EAI Endorsed Transactions
on Industrial Networks and Intelligent Systems
EAI.EU Research Article

Secure UAV-assisted Mobile Edge Computing for IoT with Backscatter Communication in the Presence of a Moving Eavesdropper

Van-Long Nguyen[1], Duy-Hung Ha[2,*], Van-Truong Truong[3,4], Truc Thanh Tran[5], Dac-Binh Ha[1]

[1]School of Engineering and Technology, Duy Tan University, Da Nang, 550000, Vietnam.
[2]Wireless Communications Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, HCMC, Vietnam.
[3]Faculty of Electrical-Electronic Engineering, Duy Tan University, Da Nang, 550000, Viet Nam.
[4]Institute of Research and Development, Duy Tan University, Da Nang, 550000, Viet Nam.
[5]Department of Information Technology, Greenwich Vietnam, FPT University, Da Nang, 550000, Vietnam.

Abstract

The perception layer security (PLS) is crucial for ensuring that the data collected by Internet of Things (IoT) devices is accurate, reliable, and protected against various security threats. It helps maintain the overall integrity of the IoT ecosystem and builds trust in its applications. Our work explores the integration of network and PLS in a UAV-enabled mobile edge computing (MEC) system for IoT. This system supports multiple users with a combined non-orthogonal and time-division multiple access (NOTDMA) scheme and is based on backscatter communication (BC). In this system, the UAV-mounted server functions as a hybrid access point (HAP) and hovers over a cluster of energy-constrained IoT devices to transmit RF energy and assist them in performing tasks by employing BC. The IoT devices apply the combined NOTDMA scheme to offload their tasks to the HAP. A mobile passive eavesdropper attempts to intercept information from IoT devices without actively launching any attacks. A partial offloading scheme with various encryption algorithms is proposed to improve the system's secrecy, which adapts to the users' non-linear harvested energy levels. In addition, considering the network and physical security, we derive a approximation expression for the secrecy successful computation probability (SSCP). This expression incorporates factors such as harvested energy, local computing and encryption latency, edge offloading latency, processing, decryption, and the associated secrecy costs. The optimization problem for maximizing SSCP is formulated and solved using an Immune algorithm to find the optimal set of device parameters and UAV altitude. Key parameters affecting secrecy and latency performance are analyzed to better understand the system's behavior. Numerical simulations are provided to validate the accuracy of our analysis.

Received on 12 March 2025; accepted on 27 April 2025; published on 23 October 2025

Keywords: physical layer security, Internet of Things, mobile edge computing, unmanned aerial vehicle, RF energy harvesting, secrecy successful computation probability

doi:10.4108/eetinis.v12i3.8889

1. Introduction

The Internet of Things (IoT) refers to a network of interconnected devices, objects, sensors, and vehicles communicating over the Internet. This connectivity enables them to collect, share, and exchange data without direct human intervention [1]. Rapidly deploying real-time IoT applications has created a growing demand for significant mobile data transmission and computing capabilities. However, three important challenges must be addressed: efficient real-time data processing, energy charging, and security [2].

To tackle the first challenge, a mobile edge computing (MEC) solution is proposed, which involves relocating servers to the network's edge to support users better

*Corresponding author. Email: haduyhung@tdtu.edu.vn
This article was presented in part at the International Conference on Industrial Networks and Intelligent Systems (INISCOM), 2025.

[3]. Unmanned aerial vehicles (UAVs) are utilized in this context due to their mobility, Internet access, computing resources, and energy services, particularly in disaster-stricken areas or emergencies [4, 5]. Additionally, backscatter communication (BC) technology is a suitable method for IoT applications, enabling the transfer of RF energy to users and allowing devices to reflect signals to a reader to transmit data [6]. Furthermore, radio frequency (RF) energy harvesting (EH) technology captures and converts ambient RF signals, such as those emitted by communication systems, into usable electrical energy. This process is particularly beneficial for powering low-energy devices, such as sensors and IoT devices, without relying on batteries or wired power sources [7]. Unlike traditional orthogonal multiple access (OMA) schemes, such as FDMA, TDMA, and CDMA, where different users are assigned distinct frequency bands, time slots, or codes to prevent interference, NOMA enables multiple users to share the same OMA resources by exploiting variations in their power levels [8]. The study in [9] explored the simultaneous transmitting and reflecting reconfigurable intelligent surface-assisted uplink NOMA MEC systems. The integration of NOMA with BC in IoT networks has been examined in [10].

IoT security is a crucial aspect of the overall security landscape, requiring a comprehensive strategy encompassing device security, data protection, network defenses, and user privacy. As the number of IoT devices continues to rise, there is an urgent need for robust security measures to protect against potential threats and vulnerabilities, ensuring the safe and reliable operation of IoT systems [11]. Perception layer security refers to the security measures implemented at the perception layer of the IoT architecture [12]. The perception layer is the lowest in the IoT framework and is responsible for data collection through various sensors and devices. As these devices collect and transmit data, ensuring the security and integrity of that data is crucial. In this context, network security means ensuring data is encrypted when transmitted over a network to protect it from eavesdropping or interception. Another emerging approach is physical secrecy, which enhances the security of IoT systems by leveraging the inherent fading characteristics of wireless channels in wireless communication systems [13].

Several studies have focused on security issues in BC-based UAV-enabled MEC networks [14–19]. For instance, the work in [14] introduced a two-way ambient BC (TW-AmBC) network that includes an eavesdropper. This study derived analytical and asymptotic expressions to assess the physical layer security, focusing on outage and intercept probability. In [15], researchers examined physical-layer authentication to identify users and prevent unauthorized access and malicious activities within AmBC-based NOMA symbiotic networks. They developed three physical layer authentication (PLA) schemes based on the multiplexing methods used for authentication tags to enhance secrecy performance. In [18], the authors examined secure data transmissions within a UAV-aided communication system, where the UAV functions as a flying base station that transmits confidential information to a ground user. Simultaneously, an eavesdropper moves nearby, trying to intercept the legitimate data transmission. The UAV's trajectory is optimized in response to the unpredictable movements of the eavesdropper to maximize secrecy throughput in this fast-changing environment. The authors propose a deep reinforcement learning framework by reformulating the problem as a Markov decision process. The work [19] designed secure multi-task multi-step computing offloading mechanisms in ultradense multi-task NOMA-enabled IoT networks. The joint overall energy consumption optimization, such as device association, channel selection, security service assignment, power control, and computation offloading, are carried out, considering proportional resource allocation and constraints on latency and security costs.

Unlike previous studies, our work examines secrecy performance and optimization in a multi-user UAV-assisted MEC IoT system, focusing on integrating network and physical security. This system utilizes BC and a combined NOTDMA scheme. The main contributions of our paper are as follows:

- We propose a novel model for a multi-user UAV-assisted MEC IoT network, where the UAV-mounted server acts as a high-altitude platform, providing RF energy and computing services to support IoT devices.
- In the context of perception layer security, the considered system's approximation expressions of secrecy successful computation probability (SSCP) is derived.
- The multi-objective optimization problem in terms of SSCP is formulated under the constraint of security cost. Accordingly, an advanced Immune algorithm is proposed to find the optimal front to achieve the best performance for this proposed system.
- The impact of network parameters, e.g., transmit power, bandwidth, and task allocation, on the system secrecy performance is examined by numerical results to verify the efficiency and effectiveness of UAV, partial offloading scheme, and encryption algorithm deployment in the MEC network.

The remainder of this paper is organized as follows: Section 2 introduces the proposed system model. Section 3 provides performance analysis and optimization of

the system. Section 4 presents numerical results and discussion. Finally, Section 5 concludes the paper.

2. System Model

We consider a secure UAV-enabled mobile edge computing (MEC) system for IoT applications, where a UAV equipped with an edge server provides energy and computing services to pairs of ground IoT devices. These IoDs communicate with the UAV via backscatter communication (BC), using NOMA for intra-pair access and TDMA across pairs. Each IoD partially offloads computation tasks while facing the threat of a mobile eavesdropper attempting to intercept their data. This work emphasizes the security of the IoT perception layer, where data acquisition and communication occur, by jointly applying physical-layer secrecy and stream-cipher-based encryption at the network level.

2.1. System and Channel Model

Figure 1 illustrates a UAV-enabled MEC IoT system that utilizes BC. In this system, a UAV hybrid access point (HAP), denoted as $\mathbf{U}$, is deployed to serve K pairs of energy-constrained ground IoT devices, denoted as $\{D_{1k}, D_{2k}\}$, $k \in \{1, 2, ..., K\}$, in the presence a passive eavesdropper, denoted as $\mathbf{E}$. Specifically, the $\mathbf{U}$, which is equipped with an edge server, hovers in the sky over the IoT devices (IoDs) to provide them with energy and computing services. The IoDs apply a BC scheme to harvest RF energy, enabling them to perform some subtasks locally while offloading the remaining tasks to the MEC server. The ground IoDs are divided into near and far users, which are paired to implement the NOMA scheme. Meanwhile, K user pairs employ TDMA to access the server at $\mathbf{U}$. These users modulate their data bits based on incident RF signals and reflect this information on $\mathbf{U}$. Meanwhile, the eavesdropper $\mathbf{E}$ attempts to intercept the information transmitted by these IoDs without engaging in malicious attacks. All transceivers, including the HAP, are assumed to be single-antenna devices operating in half-duplex mode. The IoDs are assumed to be on the ground and randomly distributed within two circular areas centered at $\mathbf{O} = (0, 0, 0)$ following the same uniform distribution. In which the near users are located in a circular area with a radius of r, while the far users are distributed between two circular areas with a radius of r and R, where $r < R$. The $\mathbf{U}$ hovers at the position as $(0, 0, z_U)$, while the $\mathbf{E}$ roams through the coverage of $\mathbf{U}$ as in Figure 1.

