Cluster Head Selection Algorithm for UAV Assisted Clustered IoT Network Utilizing Blockchain

LIN Xinhua, ZHANG Jing, LI Qiang

(Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract: To guarantee the security of Internet of Things (IoT) devices, the blockchain technology is often applied to clustered IoT networks. However, cluster heads (CHs) need to undertake additional control tasks. For battery-powered IoT devices, the conventional CH selection algorithm is limited. Based on the above problem, an unmanned aerial vehicle (UAV) network assisted clustered IoT system is proposed, and a corresponding UAV CH selection algorithm is designed. In this scheme, UAVs are selected as CHs to serve IoT clusters. The proposed CH selection algorithm considers the maximal transmit power, residual energy and distance information of UAVs, which can greatly extend the working life of IoT clusters. Through Monte Carlo simulation, the key performance indexes of the system, including energy consumption, average secrecy rate and the maximal number of data packets received by the base station (BS), are evaluated. The simulation results show that the proposed algorithm has great advantages compared with the existing CH selection algorithms.

Keywords: cluster head selection; unmanned aerial vehicle; blockchain; IoT; average secrecy rate

DOI: 10.12142/ZTECOM.202101005

https://kns.cnki.net/kcms/detail/34.1294.TN.20210223.1206.002.html, published online February 20, 2021

Manuscript received: 2020-12-10

Citation (IEEE Format): X. H. Lin, J. Zhang, and Q. Li, "Cluster head selection algorithm for UAV assisted clustered IoT network utilizing blockchain," *ZTE Communications*, vol. 19, no. 1, pp. 30 – 38, Mar. 2021. doi: 10.12142/ZTECOM.202101005.

1 Introduction

With the development of fifth-generation (5G) networks, which provide extended coverage, higher throughput, lower latency and higher connection density with a massive bandwidth, 5G based Internet of Things (5G-IoT) devices have emerged as small-size, low-cost, typically battery-powered and densely distributed devices to support large-scale information exchange. Therefore, the 5G-IoT is a core component of the future network. On the one hand, the evolution of 5G networking not only has paved the way for the connection of massive IoT nodes to the Internet to facilitate the advancement of various IoT applications from theory to reality, but also has led to the proposal of various potential technologies, such as millimeter-wave, massive multiple-input multiple-output and device-to-device. On the other hand, over 75 billion devices will be connected to the IoT by 2025, which is expected to have a dramatic impact on our lives in the near future[1]. This will be beneficial for supporting networks in generating enormous amounts of information traffic, enabling humans to obtain messages about anything and anyone at any time and any place (4A)[2]. Despite the fruitful developments in 5G-IoT communications, several issues that hamper effective IoT communication in 5G networks remain unsolved, including redundancy in data, dynamic size of the network, less reliable medium, heterogeneous network, and multiple base stations (BSs) or sink nodes. To process data in a distributed way, remove redundant data and improve the energy efficiency, the IoT system needs to adopt clustering

technology[3]. Clustering builds a hierarchy of clusters or groups of sensing nodes that collects and transfers the data to its respective cluster heads (CHs). The CH then groups and sends the data to the sink node or BS. The CHs act as middleware between the end user and the network, so the selection of CHs is particularly important[4].

Due to the limited computing capacity and energy of IoT devices in the process of data transmission, it is difficult to adopt highly complex algorithms and frameworks to ensure the data security. Therefore, IoT devices face many security issues that include the authenticity and confidentiality of data[1]. Blockchain, which can guarantee the integrity, transparency and security of data in industrial data processing, has attracted great attention in the application of IoT[5]. Integrating blockchain and IoT has many advantages. Firstly, it can improve resilience and adaptability of the IoT system. Blockchain can store redundant replicas of data in the form of transactions over blockchain nodes, which helps to maintain data integrity and provide resilience to the IoT system. Secondly, since blockchain is a distributed ledger, using blockchain as the data management mechanism for the IoT can adapt to varying environments and use cases to meet the growing needs and demands of IoT devices, which improves the adaptability of the system. Finally, integrating blockchain and IoT can enhance the fault tolerance and security of the whole system. However, due to the verification of blockchain, IoT devices will perform additional computing tasks, which will greatly increase energy consumption and reduce the service life of IoT systems.

