frontiers in Physics

TYPE Original Research
PUBLISHED 08 October 2026
DOI 10.3389/fphy.2026.1964844

Check for updates

OPEN ACCESS

EDITED BY
Yuexia Zhang,
Beijing Information Science and Technology University, China

REVIEWED BY
Hongjiang Lei,
Chongqing University of Posts and Telecommunications, China
Xinyi Wang,
Beijing University of Posts and Telecommunications (BUPT), China

*CORRESPONDENCE
José Escorcia-Gutierrez,
j.escorci56@cuc.edu.co
Darius Andriukaitis,
darius.andrikaitis@ktu.lt

RECEIVED 11 August 2026
REVISED 01 September 2026
ACCEPTED 04 September 2026
PUBLISHED 08 October 2026

CITATION
Alalmaei S, Hinov N, Al-Turjman F, Salama R, González López HA, Aristizábal LF, Neira-Rodado D, Escorcia-Gutierrez J and Andriukaitis D (2026) Novel framework for physical-layer secrecy and network secrecy energy efficiency of UAV-assisted device-to-device communication.
Front. Phys. 14:1964844.
doi: 10.3389/fphy.2026.1964844

COPYRIGHT
© 2026 Alalmaei, Hinov, Al-Turjman, Salama, González López, Aristizábal, Neira-Rodado, Escorcia-Gutierrez and Andriukaitis. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

Novel framework for physical-layer secrecy and network secrecy energy efficiency of UAV-assisted device-to-device communication

Shiyam Alalmaei[1], Nikoly Hinov[2,3], Fadi Al-Turjman[4], Ramiz Salama[4], Hugo Alberto González López[5], Leandro Flórez Aristizábal[5], Dionicio Neira-Rodado[6], José Escorcia-Gutierrez[7]* and Darius Andriukaitis[8]*

[1]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia, [2]CoE "National Center of Mechatronics and Clean Technologies", Technical University of Sofia, Sofia, Bulgaria, [3]Faculty of Computer Systems and Technologies, Sofia, Bulgaria, [4]AI and Software Engineering Department, AI and IoT Research Center, AI and Informatics Faculty, Near East University, Mersin, Türkiye, [5]School of Engineering, Institución Universitaria Antonio José Camacho, Cali, Colombia, [6]Department of Productivity and Innovation, Universidad de la Costa, CUC, Barranquilla, Colombia, [7]Department of Computational Science and Electronics, Universidad de la Costa, CUC, Barranquilla, Colombia, [8]Department of Electronics Engineering, Kaunas University of Technology, Kaunas, Lithuania

Introduction: Wireless networks are anticipated to continue connecting billions of devices and producing enormous amounts of data with the next sixth-generation (6G) technologies, propelling the development of artificial intelligence applications in a variety of industries. Unmanned aerial vehicles have shown promise in this regard as a way to deal with the problems brought on by the expanding environment. UAVs are especially well-suited for delivering on-demand services to mobile devices because of their special qualities, which include their mobility, flexibility, and capacity to create line-of-sight communication links. This is especially true in areas with limited terrestrial infrastructure, such as hot areas and disaster communication. Therefore, by acting as relaying points, aerial base stations, and data collectors, UAVs may greatly increase the capacity and reach of networks.
Methods: To address the challenges of energy limitations, spectrum scarcity, and severe co-channel interference in device-to-device (D2D) communication networks supporting UAVs in passive eavesdropping environments, the concept of secrecy energy-efficiency was introduced by considering each user's privacy level and transmission power limitations. Based on physical layer secure transmission theory, the common problem of optimizing spectrum multiplexing and energy management strategies to maximize the energy efficiency of network secrecy was studied. A resource allocation algorithm combining the two algorithms was proposed to ensure the convergence of the original problem to a global optimal solution using the Dinkelbach algorithm and to transform the non-convex optimization problem into a geometric planning problem using the convex approximation algorithm. The problem was non-linear and non-convex.
Results and Discussion: Simulation results show that the recommended approach can effectively reduce co-channel interference, improve the energy

efficiency of network privacy, and achieve a balance between network energy consumption and secure communication performance.

KEYWORDS

co-channel interference, D2D communication, eavesdropping, physical layer secrecy, secrecy optimization, UAV communication

1 Introduction

In complex and harsh environments, communication is easily subject to problems such as electromagnetic interference, satellite signal denial and infrastructure destruction. Unmanned aerial vehicles (UAVs) have advantages such as strong concealment, flexibility and mobility, and can provide line-of-sight (LoS) links. They can perform diversified tasks such as auxiliary communication, intelligence gathering and electronic countermeasures. The role of UAV-assisted communication is particularly prominent [1]. Device-to-device (D2D) communication supports direct terminal connection and instant activation, which can improve the transmission rate and reduce transmission delay. Especially in edge areas or communication blind spots, the coverage of the network can be improved through multi-hop D2D communication technology [2]. By using UAVs as air base stations and combining them with D2D communication, a local high-speed private network with "wide coverage, high speed and strong compatibility" that does not rely on fixed infrastructure can be constructed. This can expand the capacity of the communication system and improve the information secrecy capability [3]. However, the characteristics of LoS transmission and wireless broadcasting of UAV communication networks make them susceptible to eavesdropping by malicious ground nodes [4]. In addition, UAV-assisted D2D communication networks also have problems such as limited spectrum resources and limited equipment energy. To ensure secure transmission in UAV-assisted D2D communication networks under passive eavesdropping, while mitigating co-channel interference and reducing network power consumption, it is necessary to study the network secrecy and communication resource allocation issues of UAV-assisted D2D communication networks under passive eavesdropping.

The existing information secrecy protection measures mainly adopt encryption technology, but it often has high requirements for the computing power and power consumption of the equipment. For UAVs that are deployed in the open, are easily captured, and have limited resources, it is difficult to achieve secure communication by using encryption technology. It is anticipated that physical layer secure transmission technology will balance network secrecy communication with UAV power consumption. The research on physical layer secure transmission originated from the eavesdropping channel model was proposed by [5]. Subsequent studies have demonstrated that there is always an encoding technique that enables the legitimate receiver to receive the confidential information with nearly no errors while the eavesdropper cannot obtain any confidential information when the legitimate channel's capacity exceeds that of the eavesdropping channel [6]. Physical layer secure transmission technology leverages the physical layer properties of the channel itself to accomplish secure transmission as a potent addition to the upper-layer encryption technique. It does not require complex encryption algorithms, has inherent secrecy attributes, low computational complexity and low power consumption, and is well adapted to large-scale, distributed network architectures [7]. A cellular user's spectrum resources can be shared with several D2D pairs in the "many-to-many" multiplexing mode, and a D2D pair can reuse the spectrum resources of several cellular users. While sharing spectrum resources among multiple users can lead to mutual interference, co-channel interference can be reduced and the distance between legitimate and eavesdropping channels can be increased by using appropriate spectrum reuse and power control techniques. This could lead to secure communication.

However, existing research on secure communication of UAV-assisted wireless networks under passive eavesdropping mainly focuses on optimizing the flight trajectory of UAVs [8, 9] or optimizing mode selection and cooperative interference strategies [10]. The secure transmission issue of UAV-assisted D2D communication networks from the standpoint of resource allocation based on physical layer secure transmission theory has not received much attention from researchers. In order to increase the energy efficiency of secure communication and simultaneously optimize user scheduling and UAV three-dimensional flight trajectory, the authors of [8] concentrated on UAV-assisted cellular network communication systems. The authors in [9] focused on scenarios in the Internet of Things (IoT) where there are active full-duplex eavesdroppers, and UAVs can track eavesdroppers and interfere with the eavesdropping channel, aiming to maximize the system's confidentiality capacity, and proposed a UAV trajectory optimization algorithm based on Q-learning. In order to improve the performance of covert communication, the authors in [10] suggested a joint mode selection and cooperative interference strategy. In this strategy, each user adaptively switched between half-duplex and full-duplex communication modes, and idle D2D users could work together to send interference signals to thwart eavesdroppers. Although the above references considered the secure communication of the network, they do not consider the total power consumption of UAVs and ground users.

The ratio of transmission rate to power consumption is known as energy efficiency, and it is now a crucial metric for gaging the effectiveness of UAV-assisted wireless communication networks. UAV-assisted communication networks' secrecy communication performance can be measured using secrecy efficiency, which is the ratio of secrecy rate to power consumption. Most existing works study the problem of maximizing energy efficiency, without considering the secure transmission of the network under passive eavesdropping [11–15]. The authors in [11] focused on UAV-assisted industrial Internet of Things (IIoT) based on simultaneous wireless information and power transfer (SWIPT) and jointly optimized the

UAV position and resource allocation technique to maximize the D2D communication energy efficiency. The authors in [12] focused on UAV-assisted mobile edge computing (MEC) systems based on D2D communication in order to optimize D2D communication energy efficiency. Together, they optimized the UAV trajectory, user scheduling strategy, and transmission power of D2D and UAV users. The authors in [13] focused on the scenario where several UAVs provided energy for D2D users and transferred data for cellular users in order to improve the energy efficiency of D2D communication. They jointly optimize beamwidth, power, and energy harvesting (EH) time ratio. The authors in [14] focused on the scenario where UAVs acted as communication relays and base stations, and maximized the network energy efficiency by optimizing the power and *band* width of D2D pairs, UAV trajectories and user associations. The authors in [15] focused on D2D-assisted UAV-MEC communication systems, and aimed to minimize the total power consumption during task offloading and local computing, and jointly optimized the trajectory, bit allocation and task allocation of UAVs.

Currently, only some studies focus on improving the secrecy efficiency of UAV-assisted communication networks [16–19]. The authors in [16] addressed the secrecy communication problem in the air-to-ground downlink passive eavesdropping scenario, considered the minimum legal channel data rate constraint and the maximum eavesdropping channel rate constraint under UAV jitter conditions, and jointly optimized the beamforming vector and artificial noise vector to minimize the UAV's transmission power. The authors in [17] utilized the interference generated by channel multiplexing in D2D communication, and ensured that the transmission rate and secrecy rate of all ground users satisfy the requirements while optimizing the D2D communication efficiency through power control and channel allocation. However, it studied the secrecy communication problem under the condition of eavesdroppers. The optimization goal of optimizing the ratio of D2D transmission rate to power consumption is not practically significant, even if the secrecy rate is utilized as a restriction. Orthogonal frequency division multiple access networks (OFDMA), which divided the user's signal into two segments for EH and information decoding, respectively, were the focus of the authors of [18]. With the goal of maximizing secrecy efficiency and minimizing energy consumption, a power allocation algorithm was proposed. The authors in [19] focused on UAV-MEC systems. Under the constraints of given task latency, UAV-CPU computing frequency and task offloading rate, it jointly optimized the legal UAV hovering position, CPU computing frequency allocation and computing task complexity differentiation strategy to maximize the SEE.

