}_{\mathrm{Ray}}\right), \quad (5)$$

where g_0 represents the channel power gain from the ground source to the aerial destination at a reference distance of 1 meter, and $D_{m\to u}$ denotes the distance between IU$_m$ and UAV, defining as

$$D_{m\to u}=\sqrt{\left(x_u-x_m\right)^2+\left(y_u-y_m\right)^2+h_u^2}, \quad (6)$$

where (x_u,y_u,h_u) is the 3D coordinates of UAV and (x_m,y_m) is the 2D horizontal coordinates of IoT user. Whereas, the small-scale fading adopts Rician channel model, where K is the Rician factor ($K_B=10log_{10}(K)$ in dB), $\mathbf{g}_{\mathrm{LoS}}\in\mathbb{C}^{N\times1}$ denotes LoS component, and $\mathbf{g}_{\mathrm{Ray}}\in\mathbb{C}^{N\times1}$ represents the NLoS Rayleigh fading component.

Besides, the channel between IoT users and ground Eve is modeled as a Nakagami-m fading channel. This channel model characterizes the signal propagation through various fading environments and captures the fluctuations in signal strength due to multipath propagation, shadowing, and other factors [45]. The Nakagami-m fading channel model is versatile, as it can represent different fading conditions by adjusting the m parameter. A higher value of m indicates less severe fading, whereas a lower value represents a more severe fading environment.

B. Signal Models

In the uplink, we consider IoT nodes operating in the same frequency band, and the signal received by the UAV from IoT users can be represented as

$$y_u=\sum_{\mathcal{M}}\mathbf{g}_{m,u}^{\dagger}\mathbf{w}_m\sqrt{p_m}s_m+n_m, \quad (7)$$

where p_m denotes the uplink transmission power of IU$_m$, $\mathbf{g}_{m,u}^{\dagger}\in\mathbb{C}^{1\times N}$ denotes the channel sate information (CSI) from IU$_m$ to UAV, $\mathbf{w}_m\in\mathbb{C}^{N\times1}$ is the beamforming vector at UAV for shaping the signal from IU$_m$, s_m contains the confident information expected to be delivered to the satellite backhaul network, n_m is the noise received by UAV.

Based on our considered eavesdropping model, due to the openness of wireless channel and the ground Eve operating in the same frequency band as the IoT nodes, the received signal by the Eve can be represented as

$$y_e=\sum_{\mathcal{M}}\mathbf{g}_{m,e}^{\dagger}\mathbf{w'}_m\sqrt{p_m}s_m+n_e, \quad (8)$$

where $\mathbf{g}_{m,e}^{\dagger}\in\mathbb{C}^{1\times N}$ denotes the wiretap channel from IU$_m$ to Eve, $\mathbf{w}'\in\mathbb{C}^{N\times1}$ is the beamforming vector at Eve, and n_e denotes the noise received by UAV and Eve, respectively.

From (7–8), it can be seen that the uplink signal of the IoT user has co-channel interference, and the signal received by the Eve also experiences co-channel interference among users. Based on this, we calculate the uplink SINRs of IU$_m$ at UAV and Eve, respectively, which are obtained as

$$\gamma_{m,u}=\frac{p_m\left\|\mathbf{g}_{m,u}^{\dagger}\mathbf{w}_m\right\|^2}{\sum\limits_{i\neq m,i\in\mathcal{M}}p_i\left\|\mathbf{g}_{i,u}^{\dagger}\mathbf{w}_i\right\|^2+\delta_m^2}, \quad (9)$$

$$\gamma_{e,m}=\frac{p_m\left\|\mathbf{G}_{m,e}^{\dagger}\mathbf{w'}_m\right\|^2}{\sum\limits_{i\neq m,i\in\mathcal{M}}p_i\left\|\mathbf{g}_{i,e}^{\dagger}\mathbf{w'}_i\right\|^2+\delta_e^2}, \quad (10)$$

where the δ_m^2 and δ_e^2 denote the noise power received by IU$_m$ and Eve.

C. Problem Formulation

Using (9) and (10), the secrecy rate of transmission from IU$_m$ to UAV is obtained as

$$R_m=\left[\log_2\left(1+\gamma_{m,u}\right)-\log_2\left(1+\gamma_{e,m}\right)\right]^+. \quad (11)$$

To enhance the uplink secrecy rate from IoT users to UAV and guarantee the secrecy fairness, we devise a problem formulation aimed at maximizing the minimum secrecy rate across uplink transmissions, which can be mathematically expressed as

$$\mathcal{P}1:\quad \underset{\{x_u,y_u,p_m,\mathbf{w}_m\}}{\mathrm{MaxMin}}\ \{R_m\} \quad (12)$$

$$\text{s.t.:}\quad \sum_{m\in\mathcal{M}}p_m\leq\mathcal{Q}, \quad (12a)$$

$$0\leq p_m\leq P_{\max}, \quad (12b)$$

$$\|\mathbf{w}_m\|=1, \quad (12c)$$

where (12a) constrains the sum power of IoT users with a predefined $\mathcal{Q}$, (12b) represents the constrained-power of IU_m, and (12c) constrains the beamforming at UAV. The formulated problem $\mathcal{P}1$ aims at uplink secure fairness by jointly optimizing the uplink power allocation, the UAV's position and the beamforming at the UAV's receiving end.

In addition, the formulated problem $\mathcal{P}1$ exhibits non-convexity due to three key factors: (i) The secrecy rate (11), calculating the difference between two logarithmic functions, inherently creates non-convexity; (ii) The Max-Min objective, targeting to maximize the minimum secrecy rate across uplink transmissions, adds complexity to the problem due to the need for multi-objective optimization; (iii) Power constraints (12a and 12b) and the unit-norm beamforming constraint (12c) further enhance non-convexity. Due to the problem's non-convexity, conventional convex optimization falls short. Thus, advanced mathematical simplifications and optimization techniques are imperative, warranting meticulous scrutiny of potential local optima.

IV. Joint Optimization of UAV Placement, UAV beamforming, and Uplink Power Allocation

In this section, we propose an approach that jointly optimize the UAV placement and the power allocation of IoT users to improve the secrecy rate performance of IoT users for the uplink transmissions. Since the formulated problem in (12) is non-convex and entails situations where multiple optimization variables are multiplied, in addition to the presence of numerous quadratic optimization variables, we initially undertake a transformation and simplification of the original problem. Specifically, we recast the original problem as a two-stage solution problem. In the first stage, we jointly optimize the uplink power allocation for IoT nodes and UAV beamforming. Subsequently, in the second stage, the placement of UAV is also optimized. Finally, the optimization of these two stages is iteratively alternated until performance converges.

For facilitating the derivation of formulas, the secrecy rate in (11) is further represented as shown in (13), where the following replacements are adopted ,

$$\mathbf{G}_{m,u} = D^2_{m\to u}\mathbf{g}_{m,u}\mathbf{g}^{\dagger}_{m,u}, \tag{14}$$

$$\mathbf{G}_{m,e} = D^2_{m\to u}\mathbf{G}_{m,e}\mathbf{G}^{\dagger}_{m,e}. \tag{15}$$

$$\mathbf{W}_m = \mathbf{w}^{\dagger}_m\mathbf{w}_m. \tag{16}$$

Based on (13), the inter-user interference can have a significant impact on the achievable secrecy rate for each user in a multi-user network with an eavesdropper. This is because the interference power increases as the transmission power of each IoT user increases, and also as the number of users in the network increases. In addition, changes in the position of the UAV can also have an impact on the security rate performance.