Considering the energy limitation of IoT devices, there are many clustering technologies and CH selection algorithms to reduce energy consumption of the IoT system. HEINZELMAN et al. proposed a low-energy adaptive clustering hierarchy (LEACH) protocol[6], in which CHs were randomly selected in each round. Since the selection of CHs is random, the nodes with low energy are at the same priority as those with high energy. If the nodes with low energy are selected as CHs, they will fail quickly, thus shortening the network life. Based on the LEACH, TRUPTI et al. proposed a CH selection algorithm based on residual energy, which is to choose the devices with more residual energy as the CH[4]. YOUNIS et al. adopted the hybrid energy efficient distributed clustering (HEED) algorithm, which could select devices with high battery power as the CH through the proposed iterative CH selection algorithm[7]. In the above works, wireless sensors or IoT devices are selected as CHs. Although the energy limits of devices are considered in these algorithms when selecting CHs, the energy limitations of IoT devices will lead to frequent failure, resulting in more system energy consumption. AADIL et al. proposed energy aware link-based clustering (EALC), which adds two other parameters (energy level and distance) to the neighborhood to select the optimal CH. EALC extends cluster life and reduces energy consumption[8].

Due to the large difference of devices and limited resources of the blockchain-based IoT system, which needs to perform additional blockchain computing tasks, the choice of IoT devices as the CHs will have great limitations. The emergence of unmanned aerial vehicles (UAVs) provides new opportunities for the blockchain-based IoT system. When UAVs are used as flying BSs, they can support the connectivity of existing ground wireless networks to help land systems achieve good coverage and effectively reduce the data traffic of other BSs. Moreover, as devices with flexible deployment, UAVs are equipped with high-performance calculators with high computing capacity, which can quickly respond to the communication and computing needs of IoT devices, thus improving the quality of service[9]. In addition, solar-powered UAVs can convert solar energy into electric energy, thus increasing its service time[10]. Moreover, a large number of UAVs can cooperate with each other through relay nodes to build a self-organizing intelligent UAVs network to complete complex tasks[11]. Therefore, it has great advantages to choose UAVs as CHs.

To solve the problems of limited resources and security faced by IoT clusters, the main contributions of this paper are as follows. Firstly, the UAV network served IoT cluster system is built. To ensure the security of data, the IoT devices in the system use blockchain technology to store data. Secondly, we propose a UAV CH selection algorithm. The algorithm jointly considers the distance between UAVs and IoT devices, the distance between UAVs and BSs, residual energy, and the maximal transmit power of UAVs. The IoT devices calculate the corresponding weighted value of the UAV through the proposed algorithm, and choose the UAV with the smallest weighted value to vote. The UAV with the most votes serves the IoT cluster as the CH. Finally, based on the proposed algorithm, this paper evaluates several performance indicators such as the energy consumption of the IoT cluster, the average secrecy rate and the maximal number of packets received by the BS, and compares the performance with several existing CH selection algorithms, which demonstrates the superiority of the proposed algorithm.

This paper is structured as follows. Section 2 presents our system model and the basic procedure of the practical Byzantine fault tolerance (PBFT) consensus algorithm. Moreover, we use received signal strength (RSS) technology to estimate the distance between IoT devices and UAVs in this section. In Section 3, we propose a UAV selection algorithm based on a private blockchain and introduce performance evaluation indicators. The simulation results are analyzed in Section 4. Finally, Section 5 concludes this paper.

2 System Model

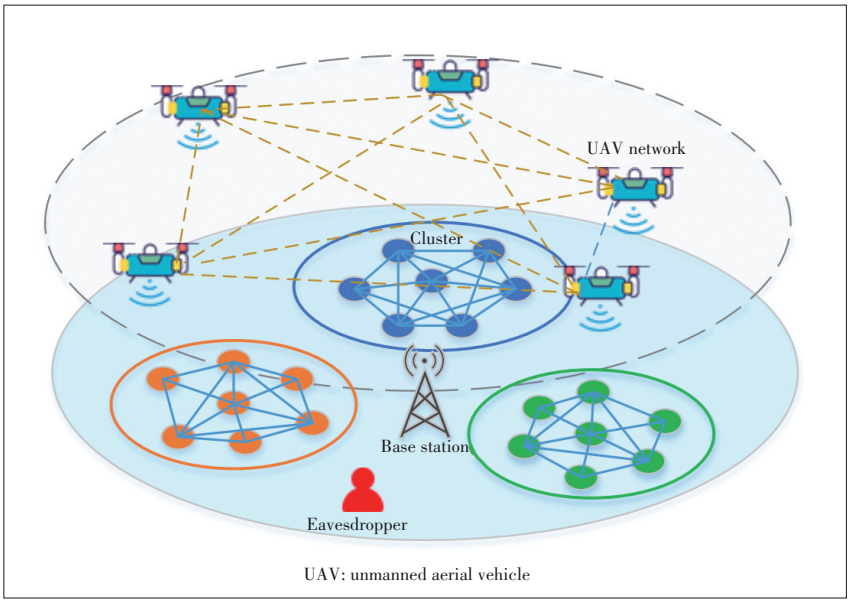
2.1 Network Topology

To enable secure energy-efficient communication, a blockchain-based CH selection algorithm is proposed in this paper.