Table 1 compares the performance metrics of several algorithms with the proposed algorithm.

The aforementioned approaches either only consider the network transmission secrecy without regard to power consumption, or only focus on maximizing communication energy efficiency without considering the presence of eavesdroppers, or introduce technologies such as SWIPT and EH into the scenario. These approaches are unsuitable for the scenario of UAV base station-assisted ground D2D communication under passive eavesdropping, which is the focus of this paper, and cannot simultaneously meet the requirements of secure communication, mitigation of co-channel interference, and power saving. Therefore, this paper aims to maximize the total secrecy energy efficiency (TSEE), that is, to optimize the secrecy rate to power ratio for D2D pairings and cellular users. The following are this paper's primary contributions.

1. For UAV-assisted D2D communication networks under passive eavesdropping conditions, considering minimum secrecy rate and maximum transmit power constraints, the concept of network secrecy efficiency is introduced. Based on physical layer secure transmission theory, spectrum reuse and power control strategies are optimized to widen the difference between legitimate and eavesdropping channels and maximize network secrecy efficiency. Since this optimization issue is nonlinear and nonconvex, it is challenging to find a direct analytical solution.
2. The Dinkelbach algorithm and the convex approximation algorithm are integrated in a combined internal and external iterative optimization process. While the convex approximation procedure transforms the non-convex optimization problem into a geometric programming problem, the Dinkelbach approach ensures that the original problem converges to the optimal solution. The computational complexity analysis and steps of the proposed algorithm are also given.
3. The suggested algorithm's efficacy in enhancing secrecy energy efficiency, reducing co-channel interference, and optimizing spectrum reuse and power control strategies is confirmed by comparison with benchmark algorithms. Simulations evaluate the impact of UAV altitude on network secrecy efficiency.

2 System model and problem description

2.1 Scenario description

The UAV-assisted D2D communication network is illustrated Figure 1. The UAV base station is located in the center of the service area and hovers at a predetermined height. It deploys N number of D2D pairs and M number of cellular users which are distributed at random throughout the region. Cellular users employ frequency division multiple access (FDMA) to connect to the UAV base station in the cellular network uplink transmission scenario. Each of the M cellular clients receives one of the M sub-channels that make up the network's spectrum resources. Several D2D pairs in the network exchange data by multiplexing the sub-channels of numerous cellular subscribers. As a result, the D2D pair transmitters can interfere with the UAV base station's ability to receive signals from cellular users, while cellular users and other D2D pair transmitters that multiplex the same spectrum resources can interfere with the D2D pair receivers. A passive eavesdropper also exists in the network, simultaneously eavesdropping on the transmission data of both the cellular network and the D2D communication.

TABLE 1 Performance comparison of existing works with proposed scheme.

Refs.	Energy efficiency	Aerial eavesdroppers	Relay deployment	Ground eavesdroppers	Optimization goal
[26]	No	No	No	Multiple	Worst-case secrecy rate
[27]	No	No	Yes	Multiple	Sum secrecy rate
[28]	No	No	No	Multiple	Minimum average covert rate
[29]	No	No	No	Single	Average secrecy rate
[30]	Yes	No	No	Multiple	Fairness-aware SEE
[31]	Yes	No	No	No	Energy efficiency
[32]	No	Multiple	No	No	Long-term secrecy throughput
[33]	No	Single	No	No	Secrecy
[34]	Yes	Single	Yes	No	SEE
[35]	Yes	Single	No	No	SEE
Proposed	Yes	No	Yes	No	TSEE

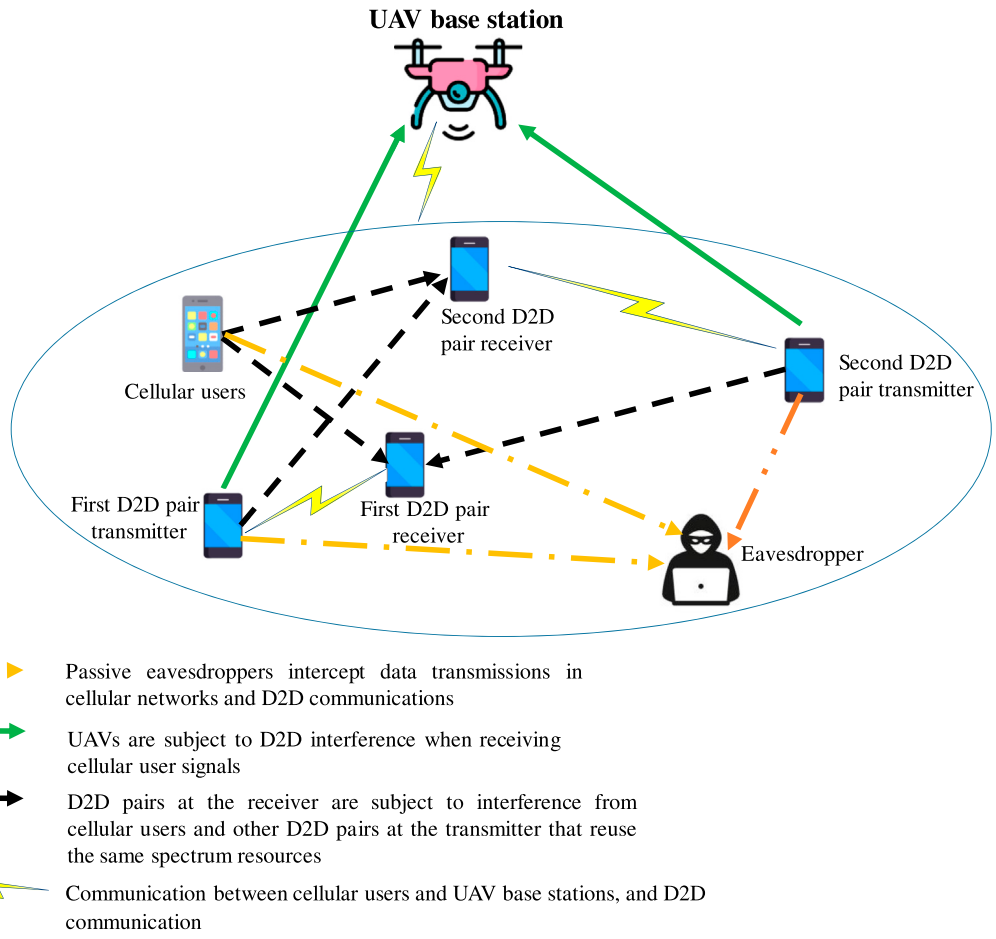


FIGURE 1
Proposed network model.

2.2 Channel model

The symbols $\{C_1, C_2, \ldots, C_M\}$ and $\{D_1, D_2, \ldots, D_N\}$ represent the sets of cellular users and D2D pairs, respectively. Let $D_{\mathrm{Tx},n}$ and $D_{\mathrm{Rx},n}$ represents the transmitter and receiver of the n th D2D pair.

Both the channels between D2D transmitters and UAVs and the channels between cellular users and UAVs are air-to-ground channels. This section uses the air-to-ground channel model created in [20] to represent the path loss as a probability-weighted sum of LoS and NLoS components for air-to-ground channels. The cellular user C_m and UAV's average path loss is defined by Equation 1:

$$\mathrm{PL}_{m,\mathrm{U}}^{\mathrm{dB}} = \mathrm{PL}_{m,\mathrm{U}}^{\mathrm{LoS}} P_{m,\mathrm{U}}^{\mathrm{LoS}} + \mathrm{PL}_{m,\mathrm{U}}^{\mathrm{NLoS}} P_{m,\mathrm{U}}^{\mathrm{NLoS}} = \frac{A}{1+\alpha e^{-\beta[\theta_{m,\mathrm{U}}-\alpha]}} + 20\log d_{m,\mathrm{U}} + B \tag{1}$$

where, the sub-parameters are defined by Equations 2–5 as follows:

$$A = \eta_{\mathrm{LoS}} - \eta_{\mathrm{NLoS}} \tag{2}$$

$$B = 20\log\left[\frac{4\pi f_c}{c}\right] + \eta_{\mathrm{NLoS}} \tag{3}$$

$$\theta_{m,\mathrm{U}} = \frac{180}{\pi}\tan^{-1}\left\{\frac{h}{r_{m,\mathrm{U}}}\right\} \tag{4}$$

$$d_{m,\mathrm{U}} = \sqrt{h^2 + r_{m,\mathrm{U}}^2} \tag{5}$$

where α is path loss factor, $\theta_{m,\mathrm{U}}$ is the pitch angle of the cellular user C_{m} and the UAV; $d_{m,\mathrm{U}}$ is the distance between the cellular user C_{m} and the UAV; η_{LoS} and η_{NLoS} are the average additional path loss under LoS and NLoS (related to the environment); f_c is the carrier frequency; c is the speed of light; h is the altitude of the UAV; and $r_{m,\mathrm{U}}$ is the horizontal Euclidean distance between the LoS and NLoS components.

The channel gain $\mathrm{g}_{m,\mathrm{U}}$ between UAV and the m-th cellular user C_{m} is represented by Equation 6:

$$\mathrm{g}_{m,\mathrm{U}} = 10^{\frac{-\mathrm{PL}_{m,\mathrm{U}}^{\mathrm{dB}}}{10}} \tag{6}$$

Similarly, the expression for the channel gain $\mathrm{g}_{n,\mathrm{U}}$ between the n th D2D pair's transmitter $\mathrm{D}_{\mathrm{T}_{x,n}}$ and UAV is expressed by Equation 7:

$$\mathrm{g}_{n,\mathrm{U}} = 10^{\frac{-\mathrm{PL}_{n,\mathrm{U}}^{\mathrm{dB}}}{10}} \tag{7}$$

For the channel between ground users, between $\mathrm{D}_{\mathrm{T}_{x,n}}$ and $\mathrm{D}_{\mathrm{R}_{x,n}}$, the channel gain $\mathrm{g}_{n,\mathrm{n}}$ is [21] defined by Equation 8:

$$\mathrm{g}_{n,\mathrm{n}} = G d_{n,n}^{-\xi}\xi_{n,n} \tag{8}$$

where G is the path loss constant between $\mathrm{D}_{\mathrm{T}_{x,n}}$ and $\mathrm{D}_{\mathrm{R}_{x,n}}$; $\mathrm{d}_{n,n}$ represents the distance between $\mathrm{D}_{\mathrm{T}_{x,n}}$ and $\mathrm{D}_{\mathrm{R}_{x,n}}$; ξ denotes the exponent of path loss; and $\xi_{n,n}$ represents the channel gain corresponding to the channel shadowing fading between $\mathrm{D}_{\mathrm{T}_{x,n}}$ and $\mathrm{D}_{\mathrm{R}_{x,n}}$, which follows a log-normal distribution.