We assume that the wireless channels for ground-to-UAV (G2U) and UAV-to-ground (U2G) communications are modeled using two types of fading: large-scale fading and small-scale fading [20]. According to [5], the mean path loss considering the probability of both LoS and NLoS links between the $\mathbf{U}$ and the user D_{ik} $(i \in \{1, 2\})$

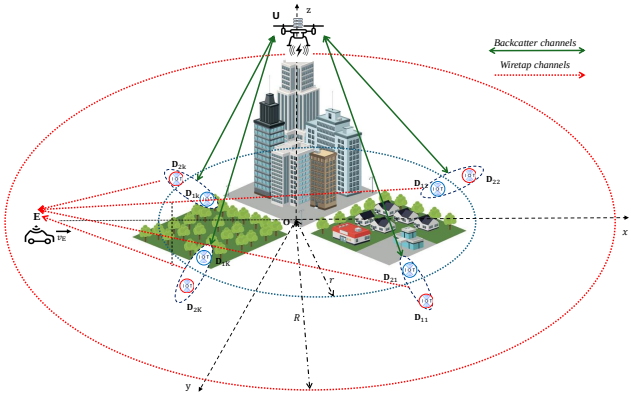

Figure 1. System model for UAV-enabled MEC IoT BC network with an eavesdropper

is given as:

$$\mathcal{L}_{ik}\left(d_{ik}, \theta_{ik}\right) = \left[\Phi_{NLoS} + \frac{\Phi_{LoS} - \Phi_{NLoS}}{1 + b.e^{a\left(-\frac{180}{\pi}\theta_{ik} + b\right)}}\right] d_{ik}^{\alpha}, \quad (1)$$

where d_{ik} denotes the distance between $\mathbf{U}$ and D_{ik}, $\theta_{ik} \triangleq \arcsin\left(\frac{z_U}{d_{ik}}\right)$ represents the incident angle of D_{ik}, α stands for the path-loss exponent, a and b denote the constant parameters according to the ambient environment (rural, urban, dense urban, etc.). The parameter Φ_{Δ}, which depends on the environment, is defined as:

$$\Phi_{\mathcal{X}} \triangleq \frac{4\pi f_c \Psi_{\mathcal{X}}}{c}, \quad (2)$$

where $\Psi_{\mathcal{X}}$, $\mathcal{X} \in \{\text{LoS,NLoS}\}$, denotes the excessive path loss of the LoS and NLoS propagation (as also used in [20]), f_c stands for the carrier frequency, c represents the speed of light.

The channel coefficients of $D_{ik} - \mathbf{U}$ and $D_{ik} - \mathbf{E}$ links are denoted as h_{ik}, h_{ikE}, respectively. Assume that the channel coefficients of the $D_{ik} - \mathbf{U}$ links are independent and identically distributed (i.i.d.) and follow a Nakagami-m distribution. Thus, the cumulative distribution function (CDF) and the probability density function (PDF) of the channel power gains $V = |h_{ik}|^2$ are given as follows [9]:

$$F_V(x) = 1 - e^{-\frac{m_V}{\lambda_V}x} \sum_{l=0}^{m_V - 1} \frac{1}{l!}\left(\frac{m_V}{\lambda_V}x\right)^l, \quad (3)$$

$$f_V(x) = \frac{1}{(m_V - 1)!}\left(\frac{m_V}{\lambda_V}\right)^{m_V} x^{m_V - 1} e^{-\frac{m_V}{\lambda_V}x}, \quad (4)$$

where $\lambda_V = \mathbf{E}[V]$, $m_V \geq 1/2$ is the fading severity factor. For simplicity, we assume that $m_{|h_{ik}|^2} = m_U$, $\lambda_{|h_{ik}|^2} = \lambda_U$, $\forall k \in \{1, ..., K\}$ and $i \in \{1, 2\}$. $\mathbf{E}[.]$ stands for expectation operator.

Meanwhile, we assume that the ground channels of the $D_{ik} - \mathbf{E}$ links undergo i.d.d. Rayleigh fading.

Table 1. Summary of Key Notations and Parameters

Description	Notation
Number of IoT device pairs	K
IoT device i in pair k (near/far)	D_{ik}
UAV hybrid access point	$\mathbf{U}$
Mobile passive eavesdropper	$\mathbf{E}$
Radii for near and far zones	r, R
UAV hovering altitude	z_U
Carrier frequency	f_c
Speed of light	c
Path-loss exponent	α
Environmental parameters for LoS probability	a, b
Excessive path loss coefficients	Ψ_{LoS}, Ψ_{NLoS}
Nakagami-m fading severity	m_1, m_2
Channel coefficients (UAV, Eavesdropper)	h_{ik}, h_{ikE}
Channel power gains	X_{ik}, Z_{ik}
Backscattering reflection coefficient	ξ_{ik}
Energy conversion efficiency	η
Harvested RF power (input to nonlinear model)	P_{ik}^H
Actual harvested power (non-linear output)	P_{ik}
Task length of IoT device	L_{ik}
Task dividing ratio (local/offloaded)	β_{ik}
CPU-cycle frequency (IoT/MEC)	f_{ik}, f
CPU cycles per bit (IoT/MEC)	κ_{ik}, κ
Effective capacitance coefficient	ρ_{ik}
Encryption/decryption CPU cycles	ψ_m, ψ_m^*
Number of cryptographic algorithms	M
Security level / Expected level	q_m, $q_{k,j}^*$
Security risk coefficient	v
Maximal security cost per device	ϕ_{ik}
Average transmit SNR	γ_U
Instantaneous SNR (UAV / Eavesdropper)	γ_{ik}, γ_{ikE}
Instantaneous secrecy capacity	C_{ik}^s
System bandwidth	W
Subchannel bandwidth per user	B
Local / offloading latency	τ_{ik}^D, τ_k^U
Total latency per user pair	τ_k
Latency threshold	T

This assumption is based on typical ground-to-ground communication environments, where there is no guaranteed line-of-sight (LoS) path due to environmental obstacles. As such, Rayleigh fading serves as an appropriate channel model to capture the rapid multipath variation in scenarios such as urban or indoor eavesdropping attacks. Thus, the CDF and PDF of corresponding power gains are given by [21]:

$$F_{|h_{ikE}|^2}(x) = 1 - e^{-x}, \tag{5}$$

$$f_{|h_{ikE}|^2}(x) = e^{-x}. \tag{6}$$

2.2. Signal Model

For the sake of simplicity, in our work, we consider a representative pair, $\{D_{1k}, D_{2k}\}$, $\forall k \in \{1, ..., K\}$. For equity, the entire flight duration of UAV is divided into N equal time slots T, and each is divided again into K equal sub-time slots $\tau = \frac{T}{K}$, $\forall k \in \{1, ..., K\}$. During the τ duration, $\mathbf{U}$ serves each pair of IoDs by employing BC and NOMA schemes, where they transmit their data ε_{ik} to $\mathbf{U}$ by modulating the $\mathbf{U}$'s signal via an air modulation technique. Accordingly, the signal received at $\mathbf{U}$ can be given by

$$y_k = \left(\sqrt{\xi_{1k} P_U} \frac{h_{1k}^2}{\mathcal{L}_{1k}} \varepsilon_{1k} + \sqrt{\xi_{2k} P_U} \frac{h_{2k}^2}{\mathcal{L}_{2k}} \varepsilon_{2k} \right) s + w, \tag{7}$$

where P_U denotes the transmit power of $\mathbf{U}$, ξ_{ik} ($i \in \{1, 2\}$) stands for the backscattering reflection coefficient of $D_{ik} (0 < \xi_{ik} < 1)$, $\varepsilon_{ik} \in \{0, 1\}$ denotes the binary data (0,1) transmitted by IoD D_{ik} to $\mathbf{U}$ via backscatter communication, $\mathbf{E}[s^2] = \mathbf{E}[\varepsilon_{ik}^2] = 1$, and w denotes the additive white Gaussian noise (AWGN) with zero mean and variance σ^2, $w \sim \mathcal{CN}(0, \sigma^2)$. $\mathbf{U}$ first decodes s, followed by ε_{1k} and finally ε_{2k}, using the successive interference cancellation (SIC) technique. The instantaneous signal-to-noise ratios (SNRs) for decoding ε_{ik} at $\mathbf{U}$ are written as

$$\gamma_{1k} = \frac{\mu_{1k} |h_{1k}|^4}{\mu_{2k} |h_{2k}|^4 + 1} = \frac{\mu_{1k} X_{1k}^2}{\mu_{2k} X_{2k}^2 + 1}, \tag{8}$$

$$\gamma_{2k} = \mu_{2k} |h_{2k}|^4 = \mu_{2k} X_{2k}^2, \tag{9}$$

where $\mu_{ik} \triangleq \frac{\xi_{ik} \gamma_U}{\mathcal{L}_{ik}^2}$, $\gamma_U \triangleq \frac{P_U}{\sigma^2}$, $X_{ik} \triangleq |h_{ik}|^2$, $\forall i \in \{1, 2\}$.