As shown in **Fig. 1**, a blockchain-based clustered IoT network, where a UAV swarm composed of M UAVs, denoted by set $\{U_1, U_2, U_3, ..., U_M\}$, is deployed to serve S IoT clusters, denoted by set $\{C_1, C_2, C_3, ..., C_S\}$. Each IoT cluster contains K IoT devices, denoted by set $\{D_1, D_2, D_3, ..., D_K\}$. To reduce the power consumption of the IoT devices during data transmission, UAVs hovering in the sky collect data from the IoT devices before transmitting the collected data to the BS. Meanwhile, the IoT clusters adopt private blockchain technology to protect their collected data and to facilitate secure communication. Eavesdroppers coexisting with the IoT clusters may intercept the transmitted data. We assume that the IoT devices and the UAVs can establish Line-of-Sight (LoS) communication links for data transmission. In contrast, an eavesdropper may experience a Rayleigh fading channel while eavesdrop on the IoT devices. The UAVs first broadcast a message containing the pilot signal and the UAV information to the IoT devices. The IoT devices in each cluster use blockchain technology to verify the information received from UAVs and estimate the distance to each UAV. Using the proposed CH selection algorithm, the IoT devices in each cluster then vote through the PBFT consensus algorithm. According to the voting results, the UAV that receives the most votes from the cluster is selected as the CH. When different clusters choose the same UAV as the CH, it is assumed that when the energy of the UAV selected by a cluster is exhausted, that cluster will select a different UAV. The IoT devices in each cluster communicate using orthogonal frequency division multiple access (OFDMA) technology, with a system bandwidth of B Hz.

2.2 Message Broadcasted by UAVs

As the first step of the blockchain-based CH selection process, the M UAVs first broadcast message I_m to all IoT devices in the area. The message content includes the serial number of the UAVs, U_m, which ranges from 1 to M for the considered UAV swarm; the maximal transmit power of the UAV, P_m; the remaining energy in the battery of the UAV E_m; the distance between UAV m and BS d_{BU}^m, which is estimated at the BS by measuring the pilot signal of the UAV. The IoT devices can obtain the message of the UAV from the mark bit named Mark Signa.



▲**Figure 1. UAV assisted clustered IoT network utilizing blockchain**

2.3 Distance Estimation Based on RSS

In practice, the channel state information (CSI) between IoT devices and UAVs is unknown. To evaluate the CSI, the IoT devices usually adopt distance estimation. On the one hand, a UAV flying in the sky can provide a LoS propagation environment, which is beneficial for evaluating the distances between the IoT devices and the UAV. On the other hand, the IoT devices are powered by batteries and have a simple hardware structure, and it is difficult for them to perform complex signal processing to obtain the CSI. Therefore, distance estimation based on RSS of an IoT device is suitable for UAV-assisted IoT communication[12].

In particular, after the messages broadcast by the UAVs are received by the IoT devices, each IoT device will estimate the distance to each UAV based on the RSS. By utilizing the RSS at the IoT device and the information of the UAV's maximal transmit power provided in the broadcast message, the distance between an IoT device and a UAV can be formulated through maximum likelihood estimation as follows:

$$\hat{d}_{mk} = \left(\frac{P_{mk}}{P_m}\right)^{\frac{-1}{n_p}}, \tag{1}$$

where P_{mk} is the signal strength received by IoT device k from UAV m, i.e., the RSS; P_m is the maximal transmit power of UAV m, which is specified in the broadcast message; n_p is the path loss factor.