Similarly, the following can be used to express the channel gains $\mathrm{g}_{m,n}$ between the transmitters $\mathrm{D}_{\mathrm{R}_{x,n}}$ of the m-th cellular user C_m and the n-th D2D pair; $\mathrm{g}_{n,n}$ between $\mathrm{D}_{\mathrm{T}_{x,n}}$ and $\mathrm{D}_{\mathrm{R}_{x,n}}$; $\mathrm{g}_{m,e}$ between cellular users C_m and Eve; and $\mathrm{g}_{n,\mathrm{e}}$ between $\mathrm{D}_{\mathrm{T}_{x,n}}$ and Eve are defined by Equations 9–12:

$$\mathrm{g}_{m,n} = G' d_{m,n}^{-\xi'}\xi_{m,n} \tag{9}$$

$$\mathrm{g}_{n',n} = G' d_{n',n}^{-\xi'}\xi_{n',n} \tag{10}$$

$$\mathrm{g}_{m,e} = G' d_{m,\mathrm{e}}^{-\xi'}\xi_{m,\mathrm{e}} \tag{11}$$

$$\mathrm{g}_{n,e} = G' d_{n,\mathrm{e}}^{-\xi'}\xi_{n,\mathrm{e}} \tag{12}$$

where G' represents the path loss constant between cellular users, D2D pairs, and Eve; ξ' represents the path loss exponent between cellular users, D2D pairs, and Eve; and $\xi_{m,n}, \xi_{n',n}, \xi_{m,\mathrm{e}}, \xi_{n,\mathrm{e}}$, which have a log-normal distribution, represent the channel gains corresponding to channel shadowing fading between cellular users, D2D pairs, and Eve.

2.3 Secrecy rate and power consumption calculation

The transmission rate of the m th cellular user C_m can be normalized as follows using the Shannon-Hartley theorem in Equation 13:

$$R_m^C = \log\left\{1 + \frac{p_m \mathrm{g}_{m,\mathrm{U}}}{\sum_{n=1}^{N} p_{n,m}\mathrm{g}_{n,\mathrm{U}} + \sigma^2}\right\} \tag{13}$$

where σ^2 is the additive white Gaussian noise (AWGN) power, p_m is the transmit power of cellular user C_m, and $p_{n,m}$ is the transmit power when the nth D2D pair reuses the spectrum resources of the m th cellular user C_m.

The following formula can be used to determine the m th cellular user C_m secrecy rate by Equation 14:

$$R_m^{\mathrm{OS}} = \left\{\log\left(1 + \frac{p_m \mathrm{g}_{m,\mathrm{U}}}{\sum_{n=1}^{N} p_{n,m}\mathrm{g}_{n,\mathrm{U}} + \sigma^2}\right) - \log\left(1 + \frac{p_m \mathrm{g}_{m,\mathrm{e}}}{\sum_{n=1}^{N} p_{n,m}\mathrm{g}_{n,\mathrm{e}} + \sigma^2}\right)\right\}^+ \tag{14}$$

where, $\{x\}^+ = \max[0, x]$.

The secrecy rate for the n-th D2D link, i.e., D_n, is expressed by Equation 15:

$$R_n^{\mathrm{DS}} = \left\{\sum_{m=1}^{M}\log\left(1 + \frac{p_{n,m}\mathrm{g}_{n,n}}{p_m \mathrm{g}_{m,n} + \sum_{n'=1}^{N} p_{n',m}\mathrm{g}_{n',n} + \sigma^2}\right)_{n' \neq n} - \sum_{m=1}^{M}\log\left(1 + \frac{p_{n,m}\mathrm{g}_{n,\mathrm{e}}}{p_m \mathrm{g}_{m,\mathrm{e}} + \sum_{n'=1}^{N} p_{n',m}\mathrm{g}_{n',\mathrm{e}} + \sigma^2}\right)_{n' \neq n}\right\}^+ \tag{15}$$

where the transmit power of the n'-th D2D pair transmitter $\mathrm{D}_{\mathrm{T}_{x,n'}}$ when it reuses the spectrum resources of the m-th cellular user C_m is represented by $p_{n',m}$.

Taking into account the influence of circuit power consumption, cellular user C_m power consumption is defined by Equation 16:

$$P_m = \frac{1}{\eta} p_m = P_{\text{cir}} \tag{16}$$

The n-th D2D pair D_n power consumption can be written as follows in Equation 17:

$$P_n = \frac{1}{\eta} \sum_{m=1}^{M} p_{n,m} + 2P_{\text{cir}} \tag{17}$$

where η represents the efficiency factor of the power amplifier, and P_{cir} represents a portion of the power consumed by each device itself (e.g., the power consumed by mixers, filters, analog-to-digital converters, and baseband processing units).

2.4 Problem description and modeling

To ensure secure communication in a UAV-assisted D2D communication network under passive eavesdropping conditions, while accounting for the minimum secrecy rate and maximum transmit power constraints for cellular users and D2D pairs, improving the spectrum reuse and power control procedures enhances the network's overall secrecy efficiency. Specifically, the resource allocation strategy should meet the following constraints:

1. C1:The secrecy rate R_m^{CS} for cellular users shall not be less than the minimum secrecy rate $R_{\min}^{\text{CS}}$. That is, $R_m^{\text{CS}} \geq R_{\min}^{\text{CS}}$
2. C2: The R_n^{DS} of the D2D pair is not less than the minimum secrecy rate $R_{\min}^{\text{DS}}$. That is, $R_n^{\text{DS}} \geq R_{\min}^{\text{DS}}$
3. C3: The cellular user's transmit power (p_m) cannot be greater than the maximum transmit power ($P_{\max}$). That is, $p_m \leq P_{\max}$
4. C4: The transmit power $p_{n,m}$ cannot be greater than the maximum transmit power $P_{\max}$ when D_n reuses cellular user C_m spectrum resources. That is, $p_{n,m} \leq P_{\max}$
5. C5: The total transmit power of the D2D transmitter shall not exceed the maximum transmit power $P_{\max}$. That is, $P_n \leq P_{\max}$

Based on the above requirements, assuming that the UAV base station can obtain the optimal channel state information (CSI), the problem is modeled as follows by Equation 18:

$$\begin{aligned} &\max_{\{p_m\},\{p_{n,m}\}} \frac{\sum_{m=1}^{M} R_m^{\text{CS}} + \sum_{n=1}^{N} R_n^{\text{DS}}}{\sum_{m=1}^{M} P_m + \sum_{n=1}^{N} P_n} \\ &\text{s.t. C1:} R_m^{\text{CS}} \geq R_{\min}^{\text{CS}} \\ &\text{C2:} R_n^{\text{DS}} \geq R_{\min}^{\text{DS}} \\ &\text{C3:} p_m \leq P_{\max} \\ &\text{C4:} p_{n,m} \leq P_{\max} \\ &\text{C5:} P_n \leq P_{\max} \end{aligned} \tag{18}$$

where $\{p_m\}$ and $\{p_{n,m}\}$ represent the transmit power for cellular users and D2D pairs, respectively. Constraints C1 and C2 guaranty the minimum secrecy rate for each cellular user and D2D pair; constraint C3 sets the maximum transmit power limit for each cellular user; constraint C4 demonstrates that the transmit power of the nth D2D pair reusing the spectrum resources of the mth cellular user does not exceed $P_{\max}$; and constraint C5 demonstrates that the total transmit power of the nth D2D pair reusing the spectrum resources of multiple cellular users does not exceed $P_{\max}$. It should be noted that the spectrum reuse strategy may be achieved by solving the optimization problem P1. If $p_{n,m} > 0$, D_n is allowed to utilize the spectrum resources of cellular user C_m; otherwise, it is not allowed.

Since constraints C1 and C2 ensure that R_m^{CS} and R_n^{DS} are non-negative, removing the $\{x\}^+$ from R_m^{CS} and R_n^{DS} will not have an impact on the original optimization problem's optimal solution. Removing the $\{x\}^+$ from R_m^{CS} and R_n^{DS} yields the optimization problem P1 by Equation 19:

$$\begin{aligned} \text{P1:} &\max_{\{p_m\},\{p_{n,m}\}} \frac{\sum_{m=1}^{M} \hat{R}_m^{\text{CS}} + \sum_{n=1}^{N} \hat{R}_n^{\text{DS}}}{\sum_{m=1}^{M} P_m + \sum_{n=1}^{N} P_n} \\ &\text{s.t. C1:} R_m^{\text{CS}} \geq R_{\min}^{\text{CS}} \\ &\text{C2:} R_n^{\text{DS}} \geq R_{\min}^{\text{DS}} \\ &\text{C3:} p_m \leq P_{\max} \\ &\text{C4:} p_{n,m} \leq P_{\max} \\ &\text{C5:} P_n \leq P_{\max} \end{aligned} \tag{19}$$

where, the sub-parameters are defined by Equations 20, 21:

$$\hat{R}_m^{\text{CS}} = \log\left[1 + \frac{p_m g_{m,\text{U}}}{\sum_{n=1}^{N} p_{n,m} g_{n,\text{U}} + \sigma^2}\right] - \log\left[1 + \frac{p_m g_{m,\text{e}}}{\sum_{n=1}^{N} p_{n,m} g_{n,\text{e}} + \sigma^2}\right] \tag{20}$$

$$\begin{aligned} \hat{R}_n^{\text{DS}} = &\sum_{m=1}^{M} \log\left[1 + \frac{p_{n,m} g_{n,n}}{p_m g_{m,n} + \sum_{\substack{n'=1 \\ n' \neq n}}^{N} p_{n',m} g_{n',n} + \sigma^2}\right] \\ &- \sum_{m=1}^{M} \log\left[1 + \frac{p_{n,m} g_{n,\text{e}}}{p_m g_{m,\text{e}} + \sum_{\substack{n'=1 \\ n' \neq n}}^{N} p_{n',m} g_{n',\text{e}} + \sigma^2}\right] \end{aligned} \tag{21}$$

It is challenging to immediately find the optimal solution for the nonlinear, nonconvex optimization problem P1. In order to solve the optimization problem, an internal and external iterative optimization technique that combines the Dinkelbach algorithm and the convex approximation algorithm is provided.

3 Algorithm description

3.1 Dinkelbach algorithm

The Dinkelbach approach has strong convergence and is frequently used to address the nonlinear fractional programming issues. Thus, the optimization problem P1 is processed in this study using the Dinkelbach method [22].

The optimal network secrecy efficiency is expressed by Equation 22:

$$q^* = \max_{\{p\}\in P} \frac{\sum_{m=1}^{M} \hat{R}_m^{\mathrm{CS}} + \sum_{n=1}^{N} \hat{R}_n^{\mathrm{DS}}}{\sum_{m=1}^{M} P_m + \sum_{n=1}^{N} P_n} \tag{22}$$

where p represents the optimization variables P_m and $P_{n,m}$, and P represents the feasible solution set that satisfies constraints C1 to C5.