In our work, we consider the scenario in which the eavesdropper tries to intercept the information offloaded by IoT users to $\mathbf{U}$ without interference or attacks. Similar to (8), the signal received at eavesdropper $\mathbf{E}$ is expressed as

$$y_{Ek} = \sqrt{\frac{\xi_{1k} P_U}{\mathcal{L}_{1k} d_{1kE}^\alpha}} h_{1k} h_{1kE} \varepsilon_{1k} s + \sqrt{\frac{\xi_{2k} P_U}{\mathcal{L}_{2k} d_{2kE}^\alpha}} h_{2k} h_{2kE} \varepsilon_{2k} s + w_E, \tag{10}$$

where d_{ikE} represents the Euclidean distances from D_{ik} to $\mathbf{E}$, and $w_E \sim \mathcal{CN}(0, \sigma_E^2)$. Accordingly, the instantaneous SNRs received at $\mathbf{E}$ are expressed as

$$\gamma_{1kE} = \frac{\mu_{1kE} |h_{1k}|^2 |h_{1kE}|^2}{\mu_{2kE} |h_{2k}|^2 |h_{2kE}|^2 + 1} = \frac{\mu_{1kE} X_{1k} Z_{1k}}{\mu_{2kE} X_{2k} Z_{2k} + 1}, \tag{11}$$

$$\gamma_{2kE} = \mu_{2kE}|h_{2k}|^2|h_{2kE}|^2 = \mu_{2kE}X_{2k}Z_{2k}, \quad (12)$$

where $\mu_{ikE} \triangleq \frac{\xi_{ik}\gamma_E}{\mathcal{L}_{ik}d_{ikE}^{\alpha}}$, $\gamma_E \triangleq \frac{P_U}{\sigma_E^2}$, $Z_{ik} \triangleq |h_{ikE}|^2$, $\forall i \in \{1,2\}$.

2.3. Security Model

In this work, we focus on the security of the perception layer, which encompasses both network security and physical secrecy.

Network Security Model. Similar to the work of [19], in this system, we consider the varying security service requirements for different computational tasks of IoT devices. To ensure secure communication, we employ a variety of encryption algorithms, each with different types and levels of security. Thus, the IoT devices must encrypt computational tasks before offloading them, and the **U** must decrypt them afterward. Let $\mathcal{M} = \{1, 2, ..., M\}$ represent the set of encryption algorithms, with each algorithm m having a security protection level denoted by $q_m, \forall m \in \mathcal{M}$. We assume that algorithm m is constructed upon stream cipher principles, a form of symmetric encryption that operates by encrypting individual bits or bytes of data in a continuous stream, distinct from block ciphers, which process data in fixed-size blocks [22]. Consequently, algorithm m generates a pseudorandom keystream of equivalent length to the plaintext, constituting the offloaded task. This keystream is combined with the plaintext via an XOR operation, yielding the ciphertext. Decryption is achieved by reversing the process and reapplying the XOR operation with the identical keystream. Algorithms based on stream cipher paradigms offer the advantage of high processing speeds, rendering them suitable for IoT applications necessitating continuous data transmission [23].

When using encryption algorithm m for data protection, the CPU cycles required to encrypt and decrypt one bit of data are ψ_m and ψ_m^*, respectively. It is important to highlight that users do not get the expected protection, making offloaded tasks vulnerable to attacks and eavesdropping. It means that if the actual security level of certain IoT devices is lower than anticipated, there will be costs related to security vulnerabilities. The probability of failure when D_{ik} selects encryption algorithm m to protect subtask i is [19]:

$$\mathcal{P}_{k,m,j} = 1 - e^{-v_{k,j}\left[q_{k,j}^* - q_m\right]^+}, \quad (13)$$

where $v_{k,j}$ stands for the security risk coefficient of subtask j of device D_{ik}, $q_{k,j}^*$ denotes the expected protection level for subtask j of device D_{ik}, $[x]^+ = \max\{0, x\}$. The failure probability function $\mathcal{P}_{k,m,j}$ is designed to reflect a smooth and monotonic increase in failure risk when the selected encryption algorithm m does not meet the required protection level $q_{k,j}^*$. This formulation captures two key assumptions: (i) if the selected algorithm provides adequate protection ($q_m \geq q_{k,j}^*$), the failure probability is zero; and (ii) if the protection is insufficient ($q_m < q_{k,j}^*$), the failure probability increases exponentially with the gap.

The use of the exponential function is common in risk modeling to represent compounding effects and sensitivity to unmet constraints. The risk coefficient $v_{k,j}$ adjusts the steepness of this increase, allowing the model to express diverse security sensitivities among subtasks. This approach is consistent with probabilistic risk-based formulations used in secure computation and IoT system design.

If the encryption algorithm chosen for an D_{ik}'s subtask fails to meet the expected security level,, it will lead to financial loss. The security cost for all subtasks of D_{ik} is given by [19]:

$$\phi_{ik} = \sum_{m=1}^{M}\sum_{j=1}^{J} \alpha_j z_{i,k,m,j}\mathcal{P}_{i,k,m,j}, \quad (14)$$

where α_j denotes the financial loss when protection for subtask j fails, $z_{i,k,m,j}$ stands for the security service assignment indicator, where $z_{i,k,m,j} = 1$ represents that subtask j of D_{ik} employs the encryption algorithm m, otherwise $z_{i,k,m,j} = 0$.

Physical Security Model. Instantaneous secrecy capacity, a concept in information theory, relates to secure communication over a noisy channel. It denotes the maximum rate at which information can be securely transmitted at any given moment without interception by an eavesdropper. Mathematically, it can be represented as:

$$C_s = \left[C_M - C_E\right]^+, \quad (15)$$

where C_M denotes the instantaneous capacity of the legitimate channel while C_E stands for the instantaneous capacity of illegitimate channel, $[x]^+ = \max\{0, x\}$.

In this considered system, the instantaneous secrecy capacity of user D_{ik} is defined as follows [24]:

$$C_{ik}^s \triangleq \begin{cases} B\log_2\left(\frac{1+\gamma_{ik}}{1+\gamma_{ikE}}\right), & \gamma_{ik} > \gamma_{ikE} \\ 0, & \gamma_{ik} \leq \gamma_{ikE} \end{cases}, \quad (16)$$

where $B = \frac{W}{K}$ with W signifies the system channel bandwidth.

2.4. Energy Model

This study uses the non-linear EH model from [25] to represent the power harvested. Assuming that the IoT device can harvest RF energy during its BC phase τ and in all the remaining subtime-slots $(T - \tau)$. Thus, the harvested power at device D_{ik}, $i \in \{1, 2\}$, can be

obtained by

$$P_{ik} = \frac{P_m \left(\frac{1}{1+e^{-\omega(P_{ik}^H - \nu)}} - \Omega \right)}{1 - \Omega}, \quad (17)$$

where P_m stands for the maximum output DC power, $\Omega \triangleq \frac{1}{1+e^{\omega\nu}}$ in which ω and ν represent the constant values depending on the specific EH circuit employed at device D_{ik}. For simplicity, we assume that ω and ν are the same for all IoT devices. P_{ik}^H denotes the linear harvested RF power of device D_{ik}. It is given by

$$P_{ik}^H = \eta_{ik} P_U \frac{|h_{ik}|^2}{\mathcal{L}_{ik}} \frac{(1-\xi_{ik})\tau + (T-\tau)}{\tau} = \delta_{ik} X_{ik}, \quad (18)$$

where $\delta_{ik} = \frac{\eta_{ik}(K-\xi_{ik})P_U}{\mathcal{L}_{ik}}$, $0 < \eta_{ik} \leq 1$ stands for the energy conversion coefficient of D_{ik}. To keep things simple, we do not consider the energy consumed by the devices for circuit operations.

We assume that the tasks are independent and can be divided into subtasks of any size, enabling them to be computed in parallel on the IoD and the edge server of $\mathbf{U}$. In our work, each device divides its L_{ik}-bit task into $\beta_{ik}L_{ik}$-bit non-offloaded subtask and $(1-\beta_{ik})L_{ik}$-bit offloaded subtask, where β_{ik} represents the task dividing ratio, $0 \leq \beta_{ik} \leq 1$. The energy consumption model for local computing and encrypting is given by [3]:

$$E_{ik}^c = \rho_{ik}(f_{ik})^2 \left[\kappa_{ik}\beta_{ik} + \psi_m(1-\beta_{ik})\right] L_{ik}, \quad (19)$$

where ρ_{ik} represents the effective capacitance coefficient of the CPU about its architecture in device D_{ik}, κ_{ik} stands for the number of CPU cycles needed to accomplish the work per bit, f_{ik} signifies the CPU-cycle frequency at D_{ik}.