2.4 Private Blockchain Constructed for IoT Clusters

To ensure data security, the IoT devices adopt a private blockchain to verify their collected data. Specifically, the IoT devices transmit their received messages broadcast from the UAVs to other IoT devices in the same cluster as transactions and then apply the PBFT algorithm to reach agreement. The consensus data will be stored in blocks in the form of transaction, and each block contains the hash code of the previous block, thus forming a blockchain. To ensure the privacy and security of the data in the PBFT process, a hash algorithm and an asymmetric encryption

algorithm are introduced. We use the elliptic curve encryption (ECC) algorithm and Secure Hash Algorithm-256 (SHA-256) to detect whether transactions have been tampered with during data transmission[13]. The encryption process is shown in **Fig. 2**. By using SHA-256, we can generate a Merkle root, which can be used to effectively compress the amount of data to link each block. When using encrypted data, the IoT devices can perform the same hash calculation and compare the hash codes to verify the data. The ECC algorithm is used to generate public and private keys to encrypt the data. The data in the database will be encrypted into ciphertext by using the public key. Each user should provide his or her own private key to decrypt the encrypted message used for the custom service. These two algorithms can ensure the privacy of the data and prevent illegal operations. The consensus process of PBFT is shown in Fig. 2 which contains the following phases:

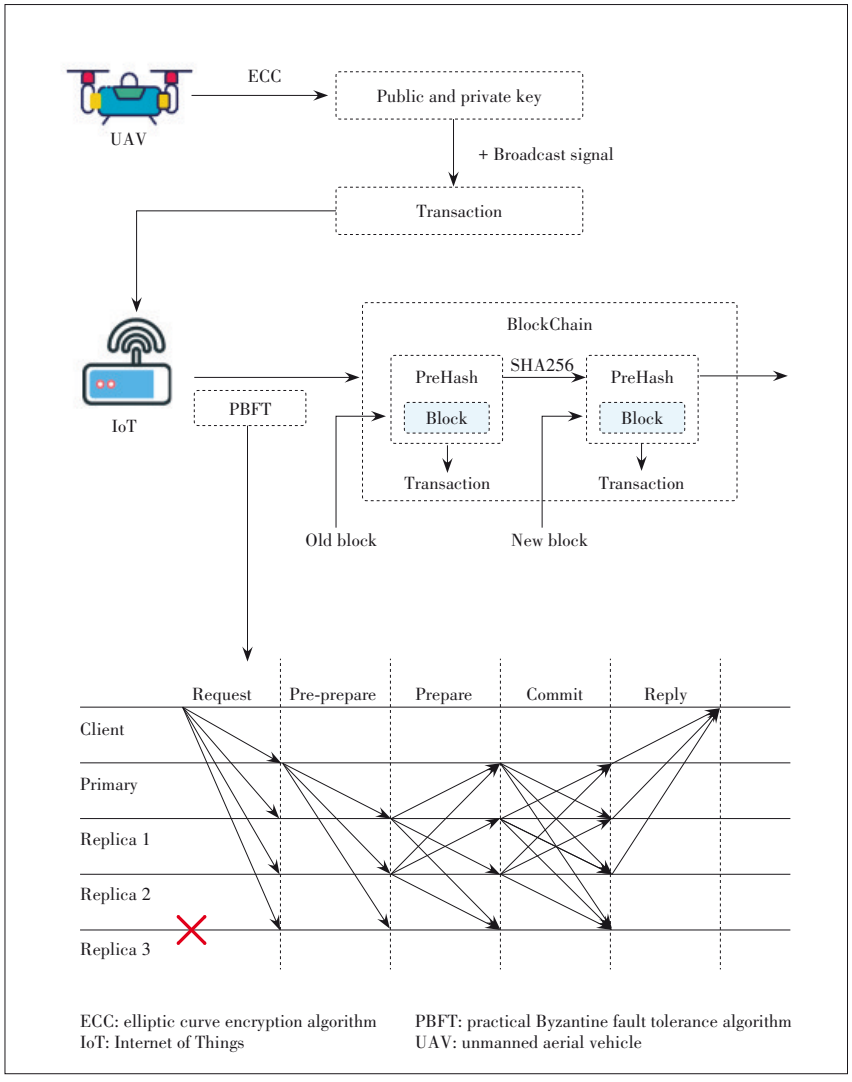
• Request phase: We refer to the IoT device that needs to publish transactions as a client. In our model, IoT devices not only act as the publisher of transactions, but also as the verifier of transactions. Before IoT devices transmit data to other nodes for verification, they need to encrypt the data.

• Pre-prepare phase: After receiving the message from the client, the primary node will assign an integer sequence number to the request, and then generate the pre-prepare message. The primary node then broadcasts the pre-prepared message to replica nodes.

• Prepare phase: The replica nodes verify the message that has not been tampered with, and then send a prepare message to other nodes.

• Commit phase: After verifying that all the prepared messages have not been tampered with, all nodes will broadcast the confirm message to other nodes.