As can be seen from Ref. [22], with the help of the auxiliary variable q, the optimization problems P1 and P2 may be interchangeable, which is expressed by Equations 23, 24:

$$\begin{aligned}
&\mathrm{P2}: \max_{\{p\}} f\{p,q\} \\
&\text{s.t. C1}: R_m^{\mathrm{CS}} \geq R_{\min}^{\mathrm{CS}} \\
&\mathrm{C2}: R_n^{\mathrm{DS}} \geq R_{\min}^{\mathrm{DS}} \\
&\mathrm{C3}: p_m \leq P_{\max} \\
&\mathrm{C4}: p_{n,m} \leq P_{\max} \\
&\mathrm{C5}: P_n \leq P_{\max}
\end{aligned} \tag{23}$$

where,

$$f(p,q) \triangleq \sum_{m=1}^{M} \hat{R}_m^{\mathrm{CS}} + \sum_{n=1}^{N} \hat{R}_m^{\mathrm{DS}} - q\left\{\sum_{m=1}^{M} P_m + \sum_{n=1}^{N} P_n\right\} \tag{24}$$

Clearly, $f(p,q)$ is a linear, monotonically decreasing function of the variable q.

The optimal network secrecy efficiency q^* is initially unknown but can be obtained using the Dinkelbach algorithm. Specifically, first, an initial strategy for spectrum reuse and power control that satisfies the constraints is chosen, and the initial secrecy efficiency $q^{(0)}$ is calculated, where the superscript $(\cdot)$ indicates an iteration of the algorithm. The related ideal resource allocation strategy and secrecy efficiency value are then obtained by solving the optimization problem P2 after setting $q = q^{(0)}$. Similarly, in each subsequent iteration, the secrecy efficiency value obtained from the previous iteration is used to update the q value, and the corresponding optimization problem is solved. After multiple iterations, the q value will converge to the optimal network secrecy efficiency q^* of optimization problem P1, and q^* satisfies $\max_{\{p\}\in P} f(p,q^*) = 0$. The iteration precision parameter is set to ε_1, and the total number of iterations is denoted by $T_1^{\max}$. The Dinkelbach algorithm is shown in Algorithm 1.

Initialize: $q^{(0)}$, $\{p_m\}^{(0)}$ and $\{p_{n,m}\}^{(0)}$
1: while $Z < T_1^{\max}$ || $\left|q^{(z)} - q^{(z-1)}\right| > \varepsilon_1$ do
2: Let $q = q^{(z)}$, solving optimization problem P2, we obtain $\{p_m\}^{(z+1)}$, $\{p_{n,m}\}^{(z+1)}$
3: $q^{(z+1)} = \frac{\sum_{m=1}^{M} \hat{R}_m^{\mathrm{CS}(z+1)} + \sum_{n=1}^{N} \hat{R}_n^{\mathrm{DS}(z+1)}}{\sum_{m=1}^{M} P_m^{(z+1)} + \sum_{n=1}^{N} P_n^{(z+1)}}$
4: end while
Output: optimal network secrecy efficiency $q^* = q^{(z)}$ and the spectrum reuse and power control strategies

Algorithm 1. Dinkelbach schem.

3.2 Convex approximation algorithm

The key to Algorithm 1 is solving the optimization problem P2. It is a non-convex optimization problem. It may be approximated as a geometric programming issue because of its comparable nature. To simplify writing Equation 25 is defined as follows:

$$C\left[\{p_{n,m}\}\right] = \sum_{n=1}^{N} p_{n,m} g_{n,\mathrm{U}} + \sigma^2 \tag{25}$$

Then the objective function of P2 can be written as Equation 26:

$$\begin{aligned}
\max_{\{p_m\},\{p_{n,m}\}} &\sum_{m=1}^{M} \log\left\{1 + \frac{p_m g_{m,\mathrm{U}}}{C\left[\{p_{n,m}\}\right]}\right\} - \sum_{m=1}^{M} \log\left\{1 + \frac{p_m g_{m,e}}{\tilde{C}\left[\{p_{n,m}\}\right]}\right\} + \sum_{n=1}^{N}\sum_{m=1}^{M} \log\left\{1 + \frac{p_{n,m} g_{n,n}}{D\left[\{p_m\},\{p_{n',m}\}\right]}\right\} \\
&- \sum_{n=1}^{N}\sum_{m=1}^{M} \log\left\{1 + \frac{p_{n,m} g_{n,e}}{\tilde{D}\left[\{p_m\},\{p_{n',m}\}\right]}\right\} - q\sum_{m=1}^{M}\left\{\frac{1}{\eta} p_m + P_{\mathrm{cir}}\right\} - q\sum_{n=1}^{N}\left\{\frac{1}{\eta}\sum_{m=1}^{M} p_{n,m} + 2P_{\mathrm{cir}}\right\}
\end{aligned} \tag{26}$$

Since both $q\sum_{m=1}^{M} P_{\mathrm{cir}}$ and $q\sum_{n=1}^{N} 2P_{\mathrm{cir}}$ are constants, they are eliminated from the objective function of optimization problem P2. Additionally, the objective function is further converted into a product form by using the characteristics of logarithmic functions. As a result, optimization problems P2 and P3 are interchangeable.

The objective function of optimization problem P2 is eliminated. Additionally, the objectrve function is further converted into a product form by using the characteristics of logarithmic functions. As a result, optimization problems P2 and P3 are interchangeable. It is expressed by Equation 27:

$$\begin{aligned}
&\mathrm{P3}: \min_{\{p_m\},\{P_{n,m}\}} \prod_{m=1}^{M}\left\{\frac{C\left[\{p_{n,m}\}\right]}{C\left[\{p_{n,m}\}\right] + p_m g_{m,\mathrm{u}}}\right\} \\
&\times \prod_{m=1}^{M}\left\{\frac{\hat{C}\left[\{p_{n,m}\}\right] + p_m g_{m,e}}{\hat{C}\left[\{p_{n,m}\}\right]}\right\} \\
&\text{s.t. C1}: R_m^{\mathrm{CS}} \geq R_{\min}^{\mathrm{CS}} \\
&\mathrm{C2}: R_n^{\mathrm{DS}} \geq R_{\min}^{\mathrm{DS}} \\
&\mathrm{C3}: p_m \leq P_{\max} \\
&\mathrm{C4}: p_{n,m} \leq P_{\max} \\
&\mathrm{C5}: P_n \leq P_{\max}
\end{aligned} \tag{27}$$

To further simplify writing, Equations 28, 29 are expressed as:

$$d_{\mathrm{c}}\left[\{p_m\},\{p_{n,m}\}\right] = C\left[\{p_{n,m}\}\right] + p_m g_{m,\mathrm{U}} \tag{28}$$

$$d_{\mathrm{D}}\left[\{p_m\},\{p_{n,m}\}\right] = D\left[\{p_m\},\{p_{n',m}\}\right] + p_{n,m} g_{n,n} \tag{29}$$

Furthermore, the function $u_i\left[\{p_m\},\{p_{n,m}\}\right]$ is defined as the i-th monomial of the positive term $d_{\mathrm{c}}\left[\{p_m\},\{p_{n,m}\}\right]$, the

function $v_j\left[\{p_m\},\{p_{n,m}\}\right]$ as the j-th monomial of the positive term $d_{\mathrm{D}}\left[\{p_m\},\{p_{n,m}\}\right]$, the function [23], $\hat{u}_i\left[\{p_{n,m}\}\right]$ as the i-th monomial of the positive term, $\hat{C}\left[\{p_{n,m}\}\right]$, and the function $\hat{v}_j\left[\{p_m\},\{p_{n',m}\}\right]$ as the j-th monomial of the positive term, $\hat{D}\left[\{p_m\},\{p_{n',m}\}\right]$. It is expressed by Equations 30–37:

$$d_{\mathrm{D}}\left[\{p_m\},\{p_{n,m}\}\right] \geq f\left[\{p_m\},\{p_{n,m}\}\right] \tag{30}$$

$$d_{\mathrm{D}}\left[\{p_m\},\{p_{n,m}\}\right] \geq \mathrm{g}\left[\{p_m\},\{p_{n,m}\}\right] \tag{31}$$

$$\hat{C}\left[\{p_{n,m}\}\right] \geq \hat{f}\left[\{p_{n,m}\}\right] \tag{32}$$

$$\hat{D}\left[\{p_m\},\{p_{n',m}\}\right] \geq \hat{\mathrm{g}}\left[\{p_{,m}\},\{p_{n',m}\}\right] \tag{33}$$

where,

$$f\left[\{p_m\},\{p_{n,m}\}\right] = \prod i\left\{\frac{u_i\left[\{p_m\},\{p_{n,m}\}\right]}{\alpha_i}\right\}^{\alpha_i} \tag{34}$$

$$\mathrm{g}\left[\{p_m\},\{p_{n,m}\}\right] = \prod j\left\{\frac{v_j\left[\{p_m\},\{p_{n,m}\}\right]}{\beta_j}\right\}^{\beta_j} \tag{35}$$

$$\hat{f}\left[\{p_{n,m}\}\right] = \prod i\left\{\frac{\hat{u}_i\left[\{p_{n,m}\}\right]}{\alpha_i}\right\}^{\hat{\alpha}_i} \tag{36}$$

$$\hat{\mathrm{g}}\left[\{p_m\},\{p_{n',m}\}\right] = \prod j\left\{\frac{\hat{v}_j\left[\{p_m\},\{p_{n',m}\}\right]}{\hat{\beta}_j}\right\}^{\hat{\beta}_j} \tag{37}$$

where α_i, β_j, $\hat{\alpha}_i$, and $\hat{\beta}_j$ are constants calculated from the optimal resource allocation result obtained in the previous iteration, and are expressed as follows by Equations 38–41:

$$\alpha_i^{(t)} = \frac{u_i\left[\{p_m\}^{(t-1)},\{p_{n',m}\}^{(t-1)}\right]}{d_{\mathrm{C}}\left[\{p_m\}^{(t-1)},\{p_{n',m}\}^{(t-1)}\right]} \tag{38}$$

$$\beta_j^{(t)} = \frac{v_j\left[\{p_m\}^{(t-1)},\{p_{n,m}\}^{(t-1)}\right]}{d_{\mathrm{C}}\left[\{p_m\}^{(t-1)},\{p_{n,m}\}^{(t-1)}\right]} \tag{39}$$

$$\hat{\alpha}_i^{(t)} = \frac{\hat{u}_i\left[\{p_{n,m}\}\right]^{(t-1)}}{\hat{C}\left[\{p_{n,m}\}\right]^{(t-1)}} \tag{40}$$

$$\hat{\beta}_j^{(t)} = \frac{\hat{v}_j\left[\{p_m\}^{(t-1)},\{p_{n',m}\}^{(t-1)}\right]}{\hat{D}\left[\{p_m\}^{(t-1)},\{p_{n',m}\}^{(t-1)}\right]} \tag{41}$$

Clearly, $f\left[\{p_m\},\{p_{n,m}\}\right], \mathrm{g}\left[\{p_m\},\{p_{n,m}\}\right], \hat{f}\left[\{p_{n,m}\}\right]$ and $\hat{\mathrm{g}}\left[\{p_m\},\{p_{n',m}\}\right]$ are all products of monomials, and are therefore monomials.