A. Uplink Power Allocation and UAV Beamforming

We assume that the UAV updates its beamforming once after its position changes, and the uplink power allocation of the IoT users is optimized at the same time. Therefore, in order to solve the original problem, in the first stage, we assume that when the UAV placement is fixed at a certain position, the original problem is simplified into a joint power allocation and beamforming optimization problem. Particularly, we first define an arbitrary variable φ with $\varphi \leq R_m, m \in \mathcal{M}$ to reformulate $\mathcal{P}1$ as

$$\begin{aligned} \mathcal{P}2: \quad & \underset{\{p_m,\mathbf{W}_m\}}{\mathrm{Max}} \; \varphi && (17)\\ \text{s.t.:} \quad & (12a), (12b), && (17a)\\ & \varphi \leq R_m, m \in \mathcal{M}, && (17b)\\ & \mathrm{Tr}\left(\mathbf{W}_m\right) = 1, && (17c)\\ & \mathbf{W}_m \succ \mathbf{0}. && (17d) \end{aligned}$$

In $\mathcal{P}2$, constraints (12a) and (12b) are retained from the original problem. The constraint condition (17b) is satisfied to simplify the max-min problem present in the single-objective function. Moreover, combining constraints (17c) and (17d) together is equivalent to constraint (12c). Based on (16), $rank\left(\mathbf{W}_m\right) = 1$ is held. To address non-convexity, $\mathcal{P}2$ applies Semi-Definite Relaxation (SDR) to handle the rank-1 constraint of UAV beamforming matrix [46], easing problem-solving.

Particularly, based on $\mathcal{P}2$, we can draw some interesting findings as follows.

Theorem 1. *Considering spectrum sharing among IoT nodes, when the maximum transmission power for the uplink is specified, given a specific receiver position and receiver beam direction, the uplink secrecy rate of IoT user monotonously increases as its power allocation.*

Proof. we take derivative of the secrecy rate in (13) is calculated as

$$\frac{\partial R_m}{\partial p_m} = \log_2 e\left(\frac{\alpha A_m}{p_m A_m + \alpha} - \frac{\beta B_m}{p_m B_m + \beta}\right), \tag{18}$$

$$\begin{aligned} R_m &= \log_2\left(1 + \frac{p_m\left\|\mathbf{g}^{\dagger}_{m,u}\mathbf{w}_m\right\|^2}{\sum\limits_{i\neq m, i\in M} p_i\left\|\mathbf{g}^{\dagger}_{i,u}\mathbf{w}_i\right\|^2 + \delta^2_m}\right) - \log_2\left(1 + \frac{p_m\left\|\mathbf{G}^{\dagger}_{m,e}\mathbf{w}'_m\right\|^2}{\sum\limits_{i\neq m, i\in M} p_i\left\|\mathbf{g}^{\dagger}_{e,i}\mathbf{w}'_i\right\|^2 + \delta^2_e}\right)\\ &= \log_2\left(1 + \frac{p_m\mathrm{Tr}\left(\mathbf{G}_{m,u}\mathbf{W}_m\right)}{\sum\limits_{i\neq m, i\in M} p_i\mathrm{Tr}\left(\mathbf{G}_{i,u}\mathbf{W}_i\right) + D^2_{m\to u}}\right) - \log_2\left(1 + \frac{p_m\mathrm{Tr}\left(\mathbf{G}_{m,e}\mathbf{W}'_m\right)}{\sum\limits_{i\neq m, i\in M} p_i\mathrm{Tr}\left(\mathbf{G}_{e,i}\mathbf{W}'_i\right) + D^2_{m\to u}}\right). \end{aligned} \tag{13}$$

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2023.3313197

where A_m, B_m, α, and β are defined as follows

$$A_m = \mathrm{Tr}\left(\mathbf{G}_{m,u}\mathbf{W}_m\right), \tag{19}$$

$$B_m = \mathrm{Tr}\left(\mathbf{G}_{m,e}\mathbf{W'}_m\right), \tag{20}$$

$$\alpha = \sum_{i \neq m, i \in M} p_i \mathrm{Tr}\left(\mathbf{G}_{i,u}\mathbf{W}\right) + D_{m \to u}^2, \tag{21}$$

$$\beta = \sum_{i \neq m, i \in M} p_i \mathrm{Tr}\left(\mathbf{G}_{e,i}\mathbf{W'}_i\right) + D_{m \to u}^2. \tag{22}$$

We note that $A_m \geq B_m$ and $\alpha \geq \beta$ due to the fact that only positive secrecy rates are feasible in our formulated problem. Therefore, we have

$$\alpha p_m A_m B_m + \alpha\beta A_m \geq \beta p_m A_m B_m + \alpha\beta B_m, \tag{23}$$

which implies that $\frac{\partial R_m}{\partial p_m} \geq 0$. This indicates the secrecy rate of IU_m monotonically increases as its power allocation.

This concludes the proof of the theorem. ■

With the constraint in (12a), the power allocation of IoT user restricts that of other users. Thus we have the following Theorem to analyze the secrecy fairness among the IoT users for secure uplink transmissions.

Theorem 2. *Secrecy fairness: For feasible power allocations of IoT users, the secrecy rates of IoT users achieve the same values, $R_m = R_i \, (m \neq i, m \in \mathcal{M}, i \in \mathcal{M})$.*

Proof. Consider the optimization problem in $\mathcal{P}2$, where the secrecy goal is reformulated to maximize φ subject to constraints (14a) through (14d).

Observe that constraint (14b) requires $\varphi \leq R_m, \forall m \in \mathcal{M}$. In the optimal solution, the goal is to maximize φ, which entails enlarging φ to the greatest possible extent while adhering to this constraint. Consequently, in the optimal solution, at least one user $m \in \mathcal{M}$ must satisfy $\varphi = R_m$.

Assume there exists at least one user $i \in \mathcal{M}$ such that $R_m < R_i$. Under this condition, φ can be augmented by reallocating power from user i to user m. This reallocation can be executed without infringing constraint (14a) and will result in a larger φ, as R_m increases and R_i decreases. This procedure can be iterated until $R_m = R_i \; \forall m \neq i, m \in \mathcal{M}, i \in \mathcal{M}$.

Thus, the secrecy rates of IoT users achieve the same values, $R_m = R_i \, (m \neq i, m \in \mathcal{M}, i \in \mathcal{M})$, for feasible power allocations of IoT users.