• Reply phase: After verifying the message, all nodes will return the result to the client.



▲**Figure 2. Private blockchain constructed for IoT clusters and PBFT process**

2.5 System Performance Metrics

To analyze the performance of the CH selection algorithm proposed in this paper, several important system parameters will be used. The CH selection process consists of four steps: An IoT cluster receives the broadcast messages from the UAVs, each IoT device chooses a UAV to serve as the CH based on the received messages, the IoT devices in the IoT cluster achieve consensus through the PBFT algorithm, and the IoT cluster sends a response message to the UAV swarm indicating the chosen CH. We utilize the energy consumption for CH selection to represent the system resource consumption of the IoT cluster. Meanwhile, system performance metrics, i. e., the average secret rate and the maximal number of received packets, will be used to evaluate the gain of our proposed algorithm.

• CH selection energy consumption: CH selection delay refers to the time taken by a cluster from receiving UAV signal to reaching consensus and finally sending the selection result to the selected UAV, which reflects the effectiveness of CH selection algorithm. Large time delay will lead to large energy consumption, which will affect the life cycle of the device.

• Average secrecy rate: The secrecy rate is a key design metric for IoT networks that is widely adopted for evaluating physical layer security is the secrecy rate. High secrecy rate will reduce the probability of data eavesdropping.

• Maximal number of packets received by the BS: The number of packets received by the BS reflects the throughput of the system, which is a very important measure of the system.

3 Working Model

3.1 UAV Selection Algorithm

Based on the messages broadcast by the UAVs, all IoT devices in a cluster adopt the PBFT algorithm to verify their received messages to achieve consensus. Then, the IoT cluster chooses a UAV from the UAV swarm as its CH by following steps.

• Step 1: According to Eq. (3), each of the K IoT devices in the IoT cluster estimates the distance d_{mk} from each UAV based on the RSS.

• Step 2: The distance between the BS and the m-th UAV, denoted by d_{BU}^{m}, can be determined from the broadcast information sent by the UAV.

• Step 3: From the broadcast messages sent by the UAVs, the IoT devices are informed of the remaining energy of each UAV, E_m. For each UAV, the energy ratio of the total remaining energy of all UAVs to the remaining energy of that UAV is

$$E_p = \frac{\sum_{m=1}^{M} E_m}{E_m}. \tag{2}$$

• Step 4: From the messages broadcast by the UAVs, the IoT devices are also informed of the maximal transmit power of each UAV, P_m. For each UAV, the ratio of the total maximal output power of all UAVs to the transmit output power of that UAV is

$$P_p = \frac{\sum_{m=1}^{M} P_m}{P_m}. \tag{3}$$

• Step 5: The weighted value of each UAV is computed as follows:

$$F_k = \alpha \hat{d}_{mk} + \beta d_{BU}^{m} + \varsigma E_p + \theta P_p, \tag{4}$$

where α, β, ς and θ are weighting factors that satisfy $\alpha + \beta + \varsigma + \theta = 1$.

• Step 6: Each IoT device calculates its corresponding weighted value F_k for each UAV following the above method. Then, the k-th IoT device votes for the UAV with the smallest F_k to serve as the CH. All IoT devices in the same IoT cluster use the PBFT algorithm to vote for consensus. Finally, the UAV with the most votes is chosen to serve the entire cluster. The proposed CH selection process is presented in Algorithm 1.

Algorithm 1. Proposed UAV CH selection algorithm

Input: UAVs $U_m (m \in 1, 2, ..., M)$ blockchain-based IoT clusters $C_s (s \in 1, 2, ..., S)$ and IoT devices D_k in each cluster, $D_k (k \in 1, 2, \cdots, K)$.

Output: UAVs chosen as the CH, $CH_s (s \in 1, 2, \ldots, S)$.

/* Initialization Phase */

Assign each UAV m transmit power P_m and residual energy E_m.

Assign the distance between UAV m and BS d_{BU}^{m}.

Assign the weighting factors $\alpha, \beta, \varsigma, \theta$.

/* Computation Phase */

While (k++<K+1) **do**

for each IoT device $D_k (k \in 1, 2, ..., K)$ **do**

Estimate the distance between IoT device k and each UAV m, d_{mk}, using (1)

end for

for each IoT device $D_k (k \in 1, 2, ..., K)$ **do**

Measure the energy ratios of the UAVs, E_p using (2).

end for

for each IoT device $D_k (k \in 1, 2, ..., K)$ **do**

Measure the maximal transmit power ratios of the UAVs, P_p using (3).

end for

Calculate F_k using (4).