For the exponential term of the objective function P3, a first-order Taylor approximation near 0 is used, which is defined by Equations 42, 43:

$$\prod_{m=1}^{M} 2^{\frac{q}{\eta}p_m} \approx \prod_{m=1}^{M}\left\{1+\left(\frac{q}{\eta}\ln 2\right)p_m\right\} \tag{42}$$

$$\prod_{n=1}^{N}\prod_{m=1}^{M} 2^{\frac{q}{\eta}p_{n,m}} \approx \prod_{n=1}^{N}\prod_{m=1}^{M}\left\{1+\left(\frac{q}{\eta}\ln 2\right)p_{n,m}\right\} \tag{43}$$

In conclusion, it is possible to approximate the optimization problem P3 as the optimization problem P4. It is expressed by Equation 44:

$$\begin{aligned}
\text{P4:}\ \min_{\{p_m\},\{p_{n,m}\}} & \prod_{m=1}^{M}\left\{\frac{C\left[\{p_{n,m}\}\right]}{f\left[\{p_m\},\{p_{n,m}\}\right]}\right\} \\
& \times\prod_{m=1}^{M}\frac{\hat{C}\left[\{p_{n,m}\}\right]+p_m g_{m,\mathrm{e}}}{\hat{f}\left[\{p_{n,m}\}\right]} \\
& \times\prod_{n=1}^{N}\prod_{m=1}^{M}\left\{\frac{D\left[\{p_m\},\{p_{n',m}\}\right]}{\mathrm{g}\left[\{p_m\},\{p_{n,m}\}\right]}\right\} \\
& \times\prod_{n=1}^{N}\prod_{m=1}^{M}\left\{\frac{\hat{D}\left[\{p_m\},\{p_{n',m}\}\right]+p_{n,m}g_{n,\mathrm{e}}}{\hat{\mathrm{g}}\left[\{p_m\},\{p_{n',m}\}\right]}\right\} \\
& \times\prod_{m=1}^{M}\left\{1+\left(\frac{q}{\eta}\ln 2\right)p_m\right\} \\
& \times\prod_{n=1}^{N}\prod_{m=1}^{M}\left\{1+\left(\frac{q}{\eta}\ln 2\right)p_{n,m}\right\} \\
\text{s.t. C1:}\ & R_m^{\mathrm{CS}} \geq R_{\min}^{\mathrm{CS}} \\
\text{C2:}\ & R_n^{\mathrm{DS}} \geq R_{\min}^{\mathrm{DS}} \\
\text{C3:}\ & p_m \leq P_{\max} \\
\text{C4:}\ & p_{n,m} \leq P_{\max} \\
\text{C5:}\ & P_n \leq P_{\max}
\end{aligned} \tag{44}$$

In optimization problem P4, the objective function is a product of positive terms, which is still a positive term. The functions in the inequality constraints are all positive terms. Therefore, optimization problem P4 is a geometric programming problem. Although geometric programming issues are not convex optimization problems, they may be transformed into convex geometric programming problems by substituting variables and transforming the objective and constraint functions in an identical way [24]. The CVX toolbox in MATLAB can directly convert geometric programming problems into convex geometric programming problems and solve them. The iteration accuracy parameter is set to ε_2, the maximum number of iterations is set to $T_2^{\max}$, and the convex approximation scheme is discussed in Algorithm 2.

Initialize: $q^{(0)}, \{p_m\}^{(0)}$ and $\{p_{n,m}\}^{(0)}$

1: while $t < T_2^{\max}$ or $\left|q^{(t)} - q^{(t-1)}\right| > \varepsilon_2$ do

2: Given $\alpha_i^{(t)}$, $\beta_j^{(t)}$, $\hat{\alpha}_i^{(t)}$, $\hat{\beta}_j^{(t)}$, solve P4, we get $\{p_m\}^{(t)}$, $\{p_{n,m}\}^{(t)}$ and $q^{(t)}$

3: Calculate $\alpha_i^{(t+1)}$, $\beta_j^{(t+1)}$, $\hat{\alpha}_i^{(t+1)}$, $\hat{\beta}_j^{(t+1)}$ based on Equations 41-44

4: end while

Output: optimal network secrecy efficiency $q^* = q^{(t)}$ at this time, as well as the spectrum reuse and power control strategies

Algorithm 2. Convex approximation schem.

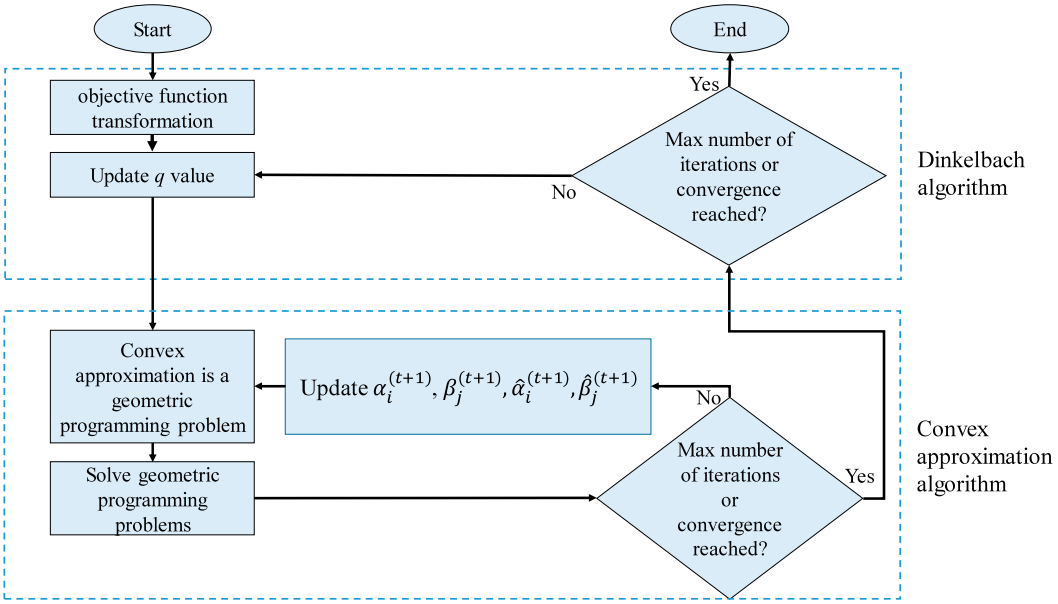


FIGURE 2
Resource allocation algorithm flowchart.

3.3 Resource allocation algorithm design

Figure 2 depicts the flow of the resource allocation method. In particular, the original nonlinear fractional programming problem P1 is converted into an equivalent subtraction form using the Dinkelbach technique. Ultimately, internal and external iterative optimization is used to determine the best resource allocation plan.

The final resource allocation algorithm with internal and external iterative optimization is shown in Algorithm 3.

4 Computational complexity analysis

The proposed algorithm mainly comprised of two parts: the Dinkelbach scheme and the convex approximation algorithm. The computational complexity of the Dinkelbach scheme is related to the iteration accuracy and the number of users [22], i.e., $O\{1/\varepsilon_1^2 \log[M+N]\}$, where M is the number of cellular users and N is the number of D2D users. The CVX toolbox solves the convex optimization problems based on the original dual interior point method [24]. Let the accuracy of CVX processing data be ε, and its complexity be $O\{\{MN\}^3 \log[1/\varepsilon]\}$. Therefore, the total computational complexity is the product of Dinkelbach algorithm complexity and the CVX optimization algorithm, i.e., $O\{1/\varepsilon_1^2 T_2^{\max}(MN)^3 \log(1/\varepsilon)\log[M+N]\}$. It should be noted that the parameter $T_2^{\max}$ is included in this complexity which represent the total number of iterations for convex approximation scheme.

Initialize: CSI, number of users, ε_1, ε_2, $T_1^{\max}$, $T_2^{\max}$, $R_{\min}^{CS}$, $R_{\min}^{DS}$, $P_{\max}$, σ^2, P_{cir}, η, $q^{(0)}$, $\{p_m\}^{(0)}$, $\{p_{n,m}\}^{(0)}$

1: while $Z < T_1^{\max}$ || $\left|q^{(z)} - q^{(z-1)}\right| > \varepsilon_1$ do
2: Let $q = q^{(z)}$
3: while $t < T_2^{\max}$ or $\left|q^{(t)} - q^{(t-1)}\right| > \varepsilon_2$ do
4: Calculate $\alpha_i^{(t+1)}$, $\beta_j^{(t+1)}$, $\hat{\alpha}_i^{(t+1)}$, $\hat{\beta}_j^{(t+1)}$ based on $\{p_m\}^{(t)}$ and $\{p_{n,m}\}^{(t)}$
5: The optimization problem P2 is approximated as P4
6: Solve for P4 to obtain $\{p_m\}^{(t+1)}$ and $\{p_{n,m}\}^{(t+1)}$
7: $q^{(t+1)} = \left\{\sum_{m=1}^{M} \hat{R}_m^{CS(t+1)} + \sum_{n=1}^{N} \hat{R}_n^{DS(t+1)}\right\} / \left\{\sum_{m=1}^{M} P_m^{(t+1)} + \sum_{n=1}^{N} P_n^{DS(t+1)}\right\}$
8: $\{p_m\}^* \leftarrow \{p_m\}^{(t+1)}$, $\{p_{n,m}\}^* \leftarrow \{p_{n,m}\}^{(t+1)}$
9: end while
10: Calculate $q^{(l+1)}$ based on $\{p_m\}^*$ and $\{p_{n,m}\}^*$
11: end while

Output: optimal network secrecy efficiency $q^* = q^{(l)}$ along with the spectrum reuse and power control strategies

Algorithm 3. Resource allocation scheme with internal and external iterative optimizatio.

5 Simulation results

5.1 Configuration

The coverage radius of the cell is set to 500 m. Eve, D2D pairs, and cellular users are distributed at random across the cell, with the

TABLE 2 Simulation parameters.