This concludes the proof of the theorem. ■

Based on the aforementioned theorem, an iterative binary search method can be employed to determine the final power allocation. However, the objective is to jointly optimize the uplink power allocation of IoT users and UAV beamforming. Therefore, we further simplify problem $\mathcal{P}2$ and utilize a convex approximation algorithm for its resolution. To elaborate, the original problem $\mathcal{P}2$ aims to maximize the worst-case secrecy rate φ among IoT uplink transmissions while optimizing both the uplink power allocation of IoT users and the UAV beamforming. By employing the proof in the theorem, we have established that in the optimal solution, the secrecy rates of all IoT users achieve the same values, i.e., $R_m = R_i$ for all $m \neq i, m \in \mathcal{M}, i \in \mathcal{M}$, given feasible power allocations. Specifically, with loss of generality, we fist assume a group of initialized power allocations, $\left\{p_m^0, m \in \mathcal{M}\right\}$. Then, we simplify problem $\mathcal{P}2$ by reformulating it into a more tractable problem, which focuses on the joint optimization of uplink power allocation of IoT users and UAV beamforming. The constraint (17b) can be reformulated as

$$\varphi \leq \log_2 e\left(u - mu - t + mt\right), \tag{24}$$

where the new introduced variables u, mu, t, and mt satisfy the following definitions

$$e^u = \sum_{i \in M} p_i \mathrm{Tr}\left(\mathbf{G}_{i,u}\mathbf{W}_m\right) + D_{m \to u}^2, \tag{25}$$

$$e^t = \sum_{i \in M} p_i \mathrm{Tr}\left(\mathbf{G}_{e,i}\mathbf{W'}_i\right) + D_{m \to e}^2, \tag{26}$$

$$e^{mu} = \sum_{i \neq m, i \in M} p_i \mathrm{Tr}\left(\mathbf{G}_{i,u}\mathbf{W}_m\right) + D_{m \to u}^2, \tag{27}$$

$$e^{mt} = \sum_{i \neq m, i \in M} p_i \mathrm{Tr}\left(\mathbf{G}_{e,i}\mathbf{W'}_i\right) + D_{m \to e}^2. \tag{28}$$

Besides, by defining $\boldsymbol{\omega}_m = p_m \mathbf{W}_m$, the joint uplink power allocation and UAV beamforming problem is reformulated as

$$\mathcal{P}3 : \underset{\boldsymbol{\omega}_m}{\mathrm{Max}}\, \varphi \tag{29}$$

$$\text{s.t.:} \quad \sum_{m \in \mathcal{M}} \mathrm{Tr}\left(\boldsymbol{\omega}_m\right) \leq \mathcal{Q}, \tag{29a}$$

$$\varphi \leq \log_2 e\left(u - mu - t + mt\right), m \in \mathcal{M}, \tag{29b}$$

$$e^u \leq \sum_{i \in M} p_i \mathrm{Tr}\left(\mathbf{G}_{i,u}\mathbf{W}_i\right) + D_{m \to u}^2, \tag{29c}$$

$$e^{\tilde{t}}\left(\tilde{t} - t + 1\right) \geq \sum_{i \in M} p_i \mathrm{Tr}\left(\mathbf{G}_{e,i}\mathbf{W'}_i\right) + D_{m \to e}^2, \tag{29d}$$

$$e^{\tilde{m}u}\left(\tilde{m}u - mu + 1\right) \geq \sum_{i \neq m, i \in M} p_i \mathrm{Tr}\left(\mathbf{G}_{i,u}\mathbf{W}_i\right) + D_{m \to u}^2, \tag{29e}$$

$$e^{mt} \leq \sum_{i \neq m, i \in M} p_i \mathrm{Tr}\left(\mathbf{G}_{e,i}\mathbf{W'}_i\right) + D_{m \to e}^2, \tag{29f}$$

$$\boldsymbol{\omega}_m \succ \mathbf{0}. \tag{29g}$$

To address $\mathcal{P}3$, we propose a successive convex approximation (SCA) based joint optimization algorithm for uplink power allocation and UAV beamforming, as illustrated in Algorithm 1.

Complexity analysis: The complexity of the algorithm mainly comes from two aspects: the semi-definite programming (SDP) problem solved using the CVX tool and the convergence criterion.

SDP: The SDP problem in Step 2 of the algorithm is solved using the CVX tool. SDP problems have a complexity that is polynomial in the number of variables and constraints. Let n denote the number of variables and m denote the number of constraints in the SDP problem. The complexity of solving an SDP problem is generally in the order of $O(n^2 m + n^3)$. In this specific problem, the number of variables and constraints will depend on the dimensions of the matrices involved and the size of the optimization problem.

Algorithm 1: SCA-based Joint Optimization Algorithm for the Uplink Power Allocation of IoT users and the UAV Beamforming

```
Require: Initial values: $\tilde{t}$ and $\tilde{mu}$. Input channel state
    information (CSI) of uplink channels, estimated CSI of
    Eve, and location information of the UAV.
Ensure: Optimized uplink power allocation $p_m$ and UAV
    beamforming matrix $\mathbf{W}_m$.
Initialize $\tilde{t}$ and $\tilde{mu}$;
repeat
    Execute semi-definite programming (SDP) using the
    CVX tool.
    Update $\tilde{t}$ and $\tilde{mu}$;
    Compute the objective function $\varphi$ using (29);
until convergence criterion is met
Compute $p_m = |\omega_m|^2$, $\mathbf{W}_m = \omega_m / p_m$
return $p_m$ and $\mathbf{W}_m$;
```

Convergence criterion: The algorithm iterates until a convergence criterion is met. Let N_{iter} denote the maximum number of iterations required for the algorithm to converge. The complexity of this part depends on how quickly the algorithm converges to the optimal solution, which can be influenced by factors such as the initial values of $\tilde{t}$ and $\tilde{mu}$, the channel state information (CSI), and the location of the UAV.

Considering both aspects, the overall complexity of the alternating optimization algorithm is $O(N_{iter}(n^2m + n^3))$. Since the algorithm employs the CVX tool to solve the SDP problem.

B. Optimization of UAV Placement

Based on the uplink power allocation parameters and UAV beamforming vectors obtained from Algorithm 1 in the first-stage, the UAV placement optimization problem inherited from the original max-min problem can be reformulated as:

$$\mathcal{P}4: \quad \underset{\{x_u, y_u\}}{\text{Max}} \ \varphi \tag{30}$$

$$\text{s.t.:} \quad \varphi \leq R_m, \tag{30a}$$

where the constraint in (30a) can be reformulated as

$$\log_2\left(\frac{\alpha' + A_m + D_{m\to u}^2}{\alpha' + D_{m\to u}^2}\right) - \log_2\left(\frac{\beta' + B_m + D_{m\to u}^2}{\beta' + D_{m\to u}^2}\right) \geq \varphi, \tag{31}$$

with

$$\begin{aligned} \alpha' &= \sum_{i\neq m, i\in M} p_i \mathrm{Tr}\left(\mathbf{G}_{i,u}\mathbf{W}_i\right), \\ \beta' &= \sum_{i\neq m, i\in M} p_i \mathrm{Tr}\left(\mathbf{G}_{e,i}\mathbf{W}_i\right). \end{aligned} \tag{32}$$

After simplification and analysis, (31) is further reformulated as shown in (33), at the bottom of this page.