2.5. Offloading and Computation Model

In our work, we use a partial offloading scheme, allowing each IoD to execute part of the task locally while offloading the remaining portion to the UAV MEC server. Accordingly, the latency τ_{ik}^D for local computing at D_{ik}, $i \in \{1, 2\}$ includes the computational delay of the non-offloaded subtask and the encryption delay of the offloaded subtask, which is expressed as

$$\tau_{ik}^D = \frac{\left[\kappa_{ik}\beta_{ik} + \psi_m(1-\beta_{ik})\right] L_{ik}}{f_{ik}}. \quad (20)$$

Meanwhile, the latency τ_k^U at $\mathbf{U}$ includes the uplink transmission delay and the computational delay at $\mathbf{U}$ that is expressed as

$$\tau_k^U = \max\{t_{1k}^o, t_{2k}^o\} + \frac{(\kappa_U + \psi_m^*)\sum_{i=1}^{2}(1-\beta_{ik})L_{ik}}{f_U}, \quad (21)$$

where $t_{ik}^o = \frac{(1-\beta_{ik})L_{ik}}{B\log_2(1+\gamma_{ik})}$ signifies the offloading time of D_{ik}, κ_U represents the number of CPU cycles needed to accomplish the work per bit, f_U stand for the CPU-cycle frequency of $\mathbf{U}$, B denotes the subchannel bandwidth for each user k ($B = \frac{W}{K}$). In our study, we ignore the task result's return delay because each IoD's computation result has a small data volume [26].

Due to the subtasks of each IoD can be computed in parallel on the local CPU and the edge server of $\mathbf{U}$, the latency for completing all subtasks of each IoD pair is given by

$$\tau_k = \max\{\tau_{1k}^D, \tau_{2k}^D, \tau_k^U\}. \quad (22)$$

2.6. Eavesdropper's Mobility Model

To reflect more realistic attack strategies, we consider a scenario where the eavesdropper traverses along the x-axis from $(-R, 0, 0)$ to $(R, 0, 0)$ over a time duration T with an average velocity $v_E = \frac{2R}{T}$. This simplified linear mobility captures essential characteristics of practical eavesdropping threats in environments such as smart factories, logistics hubs, or military zones, where malicious ground vehicles or autonomous robots may attempt to approach sensitive regions while avoiding detection [27]. Although the motion is modeled with constant average speed for tractability, the scenario is representative of controlled mobile attacks in real-world deployments.

Furthermore, the assumption of a constant velocity for the eavesdropper allows us to investigate the impact of its movement on the SSCP. Studying more complex and practical mobility patterns of IoT adversaries is also part of our future research plans.

3. Performance Analysis and Optimization

This section presents the performance analysis of the proposed system, focusing on the secrecy successful computation probability. Additionally, we formulate an optimization problem and propose a solution to solve it.

3.1. Secrecy Successful Computation Probability

The secrecy successful computation probability (SSCP), denoted as Υ_{ss}, is defined as the probability that its subtasks execution are completed within allocated sub-time slot τ and the corresponding instantaneous secrecy capacity is greater than the required offloading data rate R^{th}. In addition, it is noted that the harvested energy must be sufficient for local execution and encryption. Therefore, in the context of this proposed system, the secrecy successful computation probability of each pair can be written as

$$\Upsilon_{ss}^{(k)} \triangleq \Pr\left(\tau_k < \tau, C_{ik}^s > R_{ik}^{th}, P_{ik}^H \tau > E_{ik}^c\right), \quad (23)$$

where $R_{ik}^{th} = \frac{(1-\beta_{ik})L_{ik}}{\tau}$, $i \in \{1, 2\}$.

For K pairs of users of this system, the SSCP Υ_{ss} is obtained as follows:

$$\Upsilon_{ss} \triangleq \prod_{k=1}^{K} \Upsilon_{ss}^{(k)}. \tag{24}$$

Notably, according to (20), if $\tau_{1k}^{D} > \tau$ or $\tau_{2k}^{D} > \tau$, $\forall k \in \{1, ..., K\}$, then $\Upsilon_{ss}^{(k)} = 0$. In this case, the IoDs have not enough resource to execute locally. Here after, we consider the scenarios that the condition of $\tau_{1k}^{D} < \tau$ and $\tau_{2k}^{D} < \tau$ is satisfied. Thus, the equation (21) can be rewritten as

$$\Upsilon_{ss}^{(k)} \triangleq \Pr\left(\tau_{k}^{U} < \tau, C_{ik}^{s} > R_{ik}^{th}, P_{ik}^{H}\tau > E_{ik}^{c}\right). \tag{25}$$

To evaluate the secrecy and latency performance of this proposed system, we derive the following **Theorem 1** as follows:

Theorem 1. In this proposed multi-user UAV-assisted mobile edge computing IoT system, the approximation expression of the secrecy successful computation probability is obtained as follows:

$$\begin{aligned}\Upsilon_{ss} = {} & \frac{\pi^2}{2PQ}\sum_{p=1}^{P}\sum_{q=1}^{Q}\frac{\Lambda_2\left(-y_q \ln u_p\right)^{m_U-1}}{(m_U-1)!^2}\left(\frac{m_U}{\lambda_U}\right)^{2m_U} \\ & \times e^{\frac{m_U \ln u_p}{\lambda_U} - \frac{m_U}{\lambda_U}y_q}\sqrt{\frac{(1-\omega_p)(1-\omega_q^2)}{1+\omega_p}}\Bigg\{1 - e^{-\frac{\mu_{2k}y_q}{\mu_{2kE}B_{2k}}} \\ & - \frac{e^{\frac{\mu_{1k}\ln u_p}{\mu_{1kE}B_{1k}\left(\mu_{2k}y_q^2+1\right)}}}{\Xi}\left[e^{\Xi\frac{\mu_{2k}y_q}{\mu_{2kE}B_{2k}}} - 1\right]\Bigg\},\end{aligned} \tag{26}$$

where $A_k = \tau - \frac{(\kappa_U + \psi_m^*)\sum_{i=1}^{2}(1-\beta_{ik})L_{ik}}{f_U}$, $B_{ik} = 2^{\frac{R_{ik}^{th}}{B}}$, $C_{ik} = \frac{\Delta_{ik}}{\delta_{ik}}$, $\Delta_{ik} = \nu - \frac{1}{\omega}\ln\left(\frac{P_m\tau}{E_{ik}^{c}(1-\Omega)+P_m\tau\Omega} - 1\right)$, $\mathcal{A}_{ik} = 2^{\frac{(1-\beta_{ik})L_{ik}}{BA_k}} - 1$, $i \in \{1, 2\}$, $\mathcal{B}_{1k} = \max\{C_{2k}, \sqrt{\frac{\mathcal{A}_{2k}}{\mu_{2k}}}\}$, $\mathcal{B}_{2k} = \max\left\{C_{1k}, \sqrt{\frac{\mathcal{A}_{1k}\left(\mu_{2kE}\mathcal{B}_{1k}^2+1\right)}{\mu_{1k}}}\right\}$, $\Lambda_1 = e^{-\mathcal{B}_{2k}}$, $\Lambda_2 = \sqrt{\frac{\mu_{1k}(-\ln u_j)^2 - \mathcal{A}_{1k}}{\mu_{2k}\mathcal{A}_{1k}}} - \mathcal{B}_{1k}$, $\Lambda_3 = \frac{\mu_{2k}y_p}{\mu_{2kE}B_{2k}}$, $\Xi = \frac{\mu_{1k}\mu_{2kE}y_q\ln u_p}{\mu_{1kE}B_{1k}\left(\mu_{2k}y_q^2+1\right)} - 1$, $u_p = \frac{(\omega_p+1)\Lambda_1}{2}$, $y_q = \frac{(\omega_q+1)\Lambda_2}{2} + \mathcal{B}_{1k}$, $\omega_n = \cos\left(\frac{2n-1}{2N}\pi\right)$, $n \in \{p, q\}$, $N \in \{P, Q\}$ is the complexity-vs-accuracy trade-off coefficient.

Proof. See in Appendix A. □

3.2. Optimization: Problem formulation and solution

We are interested in the design optimization problem to jointly optimize the SSCP for the multi-user UAV-assisted mobile edge computing IoT system as follows:

$$(\mathbf{P_1}): \max_{z_U, \beta_{ik}, \xi_{ik}} \left(\Upsilon_{ss}\right) \tag{27a}$$

$$\text{s.t.:} \quad z_{\min} \le z_U \le z_{\max} \tag{27b}$$

$$0 \le \beta_{ik} \le 1 \tag{27c}$$

$$0 \le \xi_{ik} \le 1 \tag{27d}$$

$$\phi_{ik} \le \phi_{th} \tag{27e}$$

where $\forall k \in \{1, ..., K\}$, $i \in \{1, 2\}$, $(\mathbf{P_1})$ belongs to the class of single objective optimization problems, specifically, maximizing SSCP. The constraints of (27b), (27c), and (27d) in the optimization problem describe the optimal parameter set of the system, including the altitude of the UAV, the backscattering reflection coefficient, and the task dividing ratio. Additionally, constraint (27e) is used to describe the security cost limit, which is suitable for the IoT-MEC architecture-based model.

As shown in [28], the Immune algorithm (IA) has stronger local search capabilities than the Genetic algorithm (GA), effectively preventing population degradation. To solve the (P1) problem, we propose the advanced immune algorithm, namely AIA, described in as **Algorithm 1**.