Parameter	Value
Number of cellular users and D2D pairs MN	1~8, 1~8
UAV altitude h	100~1,000 m
Max transmission distance of D2D users $d_{n,n}$	25 m
Path loss between ground users and UAVs	[12.08, 0.11, 1.6, 23]
Carrier frequency f_c of $\{\alpha,\beta,\eta_{\mathrm{LoS}},\eta_{\mathrm{NLoS}}\}$	2.4 GHz
Path loss parameters (G',ξ') between D2D pairs	$\{1.58\times10^{-15},4\}$
Path loss between cellular users, eve, and D2D pairs at the receiver (G,ξ)	$\{1.55\times10^{-15},3.76\}$
Channel gains corresponding to shadow fading: $\xi_{m,n}$, $\xi_{n',n}$, $\xi_{m,e}$, $\xi_{n,e}\xi_{n,n}$	$N\sim(0,5)$
Cellular user min secrecy rate R_m^{CS}	1 bps/Hz
D2D pair min secrecy rate R_m^{DS}	1 bps/Hz
Max power for cellular users and D2D pairs $P_{\max}$	1 W
Gaussian white noise σ^2	−121.45 dBm
Power amplifier efficiency factor η	0.35
The device's circuit power consumption P_{cir}	0.1 W
Convergence thresholds $\varepsilon_1\varepsilon_2$	0.1
Dinkelbach algorithm iterations $T_1^{\max}$	30
The number of iterations $T_2^{\max}$ in the convex approximation algorithm	15

UAV base station situated in its center. The path loss parameters (G,ξ) between the D2D pairs in a densely populated area are set to $\{1.58\times10^{-15},4\}$, whereas the path loss parameters (G',ξ') between the cellular users, Eve, and the D2D pair receivers are set to $\{1.55\times10^{-15},3.76\}$. According to [20], the path loss parameters $\{\alpha,\beta,\eta_{\mathrm{LoS}},\eta_{\mathrm{NLoS}}\}$ between the ground users and UAVs can be set to $\{12.08,0.11,1.6,23\}$. Table 2 displays the particular simulation parameter settings.

5.2 Algorithm performance evaluation

5.2.1 Iterative convergence

When the number of cellular users M rises from 1 to 8 and the number of D2D pairings N is fixed at 4, Figure 3a illustrates the convergence of the suggested method. When the number of cellular users $M=4$ and the number of D2D pairs N rises from 1 to 8. Figure 3b illustrates the convergence of the suggested method where the number of cellular users M is fixed at 4 and the number of D2D pairs N rises from 1 to 8. Figures 3c,d illustrate how the number of iterations needed for convergence varies with changes in the number of cellular users M and D2D pairs N, respectively. Out of 20 simulations, the number of iterations needed for convergence has the highest frequency. In every simulation, the locations of Eve, D2D pairs, and cellular users are created at random. It is important to note that the simulation results in Figures 3a,b are from one of the 20 simulations, and the number of iterations needed for convergence in this simulation is the same as the number shown in Figures 3c,d.

The convergence and TSEE vary based on the quantity and distribution of cellular users M and D2D pairings N, as seen in Figures 3a,b. The number of iterations needed for convergence rises with the number of users, regardless of whether the number of cellular users M is fixed and the number of D2D pairings N fluctuates or *vice versa*, as Figures 3c,d demonstrate. This suggests that the number of users and the complexity of the algorithm are correlated, although the growth rate of the algorithm is comparatively sluggish.

5.2.2 Performance comparison of different algorithms

The performance of the proposed method is verified by comparing it to the following algorithms.

1. Particle swarm optimization (PSO) algorithm [25]. Each search particle's location, which corresponds to a fitness value established by the network secrecy energy efficiency, provides a workable solution to the issue (i.e., power control and spectrum reuse approach). By consulting the location of the particle with the highest fitness value, the search particle modifies its own position and velocity. It then iteratively determines the best option.
2. Random Spectrum and Power Allocation (RSPA) Algorithm. This algorithm randomly allocates resources while meeting certain constraints.
3. The algorithm found in [17]. Strategies for power regulation and spectrum reuse are optimized. The optimization

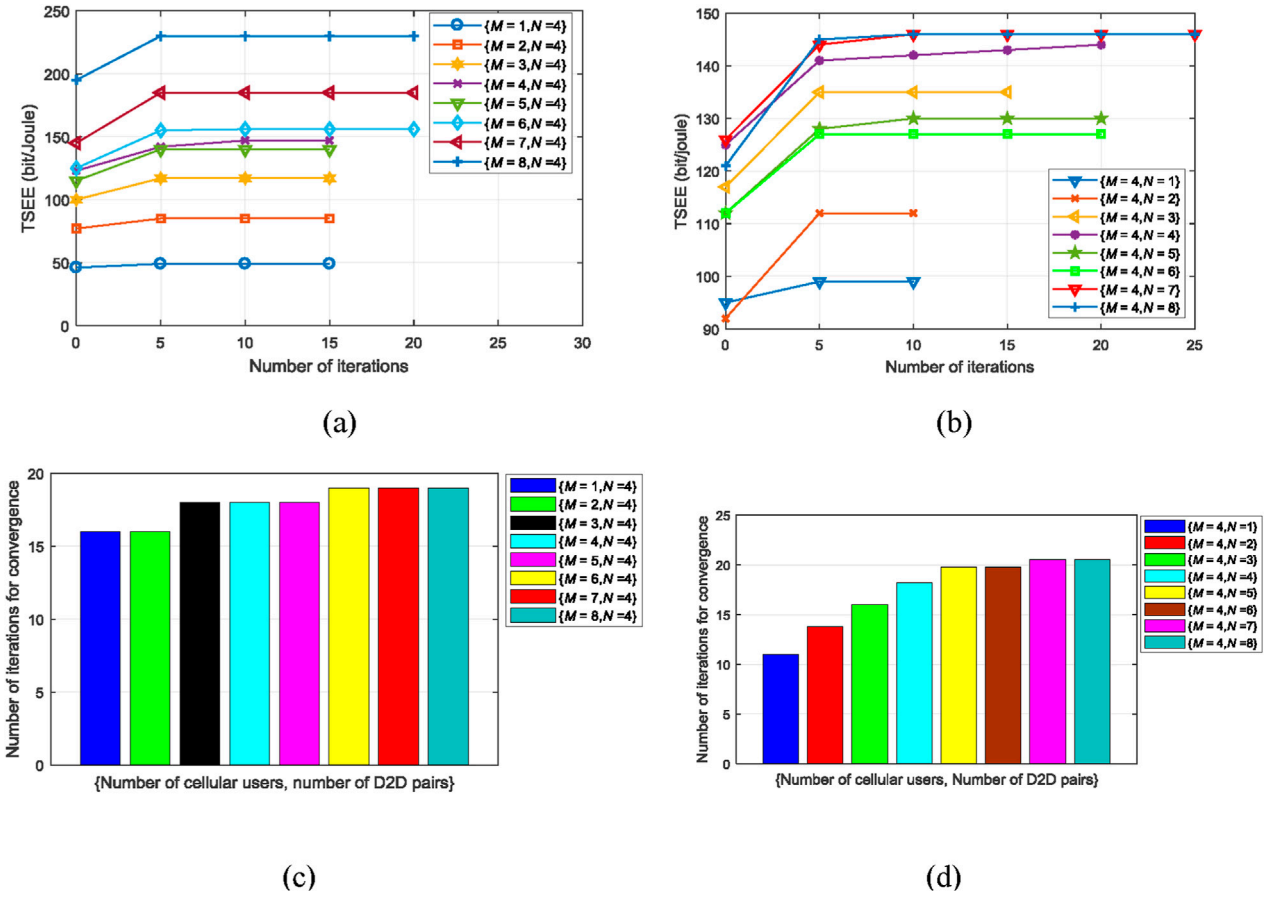


FIGURE 3
Iterative convergence of algorithms with internal and external iterative optimization. **(a)** Convergence when the number of cellular users' changes; **(b)** Convergence when D2D pairs changes; **(c)** Number of iterations required for convergence changes with the number of cellular users; **(d)** number of iterations required for convergence with changes in D2D pairs.

objective is to maximize D2D communication's energy efficiency while guaranteeing that cellular users' and D2D pairs' transmission and secrecy rates satisfy the necessary standards. Power regulation and channel allocation are the two subproblems that make up the optimization issue. Iterative optimization based on the Dinkelbach algorithm, the Lagrange dual technique, and the Kuhn-Munkres algorithm yields the ideal solution.

4. Cellular User Secrecy and Energy Efficiency Maximization (CSEEM) Algorithm. With the goal of maximizing cellular user secrecy and energy efficiency, the spectrum reuse and power control strategies are optimized, while ensuring that the transmission rate and secrecy rate of all cellular users and D2D pairs meet the requirements.

The proposed algorithm, PSO algorithm, RSPA algorithm, the algorithm in Ref. [17] and the algorithm based on CSEEM were compared under the same scenario. The TSEE comparison of different algorithms is shown in Figure 4. Among them, the result of PSO algorithm is the average of the results obtained from 20 simulations under the same scenario.

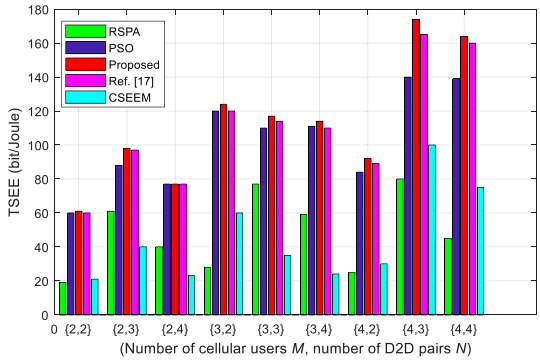


FIGURE 4
Comparison of TSEE using different algorithms with different combinations of cellular users M and D2D pairs N.

As shown in Figure 4, the proposed algorithm performs better in improving the network secrecy efficiency, followed by the algorithm in [17] and the PSO algorithm, while the algorithm based on cellular user secrecy efficiency maximization and the RSPA

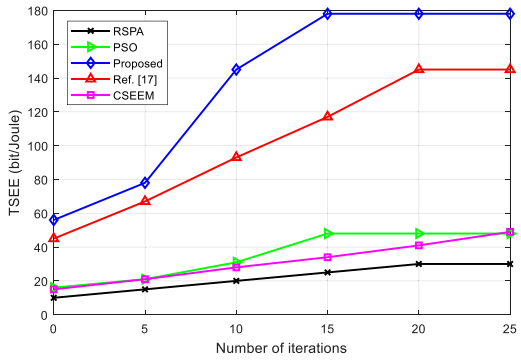


FIGURE 5
Comparison of TSEE of algorithms under increasing number of iterations.

algorithm perform the worst. The PSO method performs poorly because it is dependent on the parameter values and is prone to becoming caught in local optima. The optimization objective of the algorithm in [17] is to increase the D2D communication efficiency, but it also converts the non-convex optimization issue into a convex optimization problem for solution. The approach is somewhat less effective in increasing network secrecy efficiency than the technique in this study, according to simulation data. This is because D2D has a shorter communication distance and a higher transmission rate. Through the resource allocation algorithm, it can achieve a much higher secrecy rate than cellular users with lower power consumption than cellular users. Therefore, D2D communication efficiency has a greater impact on TSEE, and the two are positively correlated. The algorithm based on cellular user secrecy efficiency maximization aims to maximize cellular user secrecy efficiency. The findings demonstrate that increasing cellular user secrecy efficiency comes at the expense of significantly lowering D2D transmission and secrecy rates, which also lowers TSEE.