We take a replacement of $L_{m,u} = D_{m\to u}^2$ and and reformulate $\mathcal{P}3$ as

$$\mathcal{P}5: \quad \underset{\{L_{m,u}\}}{\text{Max}} \ \varphi \tag{34}$$

$$\text{s.t.:} \quad aL_{m,u}^2 + bL_{m,u} + c \leq 0, \tag{34a}$$

$$L_{m,u} \geq 0, \tag{34b}$$

$$b^2 - 4ac > 0, \tag{34c}$$

where a, b, and c are constants. Based on (33), since $2^\varphi - 1 \geq 0$, the parabola with variable $L_{m,u}$ should be at least two points of intersection with the horizontal axis of $L_{m,u}$ and thus (34b) should be satisfied.

Remark 1. *By carefully analyzing the simplifed Problem $\mathcal{P}5$, we can draw an interesting finding, which are discussed as follows. Based on (34a), we have*

$$L_{m,u} \leq \frac{-b + \sqrt{b^2 - ac}}{2a}. \tag{35}$$

Particularly, by taking the derivation of $L_{m,u}$, we have

$$\begin{aligned} \frac{\partial R_m}{\partial L_{m,u}} =& \log_2 e \left\{ \frac{B_m}{\left(\beta' + B_m + L_{m,u}\right)\left(\beta' + L_{m,u}\right)} \right. \\ & \left. - \frac{A_m}{\left(\alpha' + A_m + L_{m,u}\right)\left(\alpha' + L_{m,u}\right)} \right\} \\ \leq& \ 0, \end{aligned} \tag{36}$$

which indicates that the secrecy rate of IU_m decreases monotonously as the distance between the UAV and IU_m.

To address problem $\mathcal{P}5$ in the second stage, we introduce an iterative optimization strategy that synergizes the bisection and coordinate descent methods for optimizing the UAV's positioning, as outlined in Algorithm 1.

Algorithm 1 commences with defining the search parameters for φ with a lower (φ_{min}) and upper (φ_{max}) boundary. The algorithm repeats until it converges, assessed via a pre-established tolerance ϵ.

Each iteration incorporates two crucial steps:

Step 1: The bisection approach is utilized to revise φ. At each iteration, the current search range's midpoint is calculated as:

$$\varphi = \frac{\varphi_{min} + \varphi_{max}}{2}. \tag{37}$$

Subsequently, coefficients a, b, and c are updated based on the new φ value. The problem's feasibility is then validated through the discriminant condition:

$$\Delta = b^2 - 4ac. \tag{38}$$

$$\begin{aligned} & \left(2^\varphi - 1\right) D_{m\to u}^4 + D_{m\to u}^2 \left[2^\varphi\left(\alpha' + \beta' + B_m\right) - \alpha' - \beta' - A_m\right] + 2^\varphi\left(\alpha'\beta' + \alpha' B_m\right) \leq \alpha'\beta' + A_m\beta' \\ & \Leftrightarrow aL_{m,u}^2 + bL_{m,u} + c \leq 0; a \triangleq 2^\varphi - 1, b \triangleq 2^\varphi\left(\alpha' + \beta' + B_m\right) - \alpha' - \beta' - A_m, c \triangleq 2^\varphi\left(\alpha'\beta' + \alpha' B_m\right) - \alpha'\beta' + A_m\beta'. \end{aligned} \tag{33}$$

Algorithm 2: Synergized Bisection and Coordinate Descent algorithm

```
Initialization: $\varphi_{min} = 0$, $\varphi_{max}$ represents the upper limit, and $\epsilon > 0$ is the tolerance;
while non-convergence do
    Step 1: $\varphi$ is updated via the bisection method:
    $\varphi \leftarrow \frac{\varphi_{min}+\varphi_{max}}{2}$; $a$, $b$, and $c$ coefficients are revised based on the new $\varphi$;
    if $b^2 - 4ac > 0$ then
        Feasible problem: Adjust $\varphi_{min}$ or $\varphi_{max}$;
    else
        Infeasible problem: Modify $\varphi_{min}$ or $\varphi_{max}$;
    Step 2: Establish the optimal $L_{m,u}$ by minimizing constraint (25a) through coordinate descent;
    Refresh $L_{m,u}$ and evaluate convergence based on the tolerance $\epsilon$;
Output: Optimal values of $\varphi$ and $L_{m,u}$ with $(x_u, y_u)$.
```

If $\Delta > 0$, the problem is deemed feasible; otherwise, it's considered infeasible. Dependent on the feasibility, the search range for φ is updated accordingly.

Step 2: With the revised φ, the optimal $L_{m,u}$ is ascertained by minimizing the constraint in (25a) via coordinate descent. The update rule for $L_{m,u}$ is enforced, and the algorithm's convergence is evaluated based on the tolerance ϵ.

Finally, the convergence can be attained by alternating iterations between these two stages optimizations in Algorithm 1 and Algorithm 2.

Complexity analysis: The proposed algorithm provides an efficient and effective way to find the optimal values for φ and $L_{m,u}$, which can be utilized in the optimization of UAV placement in the given communication system. The complexity of our proposed algorithm mainly includes two aspects: the bisection method used for updating φ and the optimization technique employed for finding the optimal value of $L_{m,u}$.

Bisection method: The bisection method is known for its logarithmic convergence rate. At each iteration, the search interval is reduced by half. Let N_φ denote the maximum iteration number for the bisection method to converge. Given a predefined tolerance ϵ, the complexity of the bisection method is $O(\log_2(\frac{\varphi_{max}-\varphi_{min}}{\epsilon}))$.

Optimize $L_{m,u}$: The complexity of this step depends on the optimization technique used for minimizing the constraint in (25a). Coordinate descent is one possible method for solving this problem. Let $N_{L_{m,u}}$ denote the maximum number of iterations for the optimization of $L_{m,u}$ to converge. The complexity of this step is $O(N_{L_{m,u}})$, where the actual value of $N_{L_{m,u}}$ depends on the specific convergence rate of the chosen optimization technique.

Considering both aspects, the overall complexity of the proposed algorithm is $O(N_\varphi N_{L_{m,u}})$.

Based on the above subsection A and B, the two-stage optimization approach is completed. In the first stage, we solve optimization problem $\mathcal{P}3$ using Algorithm 1, obtaining the uplink power allocation and the UAV's beamforming vector. Based on these results, in the second stage, we solve optimization problem $\mathcal{P}5$ using Algorithm 2 to determine the position of the UAV.

The problem defined in this paper is non-convex and multi-variable, thus obtaining a global optimum solution is challenging. The problem is simplified to a bi-convex form and solved using a two-tier approach. Utilizing an alternating iterative framework, fast convergence is achieved. Although each tier achieves optimal solutions, the overall outcome is considered near-optimal.