Vote for the optimal UAV with smallest F_k.

end while

return the UAV with the most votes

3.2 Performance Metrics

3.2.1 Energy Consumption for CH Selection

In our system, the energy consumption of an IoT device mainly includes three components: the energy consumption for data transmission, E_{total}^{tx}; the energy consumption for data reception, E_{total}^{rx}; and the energy consumption for computing using the PBFT algorithm, E_{total}^{c}. For a UAV swarm composed of M UAVs and an IoT cluster with K IoT devices, each IoT device in the cluster will transmit $3K$ transactions, receive $(M + 2K - 1)$ transactions, and perform $(2K - 1)$ computing operations during the PBFT process.

The energy consumption of each IoT device during the process of transmitting transactions is calculated as[14]

$$E_{total}^{tx} = \begin{cases} 3KL \cdot \left(E_{elec} + \varepsilon_{fs} d_{mk}^{2}\right), d_{mk} < d \\ 3KL \cdot \left(E_{elec} + \varepsilon_{fs} d_{mk}^{4}\right), d_{mk} \geq d \end{cases}, \tag{5}$$

where E_{elec} is the energy dissipated per bit to run the transmitter or receiver circuit, $\varepsilon_{fs} d_{mk}^{2}$ and $\varepsilon_{fs} d_{mk}^{4}$ are the energy cost of a single amplifier under the two communication models depending on the distance between the transmitter and receiver, and d is the threshold value.

The energy consumption of each IoT device during the process of receiving transactions is calculated as

$$E_{total}^{rx} = L \cdot E_{elec} (M + 2K - 1). \tag{6}$$

The energy consumption of each IoT device during the process of verifying transactions is calculated as

$$E_k^c = k_m s_m f_k^2 LM(2K-1), \tag{7}$$

where s_m is the number of rotations required to calculate 1 bit of data, k_m is the calculation efficiency and f_k is the computing capacity of the k-th IoT device.

Considering that there are K IoT devices in the IoT cluster, the total energy consumed by all devices in the cluster for PBFT processing is calculated as

$$E_{total}^c = \sum_{k=1}^{K} E_k^c = \sum_{k=1}^{K} k_m s_m f_k^2 LM(2K-1). \tag{8}$$

In the end, the total energy consumption of the IoT cluster for selecting the m-th UAV in the UAV swarm as the CH is

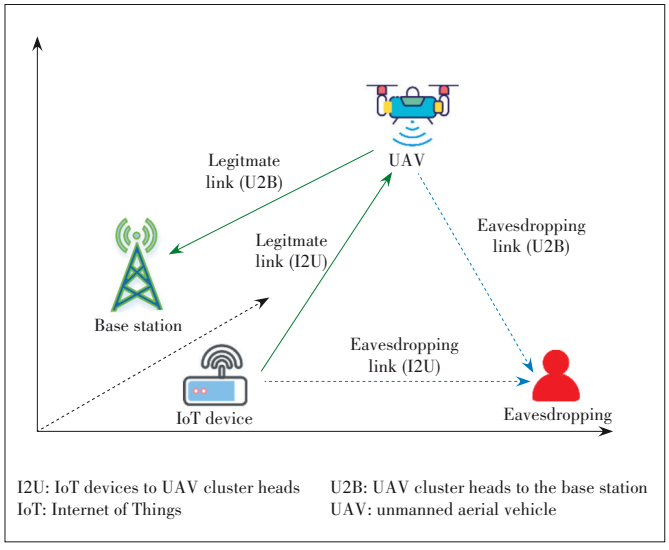
$$E_k^s = E_{total}^c + E_{total}^{tx} + E_{total}^{rx}. \tag{9}$$

For all S IoT clusters, the total energy consumption is obtained as follows:

$$E_t = \sum_{s=1}^{S} E_k^s. \tag{10}$$

3.2.2 Average Secrecy Rate of IoT Clusters

A diagram of the system secrecy rate is shown in **Fig. 3**. When the strength of legitimate links is greater than that of eavesdropping links, a nonzero secrecy rate will be achieved[15]. When the m-th UAV in the UAV swarm is chosen as the CH for an IoT cluster, the information transmitted from the IoT devices to the UAV CH and from the UAV CH to the BS can be eavesdropped on. Therefore, the secrecy rates of both types of links are analyzed in the following.