Specifically, AIA begins with the initialization phase, randomly generating an initial population of $\mathcal{N}$ potential solutions (antibodies). Each antibody represents a system parameter vector defined as $\mathcal{P} = (z_U, \beta_{ik}, \xi_{ik})$. During this phase, the main parameters of the optimization algorithm, including clone number $(\mathcal{C})$, mutation rate (ω_m), suppression rate (ω_s), number of generations$(\mathcal{I})$, and the search range, are predefined. Thereafter, in the main loop, the SSCP objective function is used to evaluate the quality of each antibody in terms of affinity $(\mathcal{A})$ according to the formula:

$$\mathcal{A} = \frac{1}{1 + \Upsilon_{ss}(\mathcal{P})}. \tag{28}$$

Next, AIA employs a roulette wheel strategy to probabilistically select the best antibody for cloning, ensuring its likelihood is proportional to its affinity. According to the formula, the Gaussian mutation is then utilized to randomly alter the antibodies' components randomly, thereby fostering population diversity.

$$\mathcal{P}_m = \mathcal{P} + m_G, \tag{29}$$

where $m_G \sim \mathcal{CN}(0, \sigma^2)$.

The suppression process is further applied to the post-mutation population, which plays a pivotal role in maintaining antibody population diversity and preventing premature convergence. By reducing the affinity of similar antibodies, this process counteracts the over-dominance of high-fitness antibodies and encourages the emergence of diverse antibodies, thereby

expanding the search space and increasing the likelihood of finding a globally optimal solution. The formula describing the suppression of an individual i when its similarity with individual j exceeds a threshold is given by

$$\mathcal{A}_i = \mathcal{A}_i - \omega_s . S(\mathcal{P}_i, \mathcal{P}_j), \tag{30}$$

where $S(\mathcal{P}_i, \mathcal{P}_j)$ is the similarity ratio, $S(\mathcal{P}_i, \mathcal{P}_j) = \frac{\mathcal{P}_i \cdot \mathcal{P}_j}{(\|\mathcal{P}_i\| \|\mathcal{P}_j\|)}$, the operator $'.'$ denote the scalar product, and $\|u\|$ is the norm of vector u.

Finally, after $\mathcal{I}$ iterations, AIA returns the best solution found, which is the optimal parameter set for the system $(z_U^*, \beta_{ik}^*, \xi_{ik}^*)$. Another note is that we use a security cost constraint to ensure that the allowable security level of the data encryption algorithm does not exceed a given threshold.

Algorithm 1 The maximal secrecy successful computation probability based on Advanced Immune Algorithm (AIA)

procedure AIA(Υ_{ss})
  Input: $\Upsilon_{ss}, \mathcal{N}, \mathcal{C}, \omega_m, \omega_s, \mathcal{I}$
  Output: Optimization set $(z_U^*, \beta_{ik}^*, \xi_{ik}^*)$
Initialization:
  Initialize antibodies $\mathcal{P}$
Main Loop:
  Evaluate affinity $\mathcal{A}$ for each antibody using (28).
  Select the best antibodies using roulette wheel strategy.
  Clone the best antibodies.
  Mutate each clone using (29).
  Suppress each antibodies using (30).
Output the Final Optimized Solution:
  Return $z_U^*, \beta_{ik}^*, \xi_{ik}^*\}$
end procedure

4. Numerical Results and Discussion

This section presents the Monte Carlo simulation results for secrecy successful computation probability, Υ_{ss}, as a function of key parameters, including the number of IoT devices, UAV altitude, transmit power, backscatter reflection coefficient, task length, and task dividing ratio.

4.1. System Setting

Similar to the work of [29], we provide the typical values of simulation parameters utilized in our work as Table 1. Specifically, for the nonlinear EH model, we set $a_k = 150$, $b_k = 0.014$ and $P_m = 0.024$ W [30]. The location of $\mathbf{U}$ is set as $(0,\ 0,\ z_U)$, the locations of 4 IoT devices are set as $([1, 2, 3, 4], [2, 2, 2, 2],\ 0)$. The distances between $\mathbf{U}$ and D_k, $k \in \{1, 2, 3, 4\}$, are calculated by

$$d_{Uk} \triangleq \sqrt{(x_U - x_k)^2 + (y_U - y_k)^2 + {z_U}^2} = \sqrt{r_k^2 + z_U^2}. \tag{31}$$

To keep things simple, all IoT devices are assumed to have identical energy conversion efficiency, backscattering reflection coefficient, task length, task division ratio, and computing resources. Simulations are conducted by 10^6 samples.

4.2. Simulation Results

Fig. 2 illustrates the impact of UAV altitude (z_U) and the number of IoT devices (K) on the Secrecy Successful Computation Probability (SSCP). The results show that SSCP follows a typical "rise–peak–fall" trend as the UAV altitude increases, confirming the existence of an optimal altitude that maximizes secure offloading performance. In addition, SSCP tends to decrease as the number of IoT devices K increases, due to increased competition for transmission resources and reduced time allocation per user pair.

The optimal altitude is influenced by multiple interrelated factors. At very low altitudes, SSCP is degraded due to severe multipath fading and signal blockage from surrounding ground-level obstacles. As the UAV ascends, line-of-sight (LoS) conditions improve, enhancing both wireless energy transfer and communication reliability. However, when the UAV altitude becomes too high, the increased path loss outweighs the benefits of improved LoS, resulting in weaker received signals and degraded SSCP.

Another key factor is the UAV transmit power. When the UAV operates at a higher transmit power, the emitted signal remains sufficiently strong even over longer distances. This helps to compensate for the increased path loss at higher altitudes, thereby maintaining a strong backscattered signal received from the IoT devices.

Moreover, since the system adopts backscatter communication, where IoT devices passively reflect the UAV's incident signal, the secrecy performance is also closely related to the strength of backscattered signals and the spatial position of potential eavesdroppers. Specifically, a lower UAV altitude improves energy harvesting at the IoT devices and leads to stronger backscattered signals, which, in turn, may increase the risk of interception if an eavesdropper is located nearby.

Furthermore, when the number of IoT devices increases, the fixed total transmission time must be divided among more user pairs, resulting in significantly shorter time slots allocated to each pair. This leads to a considerable reduction in the effective transmission rate per pair, which directly decreases the SSCP. Additionally, the MEC server experiences higher computational load, and the per-user bandwidth

Table 2. Simulation Parameters

Parameters	Notation	Typical Values
Nakagami-m severity factor	m_1, m_2	2, 2
Average transmit SNR	γ_U	0 - 40 dB
Number of IoT devices	K	2, 4, 6
Energy conversion efficiency	η	0.75
Backscattering reflection coefficient	ξ_{ik}	0.1, 0.5, 0.9
Task dividing ratio	β_{ik}	0-1
Carrier frequency	f_c	1 MHz
Speed of light	c	3×10^8 m/s
Path-loss exponent	α	2
Excessive path loss coefficients	Ψ_{LoS}, Ψ_{NLoS}	1, 20
Constant parameters of environment	a, b	9.6177, 0.1581
Constant values of EH circuit	a_k, b_k	150, 0.014
Maximum output DC power	P_m	0.024W
The CPU-cycle frequency of MEC server	f	1 GHz
The number of CPU cycles for computing each bit	κ	2
Channel bandwidth	W	0.1, 1, 10 MHz
Task length	L_{ik}	0 - 20 kb
Threshold of latency	T	0.4, 0.7, 1s
Number of cryptography algorithm	M	6
The CPU cycles required for encrypting and decrypting one bit	ψ_m, ψ_m^*	20, 80
Maximal security breach cost	ϕ_{ik}	5K $
Security risk coefficient	v	1
Expected protection level	q_m	5

also decreases, further contributing to performance degradation.

As shown in the figure 2, the SSCP reaches its peak in the altitude range of approximately 8–10 meters, depending on the number of IoT devices. This range represents a balance point where LoS conditions are favorable, energy harvesting remains efficient, and the risk of passive eavesdropping is mitigated. These results highlight the importance of altitude-aware UAV positioning in secure and energy-constrained IoT environments.

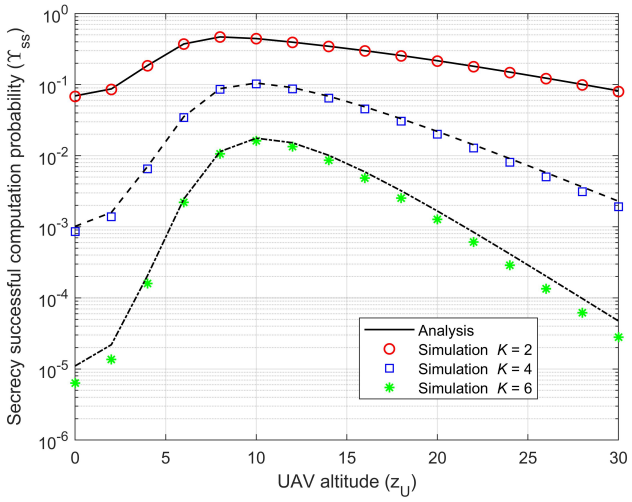

Figure 2. SSCP vs. UAV altitude with different values of user number

In Fig. 3, we investigate the system performance as a function of the average transmit SNR (γ_U) of UAV user U, under varying bandwidth (W) conditions. A distinct upward trend is observed, where system performance significantly improves with increasing γ_U across all three bandwidth scenarios. This demonstrates a positive correlation between signal strength and system operational efficiency. Enhanced transmit power leads to improved data decoding capabilities at the receiver, consequently minimizing errors and boosting transmission rates. This performance enhancement is attributed to the increased resilience of a stronger signal against noise and propagation losses in the transmission environment, thus enhancing connection quality. Notably, that the SSCP tends to saturate beyond a γ_U threshold of 25 dB, suggesting that further increments in SNR yield diminishing returns. Additionally, a clear enhancement in performance is evident with increased bandwidth. The improvement is particularly pronounced when transitioning from 0.1 MHz to 1 MHz. However, the gains in performance when increasing bandwidth from 1 MHz to 10 MHz are more significant at lower γ_U values, converging towards similar saturation levels at higher γ_U. These numerical results emphasize the critical role of optimizing transmit SNR and operational bandwidth in designing and deploying efficient IoT systems.