V. Performance Evaluations

In this section, various simulations are conducted to assess the secrecy performance of uplink transmissions for IoT users. The simulation parameters are configured as follows: IoT users are distributed according to a 2D PPP within an area with a radius of 100 meters. The initial position of the UAV is set in 3D coordinates as (0m, 0m, 100m). The imperfect channel state information (CSI) has an estimation error of $\|\upsilon\| = 0.2$, such that $\hat{\mathbf{g}}_{m,e}^\dagger = \mathbf{g}_{m,e}^\dagger + \upsilon$. The channel power gains from IoT users to the UAV in the uplink and to Eve at a reference distance of 1m are -40dB and -38.6dB, respectively. The Ricean factor for the channel from IoT users to the UAV is set at 10dB. The Nakagami-*m* parameters for the wiretap channel from IoT users to the ground-based Eve are set to (*m*=2, Ω =1). Additionally, specific parameters are introduced for each individual simulation, e.g., the maximum transmission power P_S, the number of UAV receive antennas *N*, the number of IoT users within coverage of UAV is set to *M*, the height of UAV h_u. The number of receive antennas of Eve is same as *N*. For the benchmarks, we adopt two variants of the proposed, which are respectively labeled as "Fixed PA and ZF-BF & placement opt.", representing the approach that optimizes only the UAV's position with a fixed power allocation using equal division and the UAV beamforming using Zero-Forcing beamforming associated to the eavesdropping channel, and "Fixed location & joint PA and BF opt.", representing the approach that fixes the UAV's location while jointly optimizing the uplink power allocation and the UAV's beamforming. Besides, we draw from established optimization strategies in relevant research, formulating an "Alternating SDP and Dinkelbach Optimization". Semidefinite Programming (SDP) is frequently employed for power allocation and beamforming, whilst Dinkelbach's method is regularly utilized for planning drone trajectories [47], [48]. As a benchmark, we amalgamate these techniques to address the secure fairness problem.

Fig. 2 shows the influence of the maximum transmission power on the minimum secrecy rate. As observed, the secrecy rate performance increases with the maximum transmission power, which is consistent with Theorem 1. According to Theorem 1, allocating more power to IoT users as the maximum transmission power increases results in improved secrecy rate performance. Besides, the proposed joint optimization approach involving UAV placement, IoT user power allocation, and UAV beamforming demonstrates superior performance compared to the evaluated benchmarks. Comparing the curves in Fig. 2, the following observations can be made: (1) The presence of channel estimation error can degrade the max-min secrecy rate performance; (2) Optimizing only the UAV

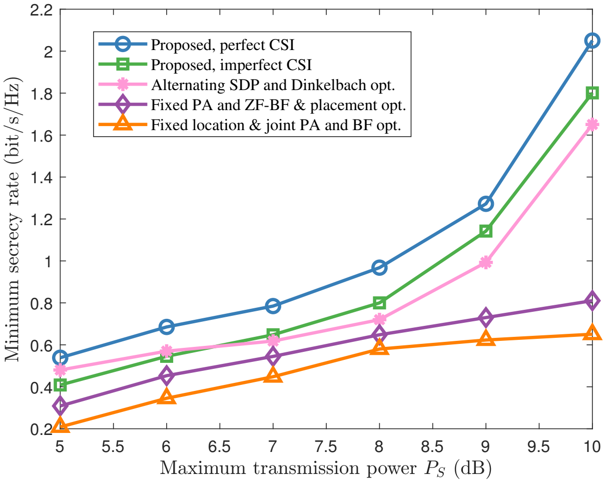


Fig. 2. Maximum transmission power P_s Vs. the minimum secrecy rate. ($N = 4, M = 4, h_u = 100$m)

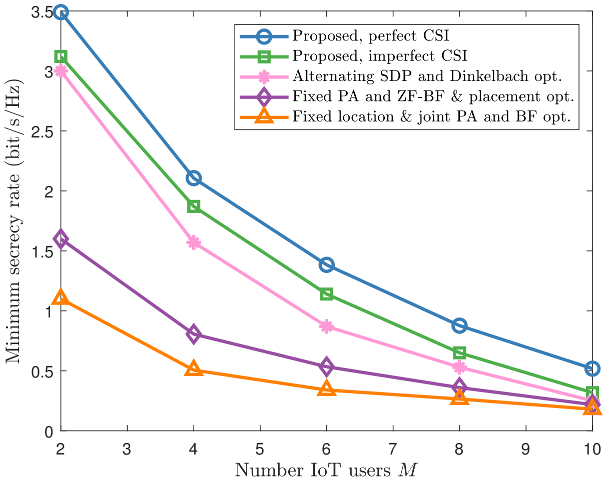


Fig. 4. Number IoT users M Vs. the minimum secrecy rate. ($N = 4, P_s =$ 10dB, $h_u = 100$m)

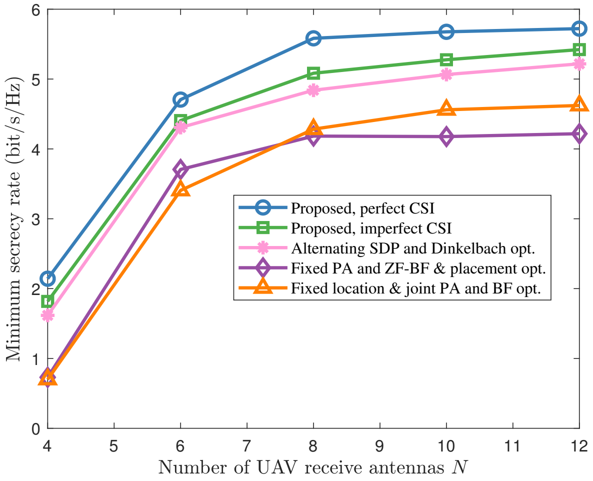


Fig. 3. Number of UAV receive antennas N Vs. the minimum secrecy rate. ($M = 4, P_s =$ 10dB, $h_u = 100$m)

placement, while using fixed power allocation and Zero-Forcing (ZF)-based UAV beamforming, could lead to leakage of legitimate signals due to ZF-based beamforming; (3) As the maximum transmission power increases, the optimal UAV placement contributes more significantly to security enhancement than the optimal power allocation and beamforming strategies.

Fig. 3 shows the effect of UAV receive antenna number on the minimum secrecy rate. As N increases, the secrecy rate performance exhibits an improvement. This enhancement can be attributed to the increased capacity of the UAV to effectively shape the uplink signal beams from IoT users with a higher number of antennas, enabling better discrimination between inter-user interference and minimizing energy leakage of valuable signals. The proposed approach presented in this paper demonstrates a notable superiority over the examined benchmarks. A detailed comparisons of the curves in Fig. 3 reveals that the presence of channel estimation error results in a decline in secrecy rate performance. Furthermore, when an adequate number of antennas are utilized, optimizing the uplink power allocation and UAV beamforming contributes more significantly to the improvement of the secrecy rate compared to the optimization of the UAV deployment location.

Fig. 4 shows the impact of the increasing number of uplink IoT users on the minimum secrecy rate performance, which demonstrates a decline as the user count grows. This outcome can be ascribed to the escalation of inter-user interference stemming from the expanding number of IoT users, leading to a consequent reduction in the SINR at the UAV receiver. Furthermore, the proposed approach consistently outperforms the other benchmark approaches, and channel errors contribute to a diminished secrecy rate performance. In large-scale IoT applications with a substantial user population, the joint optimization of UAV placement, uplink power allocation, and UAV beamforming can more proficiently safeguard the overall secrecy rate performance for IoT users.