▲**Figure 3. Diagram of system secrecy rate**

For the information transmission from IoT device k to the UAV CH, i.e., UAV m, the achievable rate is obtained as follows:

$$R_{km} = \log\left(1 + \frac{P_k \beta_0}{\sigma^2 d_{mk}^2}\right), \tag{11}$$

where P_k is the transmission power of IoT device k, β_0 is the signal gain at a distance d_0= 1 m, σ^2 is the noise power and d_{mk} is the distance between IoT device k and the chosen UAV m.

For the information transmission from UAV CH to the BS, the achievable rate is obtained as follows:

$$R_{mb} = \log\left(1 + \frac{P_m \beta_0}{\sigma^2 \left(d_{BU}^m\right)^2}\right). \tag{12}$$

When there is an eavesdropper, the transmission rate from an IoT device to the eavesdropper is calculated as

$$R_{ke} = \log\left(1 + \frac{P_k \beta_0}{\sigma^2 d_{ke}^{\gamma}}\right), \tag{13}$$

where d_{ke} is the distance between IoT device k and the eavesdropper, and γ is the path loss exponent.

For the eavesdropping link from a UAV to the eavesdropper, the transmission rate is calculated as

$$R_{ue} = \log\left(1 + \frac{P_m \beta_0}{\sigma^2 d_{me}^{\gamma}}\right), \tag{14}$$

where d_{me} is the distance between UAV m and the eavesdropper.

The average secrecy rate of an IoT cluster is

$$R_{\text{sec}}^{av} = \frac{\sum_{k=1}^{K}\left[R_{km} + R_{mb} - \left(R_{ke} + R_{ue}\right)\right]^+}{K}, \tag{15}$$

where $[x]^+ = \max(x, 0)$.

For all the S IoT clusters, the total average secrecy rate can be calculated as follows:

$$R_{\text{sec}}^{total} = \sum_{s=1}^{S} R_{ke}^{av}. \tag{16}$$

3.2.3 Maximal Number of Packets Received by BS

The number of packets received by the BS is an important indicator of the total throughput for an IoT cluster. When an IoT device transmits data packets comprising L_k bits to its UAV CH in each time slot and the UAV CH retransmits these data packets to the BS, the time consumed for the IoT device to transmit data to the UAV CH is

$$t_k = \frac{L_k}{(B/K)\log\left(1+\frac{P_k\beta_0}{(B/K)\sigma^2 d_{mk}^2}\right)}. \quad (17)$$

The IoT devices within an IoT cluster utilize the OFDMA scheme to transmit their data packets to the UAV CH, and hence, the total time consumed by the IoT cluster to transmit data to the UAV CH is

$$t_k^t = \max\left(t_k\right). \quad (18)$$

When the UAV CH retransmits these data packets to the BS, the UAV CH can utilize the whole usable bandwidth, and hence, the consumed time is

$$t_u = \frac{KL_k}{B\log\left(1+\frac{P_m\beta_0}{B\sigma^2\left(d_{BU}^m\right)^2}\right)}. \quad (19)$$

Meanwhile, the UAV also consumes propulsion power to support it as it flies in the sky. It should be noted that if the UAV uses up its energy between communication and propulsion, the UAV will be unable to retransmit the data packets, and the CH will break down. According to Ref. [16], the power consumed for propulsion is calculated as

$$P_v = \frac{\delta_d}{8}\rho s A \Omega^3 R^3, \quad (20)$$

where δ_d is the profile drag coefficient, ρ is the air density, s is the robustness of the rotor, A is the area of the rotor, and R is the radius of the rotor.

Each time a data packet is sent, the energy consumption of the UAV is

$$E_u = P_v \cdot \left(t_k + t_u\right) + KL_k \cdot E_{Rx} + P_m t_u. \quad (21)$$

The maximal number of packets that UAV m can transmit is

$$n_m^s = \frac{E_m}{E_u}. \quad (22)$$

Thus, the maximal number of packets received by the BS is

$$n_m^{total} = \sum_{s=1}^{S} n_m^s. \quad (23)$$

4 Performance Analysis and Simulation Results

In this section, numerical results are presented for evaluating the performance of the proposed CH selection algorithm. We compare our proposed CH selection scheme with other existing CH selection schemes, such as Low-Energy Adaptive Clustering Hierarchy (LEACH)[6], Hybrid Energy-Efficient Distributed Clustering (HEED)[7] and Energy Aware Link-Based Clustering (EALC)[8]. To illustrate the advantages of our proposed algorithm for blockchain-based IoT clusters, we use the existing CH selection algorithms as baselines for selecting UAV CHs and compare the system performance in each case with that achieved using the algorithm proposed in this paper. The simulation parameters are shown in **Table 1**.