In Fig. 4, we examine the system performance based on variations in task length (L_{ik}) and block time (T). The results demonstrate a clear trend of declining system performance as task length increases. This increase in task length corresponds to a proportional rise in the

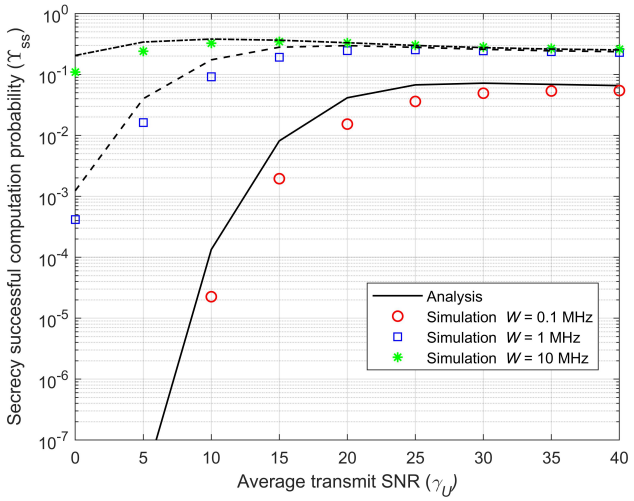

Figure 3. SSCP vs. average transmit SNR with different values of bandwidth

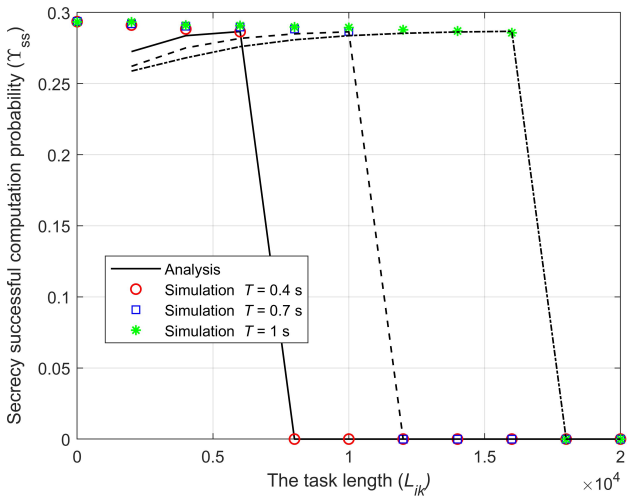

Figure 4. SSCP vs. task length with different values of block time

workload that needs to be processed, encompassing both local computation and offloading. Once L_{ik} surpasses a critical threshold, the system enters an outage statestate due to overload, making it unable to meet the required demands. This phenomenon is entirely consistent with the system's offloading model, where an extensive workload places a substantial burden on meeting processing time constraints. Conversely, as block time extends, a notable improvement in system performance is observed. This can be attributed to the fact that a longer block time allows the system more time to process and allocate resources efficiently, thereby mitigating overload conditions and enhancing task completion rates. Increasing the block time gives the system additional budget, enabling optimized processing and reducing the outages. However, excessively increasing the block time may lead to increased latency, which could impact real-time applications.

In Fig. 5, we investigate the system performance as a function of the task dividing ratio (β_{ik}) and the backscattering reflection coefficient (ξ_{ik}). The simulation results show that when β_{ik} has low values, specifically $\beta_{ik} \leq 0.4$ in this simulation, the system ceases to function. Beyond this threshold, a significant improvement in system performance is observed. This indicates that an inappropriate task division leads to an imbalance in local computation and offloading workloads, thereby hindering the intended system functionality. Furthermore, Fig. 5 explores the impact of three distinct ξ_{ik} levels, representing the signal reflection capability of IoT devices utilizing BC technology. A decrease in this coefficient is associated with improved system performance.

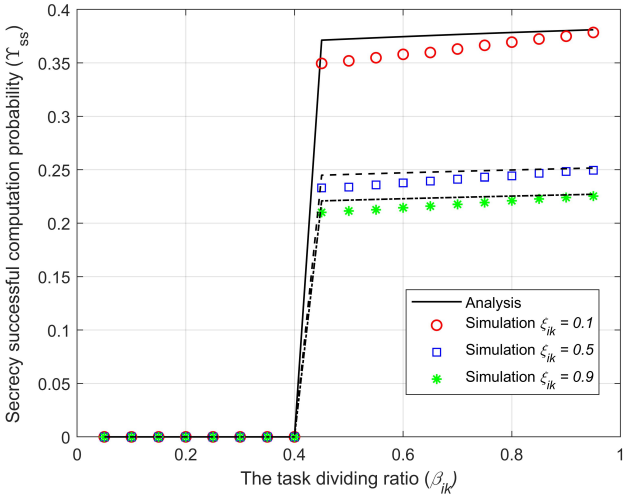

Figure 5. SSCP vs. task dividing ratio with different values of backscattering reflection coefficient

4.3. Optimization Results

In this section, we examine the convergence of the AIA optimization algorithm under various transmission power levels. We configure the algorithm with the following initialization parameters: a population size of 100, a clone number of 20, a mutation rate of 0.01, and a suppression coefficient of 0.3. Across all three simulation results, with γ_U equals 10, 15, and 20 dB, the results demonstrate that the algorithm converges well within 100 iterations. It indicates that AIA is highly effective, as it can find near-optimal solutions quickly. Furthermore, fewer iterations imply lower computational resource consumption, which benefits

resource-constrained devices like those in the proposed IoT MEC environment.

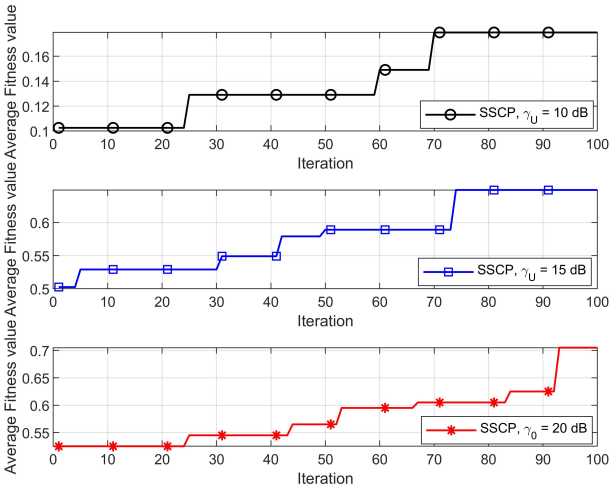

Figure 6. AIA convergence with different power levels

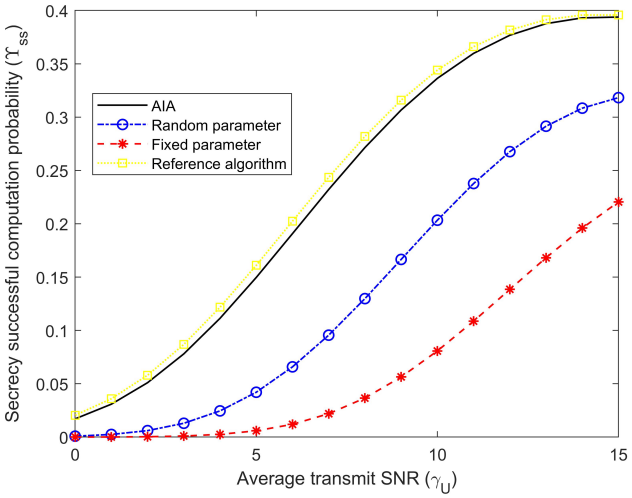

Figure 7. Comparation of AIA performance with a benchmark optimization algorithm and without optimization scenario

After employing AIA, we obtained the optimal parameter set $\{z_U^*, \beta_{ik}^*, \xi_{ik}^*\}$ and applied it for performance comparison. Accordingly, we investigated the effectiveness of the optimization algorithm in the following scenarios: (i) Using the proposed optimization algorithm, (ii) Using an exhaustive search algorithm with a precision of 0.001 as a benchmark, (iii) Using random parameters, and (iv) Using fixed parameters. For the random parameter set, we randomly initialized 1000 solutions and selected the best set for comparison. The results show that AIA delivers performance comparable to the exhaustive search algorithm, providing encouraging evidence of its ability to find near-optimal solutions. Notably, AIA has a significantly lower computational cost than exhaustive search, offering a considerable advantage in applicability to the proposed model. Another observation is that AIA significantly improves system performance compared to scenarios without optimization, i.e., (iii) and (iv). Therefore, the application of AIA is of great significance in realizing future IoT MEC-based applications.