Fig. 5 shows the impact of UAV deployment height on the minimum secrecy rate, highlighting a decrease in the secrecy rate performance as the UAV deployment height. This decline can be attributed to the exacerbation of air-to-ground channel fading due to the heightened UAV position, which undermines the quality of legitimate signal reception. Consequently, the main channel capacity of the uplink from IoT users is reduced while the eavesdropping channel remains unaltered, leading to diminished secrecy rate performance. Once again, Fig. 5 demonstrates that the proposed joint optimization of UAV placement, uplink power allocation, and UAV beamforming outperforms other benchmark approaches. Channel estimation errors can also contribute to the degradation of the max-min secrecy rate performance. Furthermore, the alteration in UAV height does not impact the significance of UAV deployment optimization over uplink power allocation and UAV beamforming optimization in terms of enhancing secrecy rate performance.

Fig. 6 shows the convergence performance of the joint

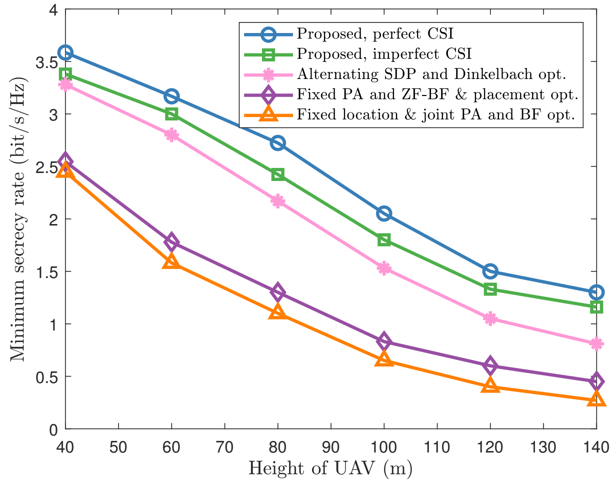


Fig. 5. UAV deployment height h_u Vs. the minimum secrecy rate. ($N = 4, M = 4, P_s = 10$dB)

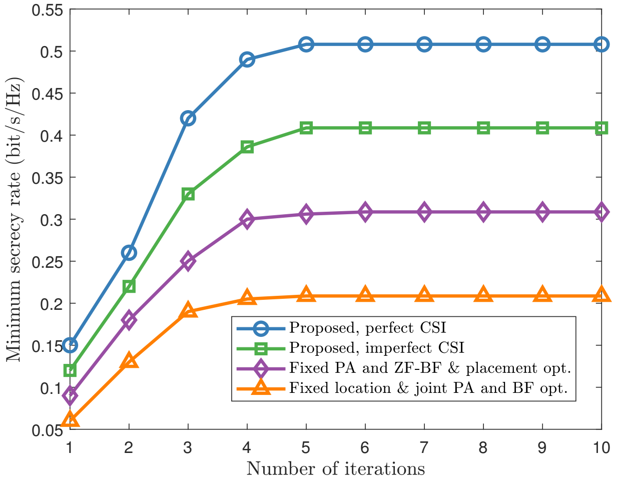


Fig. 6. Convergence analysis. ($N = 4, M = 4, P_S = 5$dB, $h_u = 100$m)

optimization algorithm for UAV placement, uplink power allocation, and UAV beamforming. The convergence performance of the algorithm is evaluated by simulating the number of iterations of the alternating optimization and the corresponding minimum secrecy rate performance. Comparing the curves in the figure, it can be seen that our proposed method, despite jointly optimizing multiple dimensions, does not significantly increase the number of iterations, and the alternating optimization using Algorithm 1 and Algorithm 2 can quickly converge.

VI. Conclusion

This paper has explored the use of UAV for enhancing the uplink secrecy rate performance in satellite-supported IoT, and the secrecy fairness among IoT users is realized. A framework is proposed that optimizes UAV placement, uplink power allocation, and UAV beamforming to ensure secure uplink transmissions while considering the energy constraints of IoT users. The non-convex max-min uplink secrecy rate problem is addressed using a two-stage optimization approach, which includes SCA-based algorithm for jointly optimizing uplink power allocation of IoT users and UAV beamforming, and synergized bisection and coordinate descent algorithm for optimizing UAV placement. In addition, numerical results verify the effectiveness of our proposed approach. Future research directions include investigating the impact of mobility on the proposed framework and optimizing the trade-off between security and energy efficiency.

References

[1] X. Shen and H. Stüttgen, "Growing our technical portfolio through cooperation with other ieee entities," *IEEE Commun. Mag.*, vol. 61, no. 3, pp. 4–6, 2023.

[2] T. Liu, J. Xia, Z. Ling, X. Fu, S. Yu, and M. Chen, "Efficient federated learning for aiot applications using knowledge distillation," *IEEE Internet Things J.*, vol. 10, no. 8, pp. 7229–7243, 2023.

[3] N. Cheng, J. He, Z. Yin, C. Zhou, H. Wu, F. Lyu, H. Zhou, and X. Shen, "6g service-oriented space-air-ground integrated network: A survey," *Chin. J. Aeronaut.*, vol. 35, no. 9, pp. 1–18, 2022.

[4] Z. Yin, N. Cheng, Y. Hui, W. Wang, L. Zhao, K. Aldubaikhy, and A. Alqasir, "Multi-domain resource multiplexing based secure transmission for satellite-assisted IoT: AO-SCA approach," *IEEE Trans. Wireless Commun.*, 2023, early access.

[5] T. K. Rodrigues and N. Kato, "Hybrid centralized and distributed learning for mec-equipped satellite 6g networks," *IEEE J. Sel. Areas Commun.*, 2023.

[6] D. Han, Q. Ye, H. Peng, W. Wu, H. Wu, W. Liao, and X. Shen, "Two-timescale learning-based task offloading for remote iot in integrated satellite-terrestrial networks," *IEEE Internet Things J.*, 2023, early access.

[7] B. Al Homssi, A. Al-Hourani, K. Wang, P. Conder, S. Kandeepan, J. Choi, B. Allen, and B. Moores, "Next generation mega satellite networks for access equality: Opportunities, challenges, and performance," *IEEE Commun. Mag.*, vol. 60, no. 4, pp. 18–24, 2022.

[8] F. Tang, X. Chen, M. Zhao, and N. Kato, "The roadmap of communication and networking in 6g for the metaverse," *IEEE Wireless Commun.*, pp. 1–15, 2022.

[9] M. López, S. B. Damsgaard, I. Rodríguez, and P. Mogensen, "An empirical analysis of multi-connectivity between 5g terrestrial and leo satellite networks," in *2022 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2022, pp. 1115–1120.

[10] I. Ashraf, Y. Park, S. Hur, S. W. Kim, R. Alroobaea, Y. B. Zikria, and S. Nosheen, "A survey on cyber security threats in iot-enabled maritime industry," *IEEE Trans. Intell. Transp. Syst.*, 2022.

[11] Y. Liu, L. Ni, and M. Peng, "A secure and efficient authentication protocol for satellite-terrestrial networks," *IEEE Internet Things J.*, vol. 10, no. 7, pp. 5810–5822, 2023.

[12] B. Wang, J. Jiao, S. Wu, R. Lu, and Q. Zhang, "Age-critical and secure blockchain sharding scheme for satellite-based internet of things," *IEEE Trans. Wireless Commun.*, vol. 21, no. 11, pp. 9432–9446, 2022.