Additionally, the TSEE of the suggested algorithm shows that when the total number of cellular users and D2D pairs is equal, the TSEE is higher when there are more cellular users than there are D2D pairs than when there are fewer cellular users. This is because, in the former case, D2D pairs have relatively more reusable spectrum resources compared to the latter. Although spectrum reuse inevitably leads to co-channel interference, spectrum reuse and power control strategies can be employed to mitigate this interference, thereby achieving a higher secrecy rate with lower transmit power. This also demonstrates the effectiveness of the proposed algorithm in optimizing spectrum reuse and power control strategies, mitigating interference, and improving network secrecy efficiency.

Figure 5 compares the TSEE of the proposed and existing algorithms under increasing number of iterations. As can be seen from Figure 5, the TSEE of all algorithms increases with increasing number of iterations. Furthermore, the proposed algorithm achieves better TSEE for less number of iterations as compared with RSPA, PSO, Ref. [17] scheme and CSEEM scheme, which further validated its effectiveness.

5.2.3 Impact of UAV altitude on network performance

The ratio of total secrecy rate to total power consumption for all cellular users is known as cellular communication secrecy efficiency (CSEE), while the ratio of total secrecy rate to total power consumption for all D2D pairs N is known as D2D communication secrecy efficiency (DSEE). The UAV altitude was changed with the number of cellular users M and D2D pairings N being {3,1}, {3,2}, {3,3}, {3,4}, and {3,5}, respectively, in order to examine the effect of UAV altitude on TSEE, CSEE, and DSEE. The suggested algorithm was used to run simulations, and Figure 6 displays the results.

Figure 6a shows that when the number of cellular users and D2D pairings is {3,2}, the TSEE tends to expand first, then decrease, and then stabilize. When the number of cellular users and D2D pairs is {3,1}, {3,3}, and {3,4}, the TSEE exhibits a trend of first dropping, then growing, and finally stabilizing. When the number of cellular users and D2D pairings is {3,5}, the TSEE gradually increases until stabilizing. This is because variations in UAV altitude have distinct effects on different places, as well as differing numbers of cellular users and D2D pairings. The TSEE may initially rise and then fall, or it may rise and then fall before stabilizing. The CSEE often exhibits a tendency of initially rising, then falling, and eventually stabilizing, as seen in Figure 6b. This is due to the fact that when UAV altitude increases, the air-to-ground channel gain initially rises and then falls. The CSEE exhibits an improving trend because cellular users can fulfill the minimum secrecy rate requirement with a lower transmit power as the air-to-ground channel gain rises. As shown in Figure 6c, the DSEE variation, which is defined in this article as the percentage of the absolute value of the difference between the greatest and lowest values within the observation range to the final stable value, is not significant. This is due to the fast transmission rate and small distance of D2D communication. Despite being impacted by interference from cellular users and other D2D pairs due to spectrum reuse and cellular users changing their transmission power with changes in UAV altitude, D2D communication can achieve a high secrecy rate by allocating resources appropriately and the interference changes of cellular users have little effect on it.

Figure 7 compares the performance of the proposed and existing algorithms under different parameters. In Figure 7a, the performance of the secrecy rate of algorithms is evaluated under maximum transmit power $P_{\max}$. As can be seen from Figure 7a, the secrecy rate of all algorithms increases with increasing $P_{\max}$. However, the proposed algorithm has improved secrecy rate over the existing algorithms, which further validated the effectiveness. In Figure 7b, the TSEE of the algorithms is compared under increasing $P_{\max}$. It is worth notable that the proposed algorithm has higher TSEE as compared to existing algorithms for every value of $P_{\max}$.

6 Conclusion

A resource allocation strategy for UAV-assisted D2D communication networks under passive eavesdropping circumstances was examined in this research. A combination optimization of spectrum reuse and power management techniques

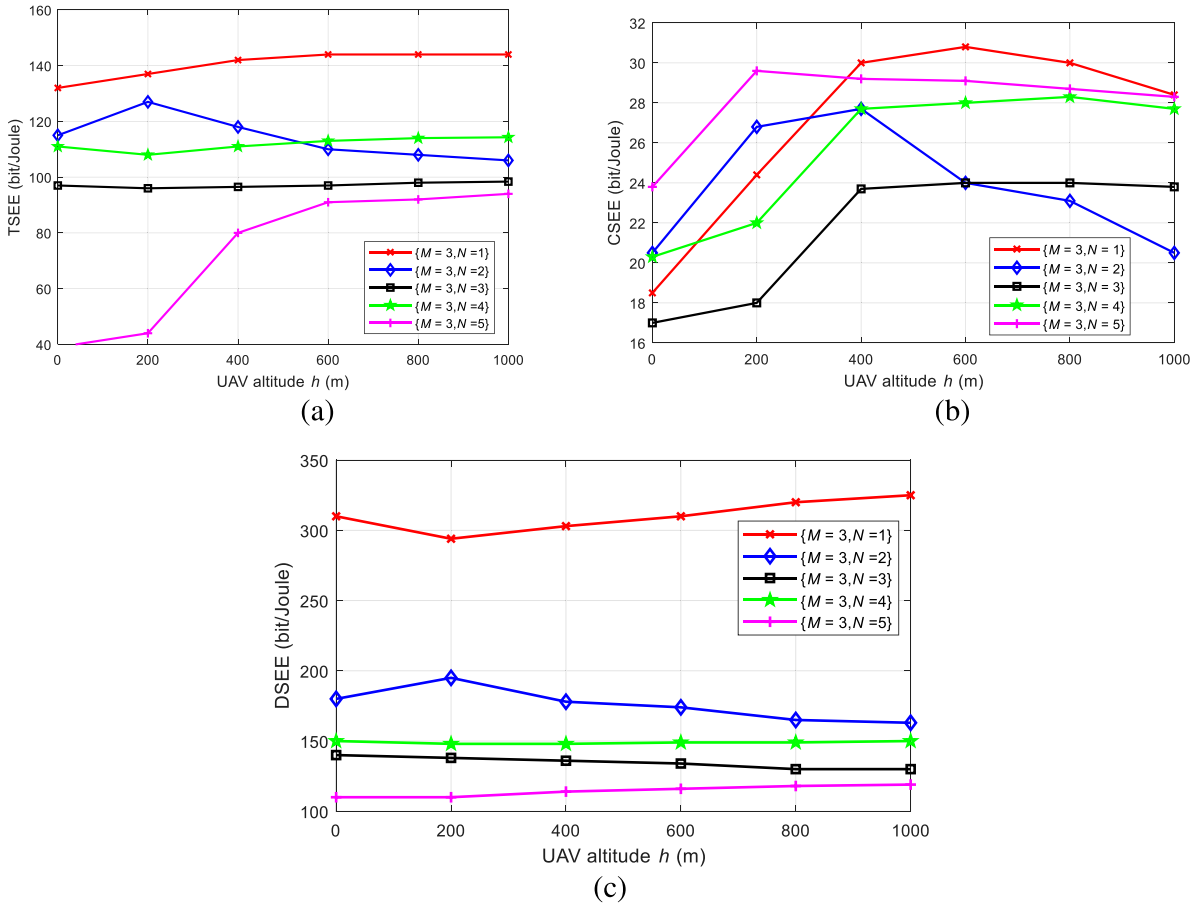


FIGURE 6
The impact of UAV altitude on TSEE, CSEE, and DSEE. **(a)** TSEE variation with UAV altitude; **(b)** CSEE variation with UAV altitude; **(c)** DSEE variation with UAV altitude.

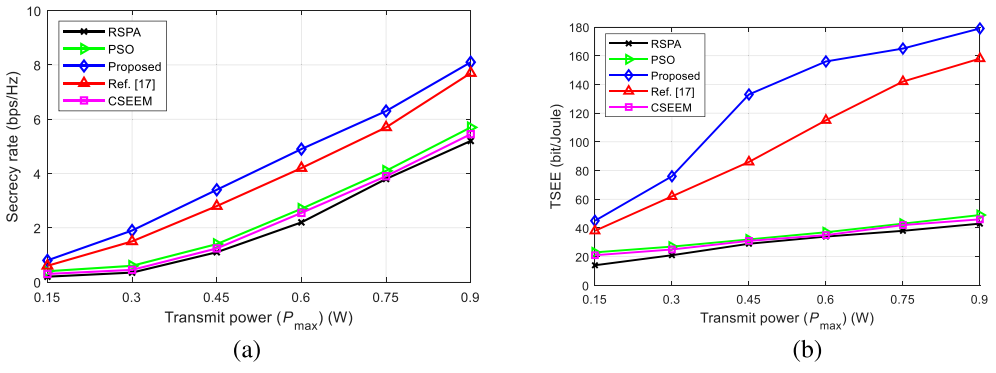


FIGURE 7
Impact of transmit power on the algorithms performance. **(a)** Secrecy rate under P_{max}; **(b)** TSEE under P_{max}.

was carried out with the goal of maximizing network secrecy efficiency while taking into account the limitations of minimum secrecy rate and maximum transmit power. Since this optimization issue was nonlinear and nonconvex, it was challenging to find a straightforward analytical solution. Consequently, this work suggested an internal and external iterative optimization technique that combined a convex approximation approach with the Dinkelbach algorithm. The usefulness of the suggested method in enhancing secrecy efficiency, reducing interference, and optimizing power control and spectrum reuse schemes was confirmed by

simulations. Additionally, the effect of UAV altitude on network secrecy effectiveness was assessed.

The proposed research was based on optimal channel state information and accurate user location information. However, in practical UAV communication networks, obtaining optimal channel state information and accurate location information is very difficult due to link latency, the dynamic flight of UAVs, and the passive nature of eavesdroppers. Therefore, future research would focus on UAV-assisted network secrecy communication technologies under conditions of imperfect channel state information and user location information.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding authors.