The secrecy capacity expressions in the theoretical analysis are approximated under the assumption of very low noise power at each receiver. This assumption simplifies the formulation and makes the theoretical derivation tractable with lower computational complexity. However, it may introduce additional deviations when compared to practical simulation settings, thereby contributing to the slight gaps observed between the theoretical and simulation curves.

In addition, the theoretical expression of SSCP is derived using approximation techniques, and still exhibits a slight deviation compared to Monte Carlo simulation results. This is primarily due to the use of the Gaussian-Chebyshev quadrature method, which is a widely adopted approach for approximating multi-dimensional integrals in wireless communication analysis. While this method enables closed-form evaluation and significantly reduces computational complexity, it inherently introduces approximation error, particularly when capturing higher-order statistical behaviors of random channels.

Nevertheless, the theoretical results remain sufficiently accurate for performance evaluation and offer valuable analytical insights for system design and optimization.

5. Conclusion

In conclusion, this paper has addressed the critical challenge of perception layer security within a UAV-enabled MEC system for a BC IoT network, emphasizing safeguarding data integrity and reliability. Accordingly, we integrated PLS, TDMA, NOMA, and BC techniques to construct a system protocol to enhance system secrecy against moving passive eavesdropping. A approximation expression for the SSCP was derived, encapsulating the complex interplay of harvested energy, computational latency, and encryption costs. Leveraging an Advanced Immune algorithm, we optimized the system parameters, including UAV altitude, backscattering reflection coefficient, and task dividing ratio to maximize SSCP. Through comprehensive numerical simulations, we validated the accuracy of our analytical framework and demonstrated the significant impact of key parameters on secrecy and latency performance. This work provides valuable insights into designing and optimizing secure and efficient UAV-assisted IoT systems, paving the way for future research into more robust and resilient PLS mechanisms in dynamic MEC environments.

In our future work, we will investigate an extended system model to incorporate multi-user, multi-antenna, and emerging technologies while optimizing algorithms and enhancing security analysis to address the challenges in complex IoT environments.

Proof of Theorem 1

Substituting (18), (16) and (21) into (25), the equation (23) can be rewritten as (A-1),

$$\begin{aligned}\Upsilon_{ss}^{(k)} &= \Pr\left\{t_{1k}^{o} < A_k, t_{2k}^{o} < A_k, \frac{1+\gamma_{1k}}{1+\gamma_{1kE}} > B_{1k}, \frac{1+\gamma_{2k}}{1+\gamma_{2kE}} > B_{2k}, X_{1k} > C_{1k}, X_{2k} > C_{2k}\right\} \\ &\approx \Pr\left\{\gamma_{1k} > \mathcal{A}_{1k}, \gamma_{2k} > \mathcal{A}_{2k}, \frac{\gamma_{1k}}{\gamma_{1kE}} > B_{1k}, \frac{\gamma_{2k}}{\gamma_{2kE}} > B_{2k}, X_{1k} > C_{1k}, X_{2k} > C_{2k}\right\}.\end{aligned} \tag{A-1}$$

where $A_k = \tau - \frac{(\kappa_U+\psi_m^*)\sum_{i=1}^{2}(1-\beta_{ik})L_{ik}}{f_U}$, $B_{ik} = 2^{\frac{R_{ik}^{th}}{B}}$, $C_{ik} = \frac{\Delta_{ik}}{\delta_{ik}}$, $\Delta_{ik} = \nu - \frac{1}{\omega}\ln\left(\frac{P_m\tau}{E_{ik}^{c}(1-\Omega)+P_m\tau\Omega} - 1\right)$, $\mathcal{A}_{ik} = 2^{\frac{(1-\beta_{ik})L_{ik}}{BA_k}} - 1$, $i \in \{1,2\}$.

Then, substituting (8), (9), (11), and (12) into (A-1), we can obtain as (A-2), where $\mathcal{B}_{1k} = \max\{C_{2k}, \sqrt{\frac{\mathcal{A}_{2k}}{\mu_{2k}}}\}$, $\mathcal{B}_{2k} = \max\left\{C_{1k}, \sqrt{\frac{\mathcal{A}_{1k}\left(\mu_{2kE}\mathcal{B}_{1k}^2+1\right)}{\mu_{1k}}}\right\}$, $\Lambda_3 = \frac{\mu_{2k}y}{\mu_{2kE}B_{2k}}$.

$$\begin{aligned}\Upsilon_{ss}^{(k)} &= \Pr\left\{X_{1k} > C_{1k}, X_{2k} > C_{2k}, \frac{\mu_{1k}X_{1k}^2}{\mu_{2k}X_{2k}^2+1} > \mathcal{A}_{1k}, \mu_{2k}X_{2k}^2 > \mathcal{A}_{2k}, \frac{\mu_{1k}X_{1k}}{\mu_{2k}X_{2k}^2+1} > \frac{\mu_{1kE}B_{1k}Z_{1k}}{\mu_{2kE}X_{2k}Z_{2k}+1},\right. \\ &\qquad \left.\mu_{2k}X_{2k} > \mu_{2kE}B_{2k}Z_{2k}\right\} \\ &= \Pr\left\{X_{1k} > \mathcal{B}_{2k}, \mathcal{B}_{1k} < X_{2k} < \sqrt{\frac{\mu_{1k}X_{1k}^2 - \mathcal{A}_{1k}}{\mu_{2k}\mathcal{A}_{1k}}}, Z_{1k} < \frac{\mu_{1k}X_{1k}\left(\mu_{2kE}X_{2k}Z_{2k}+1\right)}{\mu_{1kE}B_{1k}\left(\mu_{2k}X_{2k}^2+1\right)}, Z_{2k} < \frac{\mu_{2k}X_{2k}}{\mu_{2kE}B_{2k}}\right\} \\ &= \int_{\mathcal{B}_{2k}}^{\infty}\int_{\mathcal{B}_{1k}}^{\sqrt{\frac{\mu_{1k}x^2-\mathcal{A}_{1k}}{\mu_{2k}\mathcal{A}_{1k}}}}\int_{0}^{\frac{\mu_{2k}y}{\mu_{2kE}B_{2k}}} f_{X_{1k}}(x)f_{X_{2k}}(y)f_{Z_{2k}}(z)F_{Z_{1k}}\left[\frac{\mu_{1k}x\left(\mu_{2kE}yz+1\right)}{\mu_{1kE}B_{1k}\left(\mu_{2k}y^2+1\right)}\right]dxdydz \\ &= \int_{0}^{\Lambda_1}\frac{f_{X_{1k}}(-\ln u)}{u}\int_{\mathcal{B}_{1k}}^{\sqrt{\frac{\mu_{1k}(\ln u)^2-\mathcal{A}_{1k}}{\mu_{2k}\mathcal{A}_{1k}}}} f_{X_{2k}}(y)\underbrace{\int_{0}^{\Lambda_3} F_{Z_{1k}}\left[\frac{\mu_{1k}(-\ln u)\left(\mu_{2kE}yz+1\right)}{\mu_{1kE}B_{1k}\left(\mu_{2k}y^2+1\right)}\right]f_{Z_{2k}}(z)dz}_{I}dydu.\end{aligned} \tag{A-2}$$

By the help of (5) and (6), the integral I can be calculated as (A-3).

$$\begin{aligned}I &= F_{Z_{2k}}\left(\frac{\mu_{2k}y}{\mu_{2kE}B_{2k}}\right) - \int_{0}^{\Lambda_3} e^{-\frac{\mu_{1k}(-\ln u)\left(\mu_{2kE}yz+1\right)}{\mu_{1kE}B_{1k}\left(\mu_{2k}y^2+1\right)}-z}dz \\ &= 1 - e^{-\frac{\mu_{2k}y}{\mu_{2kE}B_{2k}}} - \frac{\mu_{1kE}B_{1k}\left(\mu_{2k}y^2+1\right)e^{\frac{\mu_{1k}\ln u}{\mu_{1kE}B_{1k}\left(\mu_{2k}y^2+1\right)}}}{\mu_{1k}\mu_{2kE}y\ln u - \mu_{1kE}B_{1k}\left(\mu_{2k}y^2+1\right)}\left[e^{\left(\frac{\mu_{1k}\mu_{2kE}y\ln u}{\mu_{1kE}B_{1k}\left(\mu_{2k}y^2+1\right)}-1\right)\Lambda_3} - 1\right].\end{aligned} \tag{A-3}$$