[13] B. Kuang, A. Fu, W. Susilo, S. Yu, and Y. Gao, "A survey of remote attestation in internet of things: Attacks, countermeasures, and prospects," *Comput Secur*, vol. 112, p. 102498, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404821003229

[14] K. Yu, J. Yu, and C. Luo, "The impact of mobility on physical layer security of 5g iot networks," *IEEE/ACM Trans. Netw.*, pp. 1–14, 2022.

[15] D. Chen, H. Wang, N. Zhang, X. Nie, H.-N. Dai, K. Zhang, and K.-K. R. Choo, "Privacy-preserving encrypted traffic inspection with symmetric cryptographic techniques in iot," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17 265–17 279, 2022.

[16] M. Shen, K. Ye, X. Liu, L. Zhu, J. Kang, S. Yu, Q. Li, and K. Xu, "Machine learning-powered encrypted network traffic analysis: A comprehensive survey," *IEEE Communi. Surve. & Tutori.*, vol. 25, no. 1, pp. 791–824, 2023.

[17] Y. Liu, Z. Su, C. Zhang, and H.-H. Chen, "Minimization of secrecy outage probability in reconfigurable intelligent surface-assisted mimome system," *IEEE Trans. Wireless Commun.*, vol. 22, no. 2, pp. 1374–1387, 2023.

[18] Z. Yin, N. Cheng, T. H. Luan, and P. Wang, "Physical layer security in cybertwin-enabled integrated satellite-terrestrial vehicle networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 5, pp. 4561–4572, 2022.

[19] P. Angueira, I. Val, J. Montalban, Ó. Seijo, E. Iradier, P. S. Fontaneda, L. Fanari, and A. Arriola, "A survey of physical layer techniques for secure wireless communications in industry," *IEEE Communi. Surv. & Tutori.*, vol. 24, no. 2, pp. 810–838, 2022.

[20] S. Han, J. Li, W. Meng, M. Guizani, and S. Sun, "Challenges of physical layer security in a satellite-terrestrial network," *IEEE Netw.*, vol. 36, no. 3, pp. 98–104, 2022.

[21] K. Cao, B. Wang, H. Ding, L. Lv, R. Dong, T. Cheng, and F. Gong, "Improving physical layer security of uplink noma via energy harvesting jammers," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 786–799, 2021.

[22] V. Bankey, S. Sharma, S. R, and A. Madhukumar, "Physical layer security of haps-based space-air-ground integrated network with hybrid fso/rf communication," *IEEE Trans. Aerosp. Electron. Syst.*, pp. 1–8, 2022.

[23] S. Aggarwal, N. Kumar, and S. Tanwar, "Blockchain-envisioned uav communication using 6g networks: Open issues, use cases, and future directions," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5416–5441, 2021.

[24] W. U. Khan, E. Lagunas, Z. Ali, M. A. Javed, M. Ahmed, S. Chatzinotas, B. Ottersten, and P. Popovski, "Opportunities for physical layer security in uav communication enhanced with intelligent reflective surfaces," *IEEE Wireless Commun.*, vol. 29, no. 6, pp. 22–28, 2022.

[25] Z. Yin, M. Jia, N. Cheng, W. Wang, F. Lyu, Q. Guo, and X. Shen, "Uav-assisted physical layer security in multi-beam satellite-enabled vehicle communications," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 2739–2751, 2022.

[26] X. Wang, Z. Fei, J. A. Zhang, and J. Huang, "Sensing-assisted secure uplink communications with full-duplex base station," *IEEE Commun. Lett.*, vol. 26, no. 2, pp. 249–253, 2022.

[27] K. Cao, B. Wang, H. Ding, L. Lv, J. Tian, and F. Gong, "On the security enhancement of uplink noma systems with jammer selection," *IEEE Trans. Commun.*, vol. 68, no. 9, pp. 5747–5763, 2020.

[28] M. Centenaro, C. E. Costa, F. Granelli, C. Sacchi, and L. Vangelista, "A survey on technologies, standards and open challenges in satellite iot," *IEEE Communi. Surve. & Tutori.*, vol. 23, no. 3, pp. 1693–1720, 2021.

[29] X. Zhu and C. Jiang, "Integrated satellite-terrestrial networks toward 6g: Architectures, applications, and challenges," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 437–461, 2021.

[30] K.-Y. Lam, S. Mitra, F. Gondesen, and X. Yi, "Ant-centric iot security reference architecture—security-by-design for satellite-enabled smart cities," *IEEE Internet Things J.*, vol. 9, no. 8, pp. 5895–5908, 2021.

[31] H. Guo, J. Li, J. Liu, N. Tian, and N. Kato, "A survey on space-air-ground-sea integrated network security in 6g," *IEEE Communi. Surv. & Tutori.*, vol. 24, no. 1, pp. 53–87, 2022.

[32] Y. Tian, G. Pan, M. A. Kishk, and M.-S. Alouini, "Stochastic analysis of cooperative satellite-uav communications," *IEEE Trans. Wireless Commun.*, vol. 21, no. 6, pp. 3570–3586, 2022.

[33] C. Liao, K. Xu, H. Zhu, X. Xia, Q. Su, and N. Sha, "Secure transmission in satellite-uav integrated system against eavesdropping and jamming: A two-level stackelberg game model," *China Commun.*, vol. 19, no. 7, pp. 53–66, 2022.

[34] D. He, Z. Sha, H. Liu, T. Mao, and Z. Wang, "Uav-assisted satellite-terrestrial secure communication using large-scale antenna array with one-bit adcs/dacs," *IEEE Trans. Commun.*, vol. 71, no. 1, pp. 580–594, 2023.

[35] D. Wang, T. He, Y. Lou, L. Pang, Y. He, and H.-H. Chen, "Double-edge computation offloading for secure integrated space-air-aqua networks," *IEEE Internet Things J.*, pp. 1–1, 2023.

[36] R. Han, L. Bai, J. Liu, J. Choi, and Y.-C. Liang, "A secure structure for uav-aided iot networks: Space-time key," *IEEE Wireless Commun.*, vol. 28, no. 5, pp. 96–101, 2021.

[37] W. Wang, X. Li, R. Wang, K. Cumanan, W. Feng, Z. Ding, and O. A. Dobre, "Robust 3d-trajectory and time switching optimization for dual-uav-enabled secure communications," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 11, pp. 3334–3347, 2021.

[38] G. Zhang, Q. Wu, M. Cui, and R. Zhang, "Securing uav communications via joint trajectory and power control," *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 1376–1389, 2019.

[39] S. Li, B. Duo, M. D. Renzo, M. Tao, and X. Yuan, "Robust secure uav communications with the aid of reconfigurable intelligent surfaces," *IEEE Trans. Wireless Commun.*, vol. 20, no. 10, pp. 6402–6417, 2021.

[40] A. S. Abdalla and V. Marojevic, "Securing mobile multiuser transmissions with uavs in the presence of multiple eavesdroppers," *IEEE Trans. Veh. Technol.*, vol. 70, no. 10, pp. 11 011–11 016, 2021.

[41] T.-X. Zheng, X. Chen, C. Wang, K.-K. Wong, and J. Yuan, "Physical layer security in large-scale random multiple access wireless sensor networks: A stochastic geometry approach," *IEEE Trans. Commun.*, vol. 70, no. 6, pp. 4038–4051, 2022.