Author contributions

SA: Conceptualization, Data curation, Formal Analysis, Investigation, Methodology, Project administration, Resources, Supervision, Validation, Visualization, Writing – original draft, Writing – review and editing. NH: Conceptualization, Formal Analysis, Investigation, Methodology, Project administration, Resources, Software, Supervision, Visualization, Writing – original draft, Writing – review and editing. FA-T: Conceptualization, Data curation, Formal Analysis, Methodology, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing – original draft, Writing – review and editing. RS: Conceptualization, Data curation, Formal Analysis, Investigation, Project administration, Resources, Supervision, Validation, Visualization, Writing – original draft, Writing – review and editing. HG: Conceptualization, Data curation, Formal Analysis, Investigation, Methodology, Resources, Software, Supervision, Validation, Visualization, Writing – original draft, Writing – review and editing. LA: Conceptualization, Data curation, Formal Analysis, Methodology, Resources, Software, Supervision, Validation, Visualization, Writing – original draft, Writing – review and editing. DN-R: Conceptualization, Data curation, Investigation, Project administration, Resources, Software, Supervision, Validation, Visualization, Writing – original draft, Writing – review and editing. JE-G: Conceptualization, Data curation, Formal Analysis, Funding acquisition, Methodology, Project administration, Resources, Software, Supervision, Visualization, Writing – original draft, Writing – review and editing. DA: Conceptualization, Formal Analysis, Investigation, Methodology, Resources, Software, Supervision, Validation, Visualization, Writing – original draft, Writing – review and editing.

Funding

The author(s) declared that financial support was received for this work and/or its publication. Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2026R952), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. This work was supported by the Operational Programme "Research, Innovation and Digitalisation for Smart Transformation 2021 - 2027" under Project NoBG16RFPR002-1.014-0006-C01 "National center of excellence for mechatronics and clean technologies."

Conflict of interest

The author(s) declared that this work was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declared that generative AI was not used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Yin C, Yang H, Xiao P, Chu Z, Palacios E. Resource allocation for UAV-assisted wireless powered D2D networks with flyinh and ground eavesdropping. *IEEE Commun Lett* (2023) 27(8):2103–7. doi: 10.1109/lcomm.2023.3289881

2. Deng X, Deng Z, Zheng L, Yang C, Chen C. Optimization of D2D emergency communication resources for UAV relay based on DA-STD3. *EURASIP J Wireless Commun Networking* (2024) 24(88):1–15. doi: 10.1186/s13638-024-02416-x

3. Alhazmi A, Arafah M. Neural network-based adaptive resource allocation for 5G heterogeneous ultra-dense networks. *Sensors* (2025) 25(24):1–13. doi: 10.3390/s25247521

4. Zhang L, Qin D, Zhao B, Yang J, Bie H, Ma L. IRL-based co-channel interference optimization for UAV cellular network communication links. *IEEE Trans Cogn Commun Networking* (2026) 12:8562–78. doi: 10.1109/tccn.2026.3697238

5. Yin X, Xue Z. Wiretap channel with information embedding on actions. *Entropy* (2014) 16(4):1–15. doi: 10.3390/e16042105

6. Lohan P, Mishra D, Nguyen J, Gupta V. Secrecy-aware UAV position-aided jamming for practical eavesdropper localization models. *Vehicular Commun* (2022) 33(1):1–15. doi: 10.1016/j.vehcom.2021.100430

7. Guo K, Cao K, Xiong J, Ma D, Zhao H. A lightweight key generation scheme for the internet of things. *IEEE Internet Things J* (2021) 8(15):12137–49. doi: 10.1109/jiot.2021.3060438

8. Yu X, Niu W, Zhu Y, Zhu H. UAV-assisted cooperative offloading energy efficiency system for mobile edge computing. *Digital Commun Networks* (2024) 10(1):16–24. doi: 10.1016/j.dcan.2022.03.005

9. Nguyen T, Hoang T, Tran P. Secrecy performance optimization for UAV-based relay NOMA systems with friendly jamming. *Computer Commun* (2025) 235:1–15. doi: 10.1016/j.comcom.2025.108086

10. Yang B, Taleb T, Fan Y, Shen S. Mode selection and cooperative jamming for covert communication in D2D underlaid UAV networks. *IEEE Netw* (2021) 35(2):104–11. doi: 10.1109/mnet.011.2000100

11. Su Z, Feng M, Tang J, Chen Z, Fu Y, Zhao N, et al. Energy-efficiency optimization for D2D communications underlaying UAV-assisted industrial IoT networks with SWIPT. *IEEE Internet Things J* (2023) 10(3):1990–2002. doi: 10.1109/jiot.2022.3142026

12. Qi H, Yuan X, Zhang Q, Yang Z. Joint power-trajectory-scheduling optimization in a mobile UAV-enabled network via alternating iteration. *China Commun* (2022) 19(1):136–52. doi: 10.23919/jcc.2022.01.011

13. Zhang J, Chuai G, Gao W. Energy-efficiency optimization for energy-harvesting-enabled mmWave-UAV heterogeneous networks. *Entropy* (2022) 24(2):1–15. doi: 10.3390/e24020300

14. Alsharoa A, Yuksel M. Energy efficient D2D communications using multiple UAV relays. *IEEE Trans Commun* (2021) 69(8):5337–51. doi: 10.1109/tcomm.2021.3078786

15. Selim M, Rihan M, Yang Y, Ma J. Optimal task partitioning bit allocation and trajectory for D2D-assisted UAV-MEC systems. *Peer-to-Peer Networking Appl* (2021) 14(1):215–24. doi: 10.1007/s12083-020-00955-w

16. Wu H, Wen Y, Tao X, Xu J. Anti-jamming and anti-eavesdropping in A2G communication system with jittering UAV. *China Commun* (2023) 20(10):230–44. doi: 10.23919/jcc.fa.2021-0430.202310

17. Chen X, Zhou X, Zhao J, Shen F, Sun S. Energy-efficient resource allocation for secure D2D communications underlaying UAV-enabled networks. *IEEE Trans Vehicular Technology* (2022) 71(7):7519–31. doi: 10.1109/tvt.2022.3168277

18. Yu Y, Guo T, Yang Y, Ji L. Secrecy energy efficiency optimization for downlink two-user OFDMA network with SWIPT. *IEEE Syst J* (2019) 13(1):324–35. doi: 10.1109/jsyst.2017.2775607

19. Li H, Hongjian L. Enhanced energy efficiency in UAV-assisted mobile edge computing through improved hybrid nature-inspired algorithm for task offloading. *J Netw Computer Appl* (2025) 243(1):1–14. doi: 10.1016/j.jnca.2025.104290

20. Al-Hourani A, Kandeepan S, Lardner S. Optimal LAP altitude for maximum coverage. *IEEE Wireless Commun Lett* (2014) 3(6):569–72. doi: 10.1109/lwc.2014.2342736

21. Liang L, Li Y, Xu W. Resource allocation for D2D-enabled vehicular communications. *IEEE Trans Commun* (2017) 65(7):3186–97. doi: 10.1109/tcomm.2017.2699194

22. Dinkelbach W. On nonlinear fractional programming. *Management Sci* (1967) 13(7):492–8. doi: 10.1287/mnsc.13.7.492

23. Jung S, Kim J, Kim J. Joint message-passing and convex optimization framework for energy-efficient surveillance UAV scheduling. *Electronics* (2020) 9(9):1–14. doi: 10.3390/electronics9091475

24. Si P, Qian L, Zhao J, Lam K. A hybrid framework of reinforcement learning and convex optimization for UAV-based autonomous metaverse data collection. *IEEE Netw* (2023) 37(37):248–54. doi: 10.1109/mnet.011.2300032

25. Montes A, Stutzle T, Birattari M, Dorigo M. Frankenstein's PSO: a composite particle swarm optimization algorithm. *IEEE Trans Evol Comput* (2009) 13(5):1120–32. doi: 10.1109/tevc.2009.2021465

26. Liu Z, Zhu B, Xie Y, Ma K, Guan X. UAV-aided secure communication with imperfect eavesdropper location: robust design for jamming power and trajectory. *IEEE Trans Vehicular Technology* (2024) 73(5):7276–86. doi: 10.1109/tvt.2023.3347769

27. Zhao M, Wang Z, Guo K, Zhang R, Quek TQS. Against mobile collusive eavesdroppers: cooperative secure transmission and computation in UAV-assisted MEC networks. *IEEE Trans Mobile Comput* (2025) 24(6):5280–97. doi: 10.1109/tmc.2025.3529929

28. Wei J, Guo Y, Wang H, Gu J, Liu J, Ding G. Cognitive jamming-aided UAV multi-user covert communication. *IEEE J Selected Areas Commun* (2026) 44:1873–87. doi: 10.1109/jsac.2025.3639012

29. Shang Y, Peng Y, Ye R, Lee J. RIS-assisted secure UAV communication scheme against active jamming and passive eavesdropping. *IEEE Trans Intell Transportation Syst* (2024) 25(11):953–63. doi: 10.1109/tits.2024.3417932

30. Zeng J, Mishra D, Habibi Gharakheili H, Seneviratne A. Fairness aware secure energy efficiency maximization for UAVassisted data collection in backscattering networks. *Vehicular Commun* (2025) 52:100881. doi: 10.1016/j.vehcom.2025.100881

31. Sun Y, An K, Zhu Y, Zheng G, Wong K-K, Chatzinotas S. Energy-efficient hybrid beamforming for multilayer RIS-assisted secure integrated terrestrial-aerial networks. *IEEE Trans Commun* (2022) 70(6):4189–210. doi: 10.1109/tcomm.2022.3170632

32. Abdissa Bayessa G, Chai R, Liang C, Wang Q, Li J, Chen Q. Attention-based hierarchical-DRL with mask for multi-timescale caching, association, and secure content delivery in UAV-enabled ISAC networks. *IEEE Trans Green Commun Networking* (2026) 10:1779–94. doi: 10.1109/tgcn.2026.3651458

33. Tran AT, Tran QN, Ha DH, Ha DB. Secure edge computing in UAV-assisted backscatter communication NOMA wireless sensor network with friendly jamming. In: NT Nguyen, editor. *Computational Intelligence in Engineering Science, Ser. Communications in Computer and Information Science*, 2584. Cham: Springer (2026). 319–34. doi: 10.1007/978-3-031-98161-6_24

34. Li T, Li Y, Chen Y, Chen CS, Shao J. Countering intelligent uav eavesdroppers via IRS-assisted UAV: a game-theoretic approach. *IEEE Trans Netw Sci Eng* (2026) 13:5229–46. doi: 10.1109/tnse.2025.3648816

35. Cui C, Jia Z, You J, Dong C, Wu Q, Han Z. Robust and secure computation offloading and trajectory optimization for multi-UAV MEC against aerial eavesdropper. *IEEE Trans Vehicular Technology* (2025) 1–14. doi: 10.1109/TVT.2025.3612755