Substituting the result of (A-3) into (A-2), we can have the equation (A-4),

$$\begin{aligned}\Upsilon_{ss}^{(k)} \overset{(*)}{=} &\frac{\pi^2}{2PQ}\sum_{p=1}^{P}\sum_{q=1}^{Q}\frac{\Lambda_2}{(m_U-1)!^2}\left(\frac{m_U}{\lambda_U}\right)^{2m_U}(-y_q\ln u_p)^{m_U-1}e^{\frac{m_U\ln u_p}{\lambda_U}-\frac{m_U}{\lambda_U}y_q}\sqrt{\frac{(1-\omega_p)(1-\omega_q^2)}{1+\omega_p}} \\ &\left\{1 - e^{-\frac{\mu_{2k}y_q}{\mu_{2kE}B_{2k}}} - \frac{\mu_{1kE}B_{1k}\left(\mu_{2k}y_q^2+1\right)e^{\frac{\mu_{1k}\ln u_p}{\mu_{1kE}B_{1k}\left(\mu_{2k}y_q^2+1\right)}}}{\mu_{1k}\mu_{2kE}y_q\ln u_p - \mu_{1kE}B_{1k}\left(\mu_{2k}y_q^2+1\right)}\left[e^{\left(\frac{\mu_{1k}\mu_{2kE}y_q\ln u_p}{\mu_{1kE}B_{1k}\left(\mu_{2k}y_q^2+1\right)}-1\right)\frac{\mu_{2k}y_q}{\mu_{2kE}B_{2k}}} - 1\right]\right\}.\end{aligned} \tag{A-4}$$

where $\Lambda_1 = e^{-\mathcal{B}_{2k}}$, $\Lambda_2 = \sqrt{\frac{\mu_{1k}(-\ln u_p)^2-\mathcal{A}_{1k}}{\mu_{2k}\mathcal{A}_{1k}}} - \mathcal{B}_{1k}$, $\Lambda_3 = \frac{\mu_{2k}y_q}{\mu_{2kE}B_{2k}}$, $u_p = \frac{(\omega_p+1)\Lambda_1}{2}$, $y_q = \frac{(\omega_q+1)\Lambda_2}{2} + \mathcal{B}_{1k}$. Notably, the Step (*) is held by employing the Gaussian-Chebyshev quadrature method, we obtain the final result as (26), and the proof ends.

References

[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[2] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on multi-access edge computing for internet of things realization," *IEEE Communications Surveys and Tutorials*, vol. 20, no. 4, pp. 2961–2991, 2018.

[3] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Communications Survey Tutorials*, vol. 19, no. 4, pp. 2322–2358, 2017.

[4] M. Abrar, U. Ajmal, Z. M. Almohaimeed, X. Gui, R. Akram, and R. Masroor, "Energy efficient UAV-enabled mobile edge computing for IoT devices: A review," *IEEE Access*, vol. 9, pp. 127 779–127 798, 2021.

[5] A.-N. Nguyen, D.-B. Ha, V.-T. Truong, D.-T. Do, and C. So-In, "Secrecy performance analysis and optimization for UAV-relay-enabled WPT and cooperative NOMA MEC in IoT networks," *IEEE Access*, vol. 11, pp. 127 800–127 816, 2022.

[6] Q. Liu, S. Sun, X. Yuan, and Y. Zhang, "Ambient backscatter communication-based smart 5G IoT network," *EURASIP Journal on Wireless Communications and Networking*, vol. 2021, no. 1, pp. 1–19, 2021.

[7] S. H. H. Raza, D. Zorbas, and B. O'Flynn, "A comprehensive survey on RF energy harvesting: Applications and performance determinants," *Sensors*, vol. 22, no. 8, p. 2990, 2022.

[8] J. Du, W. Liu, G. Lu, J. Jiang, D. Zhai, F. R. Yu, and Z. Ding, "When mobile-edge computing (MEC) meets nonorthogonal multiple access (NOMA) for the internet of things (IoT): System design and optimization," *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 7849–7862, 2021.

[9] V. T. Truong, D. B. Ha, T. T. Vu, and H. A. Nguyen, "STAR-RIS aided mobile edge computing networks with uplink NOMA scheme," in *2023 International Conference on Advanced Technologies for Communications (ATC)*, Da Nang, Vietnam, 2023.

[10] F. Jameel, S. Zeb, W. U. Khan, S. A. Hassan, Z. Chang, and J. Liu, "NOMA-enabled backscatter communications: Toward battery-free IoT networks," *IEEE Internet of Things Magazine*, vol. 3, no. 4, pp. 95–101, 2020.

[11] E. T. Michailidis, K. Maliatsos, D. N. Skoutas, D. Vouyioukas, and C. Skianis, "Secure UAV-aided mobile edge computing for IoT: A review," *IEEE Access*, vol. 10, pp. 86 353–86 383, 2022.

[12] K. Aarika, M. Bouhlal, R. A. Abdelouahid, S. Elfilali, and E. Benlahmar, "Perception layer security in the internet of things," *Procedia Computer Science*, vol. 175, pp. 591–596, 2020, the 17th International Conference on Mobile Systems and Pervasive Computing (MobiSPC), The 15th International Conference on Future Networks and Communications (FNC), The 10th International Conference on Sustainable Energy Information Technology. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050920317853

[13] M. Bloch, O. Gunlu, A. Yener, F. Oggier, H. V. Poor, L. Sankar, and R. F. Schaefer, "An overview of information-theoretic security and privacy: Metrics, limits and applications," *IEEE Journal on Selected Areas in Information Theory*, vol. 2, no. 1, pp. 5–22, 2021.

[14] H. Wang, J. Jiang, G. Huang, W. Wang, D. Deng, B. M. Elhalawany, and X. Li, "Physical layer security of two-way ambient backscatter communication systems," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, p. 5445676, 2022. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1155/2022/5445676

[15] X. Li, Q. Wang, M. Zeng, Y. Liu, S. Dang, T. A. Tsiftsis, and O. A. Dobre, "Physical-layer authentication for ambient backscatter-aided NOMA symbiotic systems," *IEEE Transactions on Communications*, vol. 71, no. 4, pp. 2288–2303, 2023.

[16] S. Han, J. Wang, L. Xiao, and C. Li, "Broadcast secrecy rate maximization in UAV-empowered IRS backscatter communications," *IEEE Transactions on Wireless Communications*, vol. 22, no. 10, pp. 6445–6458, 2023.

[17] T. Van Truong, D.-B. Ha, and M.-T. Vo, *Industrial Networks and Intelligent Systems*. Springer Nature Switzerland, 2023, ch. A Secrecy Offloading in Radio Frequency Energy Harvesting NOMA Heterogeneous Mobile Edge Computing Network, pp. 275–286.

[18] G. Su, M. Dai, B. Chen, and X. Lin, "Deep reinforcement learning aided secure UAV communications in the presence of moving eavesdroppers," *Journal of King Saud University - Computer and Information Sciences*, vol. 36, no. 4, p. 102047, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1319157824001368

[19] T. Zhou, Y. Fu, D. Qin, X. Nie, N. Jiang, and C. Li, "Secure and multistep computation offloading and resource allocation in ultradense multitask NOMA-enabled IoT networks," *IEEE Internet of Things Journal*, vol. 11, no. 3, pp. 5347–5361, 2024.

[20] G. K. Pandey, D. S. Gurjar, S. Yadav, and S. Solanki, "UAV-empowered IoT network with hardware impairments and shadowing," *IEEE Sensors Letters*, vol. 7, no. 7, pp. 1–4, 2023.

[21] V.-T. Truong and D.-B. Ha, "A novel secrecy offloading in noma heterogeneous mobile edge computing network," in *International Conference on Advanced Engineering Theory and Applications*. Springer, 2022, pp. 733–743.

[22] M. Rana, Q. Mamun, and R. Islam, "Lightweight cryptography in iot networks: A survey," *Future Generation Computer Systems*, vol. 129, pp. 77–89, 2022.

[23] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, "Advanced lightweight encryption algorithms for iot devices: survey, challenges and solutions," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–18, 2024.

[24] D. D. Tran, H. V. Tran, D. B. Ha, and G. Kaddoum, "Secure transmit antenna selection protocol for MIMO NOMA networks over Nakagami-m channels," *IEEE Systems Journal*, vol. 14, no. 1, pp. 253–264, 2020.

[25] E. Boshkovska, D. W. K. Ng, N. Zlatanov, and R. Schober, "Practical non-linear energy harvesting model and resource allocation for SWIPT systems," *IEEE Communications Letters*, vol. 19, no. 12, pp. 2082–2085, 2015.

[26] S. Gong, Y. Xie, J. Xu, D. Niyato, and Y. C. Liang, "Deep reinforcement learning for backscatter-aided data offloading in mobile edge computing," *IEEE Network*, vol. 34, no. 5, pp. 106–113, 10 2020.

[27] G. Su, M. Dai, B. Chen, and X. Lin, "Deep reinforcement learning aided secure uav communications in the presence of moving eavesdroppers," *Journal of King Saud University-Computer and Information Sciences*, vol. 36, no. 4, p. 102047, 2024.

[28] M. Abdolshah, "A review of resource-constrained project scheduling problems (RCPSP) approaches and solutions," *International Transaction Journal of Engineering, Management, Applied Sciences and Technologies*, vol. 5, no. 4, pp. 253–286, 2014.

[29] Y. Li, D. V. Huynh, V.-L. Nguyen, D.-B. Ha, H.-J. Zepernick, and T. Q. Duong, "Multiagent UAV-aided URLLC mobile edge computing systems: A joint communication and computation optimization approach," *IEEE Systems Journal*, pp. 1–11, 2024.

[30] Y. Lu, K. Xiong, P. Fan, Z. Ding, Z. Zhong, and K. B. Letaief, "Global energy efficiency in secure MISO SWIPT systems with non-linear power-splitting EH model," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 1, pp. 216–232, 2019.