[42] B. A. Homssi and A. Al-Hourani, "Modeling uplink coverage performance in hybrid satellite-terrestrial networks," *IEEE Commun. Lett.*, vol. 25, no. 10, pp. 3239–3243, 2021.

[43] P.-. Series, "Propagation model for IF77," *ITU-R Report*, pp. 1–72, 2020. [Online]. Available: http://www.itu.int/publ/R-REP/en

[44] B. Hu, L. Wang, S. Chen, J. Cui, and L. Chen, "An uplink throughput optimization scheme for uav-enabled urban emergency communications," *IEEE Internet Things J.*, vol. 9, no. 6, pp. 4291–4302, 2022.

[45] T.-H. Vu, T.-V. Nguyen, T.-T. Nguyen, D. B. da Costa, and S. Kim, "Performance analysis of short-packet noma-based cdrt networks over nakagami-m fading channels," *IEEE Trans. Veh. Technol.*, vol. 71, no. 12, pp. 12 928–12 942, 2022.

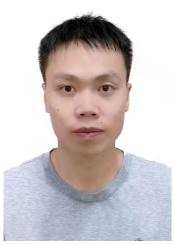
[46] S. Zargari, A. Khalili, Q. Wu, M. R. Mili, and D. W. K. Ng, "Max-min fair energy-efficient beamforming design for intelligent reflecting surface-aided swipt systems with non-linear energy harvesting model," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 5848–5864, 2021.

[47] J. Chu, R. Liu, M. Li, Y. Liu, and Q. Liu, "Joint secure transmit beamforming designs for integrated sensing and communication systems," *IEEE Trans. Veh. Technol.*, vol. 72, no. 4, pp. 4778–4791, 2023.

[48] X. Zhou, Q. Wu, S. Yan, F. Shu, and J. Li, "Uav-enabled secure communications: Joint trajectory and transmit power optimization," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 4069–4073, 2019.

Zhisheng Yin (Member, IEEE) received his Ph.D. degree from the School of Electronics and Information Engineering, Harbin Institute of Technology, Harbin, China, in 2020, and the B.E. degree from the Wuhan Institute of Technology, the B.B.A. degree from the Zhongnan University of Economics and Law, Wuhan, China, in 2012, and the M.Sc. degree from the Civil Aviation University of China, Tianjin, China, in 2016. From Sept. 2018 to Sept. 2019, Dr. Yin visited in BBCR Group, Department of Electrical and Computer Engineering, University of Waterloo, Canada. He is currently an Associate Professor in Xidian University, Xi'an, China. He is also an Associate Editor of IEEE Internet of Things Journal. His research interests include space-air-ground integrated networks, wireless communications, cybertwin, and physical layer security.

Nan Cheng (Senior Member, IEEE) received the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo in 2016, and B.E. degree and the M.S. degree from the Department of Electronics and Information Engineering, Tongji University, Shanghai, China, in 2009 and 2012, respectively. He worked as a Post-doctoral fellow with the Department of Electrical and Computer Engineering, University of Toronto, from 2017 to 2019. He is currently a professor with State Key Lab. of ISN and with School of Telecommunication Engineering, Xidian University, Shaanxi, China. His current research focuses on B5G/6G, space-air-ground integrated network, big data in vehicular networks, and self-driving system. His research interests also include performance analysis, MAC, opportunistic communication, and application of AI for vehicular networks.

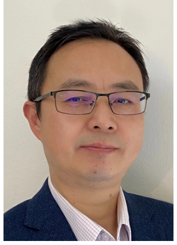


Yunchao Song (Member, IEEE) received the B.E. degree in electronic science and technology and the Ph.D. degree in circuits and systems from the Nanjing University of Posts and Telecommunications (NJUPT), Nanjing, China, in 2010 and 2016, respectively. He is currently an associate professor with the NJUPT. His research interests includes wireless communications, signal processing for communications and reinforcement learning.

Yilong Hui (Member, IEEE) received the Ph.D. degree in control theory and control engineering from Shanghai University, Shanghai, China, in 2018. He is currently an Associate Professor with the State Key Laboratory of Integrated Services Networks, and with the School of Telecommunications Engineering, Xidian University, China. He has published over 50 scientific articles in leading journals and international conferences. His research interests include wireless communication, mobile edge computing, vehicular networks, intelligent transportation systems and autonomous driving. He was the recipient of the Best Paper Award of International Conference WiCon2016 and IEEE Cyber-SciTech2017.

Yunhan Li received her B. Eng. degrees in Urban Planning from both Xi’an Jiaotong-liverpool University, P. R. China, and University of Liverpool, UK. in 2016, and M. Eng. Degree in Urbanism (Urban Design) from University of Sydney, Australia. Currently, she is a Highway Engineer, Operation Management Branch of Shaanxi Transportation Holding Group Co., Ltd., Xi’an, Shaanxi, China. Her research interests include smart transportation, vehicle information security and vehicle networking.

Tom H. Luan (Senior Member, IEEE) received the B.Eng. degree from Xi’an Jiaotong University, Xi’an, China, in 2004, the M.Phil. degree from The Hong Kong University of Science and Technology, Hong Kong, in 2007, and the Ph.D. degree from the University of Waterloo, Waterloo, ON, Canada, in 2012. He is currently a Professor with the School of Cyber Engineering, Xidian University, Xi’an. He has authored or coauthored more than 40 journal articles and 30 technical articles in conference proceedings. His research interests include content distribution and media streaming in vehicular ad hoc networks, peer-to-peer networking, and the protocol design and performance evaluation of wireless cloud computing and edge computing. Dr. Luan was the recipient of one U.S. patent. He was a TPC Member of the IEEE Global Communications Conference, the IEEE International Conference on Communications, and the IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, and the Technical Reviewer for multiple IEEE Transactions, including the IEEE Transactions on Mobile Computing, the IEEE Transactions on Parallel and Distributed Systems, the IEEE Transactions on Vehicular Technology, the IEEE Transactions on Wireless Communications, and the IEEE Transactions on Intelligent Transportation Systems.



Shui Yu (Fellow, IEEE) obtained his PhD from Deakin University, Australia, in 2004. He is a Professor of School of Computer Science, Deputy Chair of University Research Committee, University of Technology Sydney, Australia. His research interest includes Cybersecurity, Network Science, Big Data, and Mathematical Modelling. He has published five monographs and edited two books, more than 500 technical papers at different venues, such as IEEE TDSC, TPDS, TC, TIFS, TMC, TKDE, TETC, ToN, and INFOCOM. His current h-index is 72. Professor Yu promoted the research field of networking for big data since 2013, and his research outputs have been widely adopted by industrial systems, such as Amazon cloud security. He is currently serving the editorial boards of IEEE Communications Surveys and Tutorials (Area Editor) and IEEE Internet of Things Journal (Editor). He served as a Distinguished Lecturer of IEEE Communications Society (2018-2021). He is a Distinguished Visitor of IEEE Computer Society, and an elected member of Board of Governors of IEEE VTS and ComSoc, respectively. He is a member of ACM and AAAS, and a Fellow of IEEE.