4.1 Analysis of Security

1) Data trustworthiness: Data trustworthiness greatly affects the security of the collected data. Malicious nodes may insert fake data into the network and interfere with normal nodes, which may cause node failure. Our system uses the PBFT consensus algorithm, which has an error tolerance rate of $(N-1)/3$. As long as the number of failed nodes does not exceed this tolerance value, the system's data can be transmitted once the correct consensus has been reached, which can effectively guarantee the credibility of the data.

2) Privacy: Privacy is extremely important to the system. If a user's private information is leaked, this may result in enormous losses. Our system uses private blockchain technology; thus, devices will be authenticated by blockchain, and data will be stored in the blocks in the form of transactions. A block cannot be tampered with or deleted, thereby guaranteeing the undeniability and confidentiality of the data. Our proposed blockchain-based CH selection algorithm does not require the intervention of a trusted third party, thereby ensuring the robustness and privacy of the system.

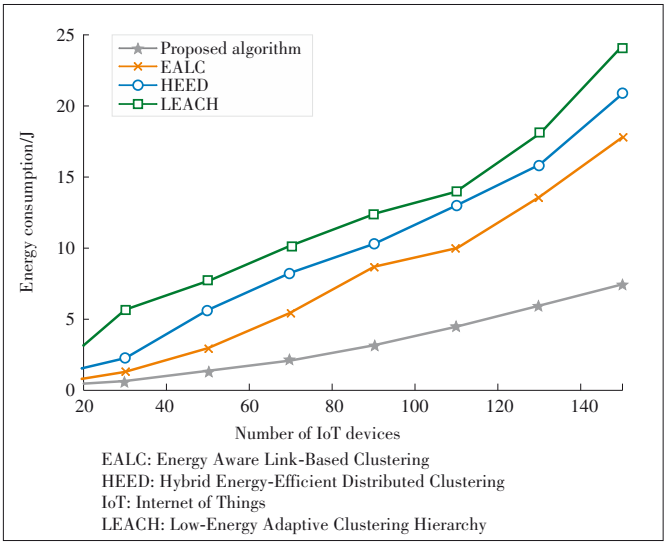
▼Table 1. Simulation parameters

Parameter	Value
Network area	100 m×100 m
Number of UAVs	5 – 30
Total number of IoT devices	10 – 150
The number of IoT in a cluster	4 – 20
UAV transmit power P_m	2 – 4 W
UAV remaining energy E_m	400 – 900 kJ
IoT transmit power P_k	0.5 – 1.5 W
Computational capability of an IoT device f_k	0.1 GHz CPU cycles/bit
Computational energy efficiency coefficient of the processors chip in an IoT device k_m	10^{-26}
Computation workload/intensity s_m	18 000 CPU cycles/bit
Sizes of transaction L	256 bit
Size of a packet transmitted by an IoT device L_k	4 000 bit
Noise power, σ^2	−100 dBm
Weighting factors, $\alpha, \beta, \varsigma, \theta$	0.3, 0.2, 0.3, 0.2

IoT: Internet of Things UAV: unmanned aerial vehicle

4.2 Analysis of Energy Consumption of IoT Devices

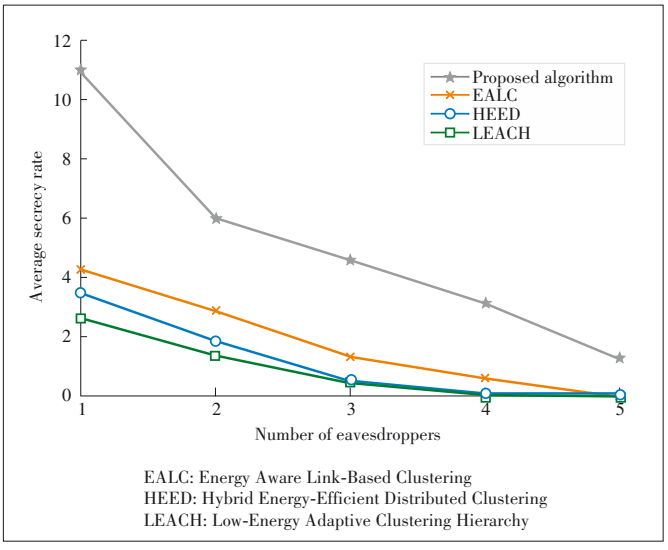
Fig. 4 plots the energy consumption versus the number of IoT nodes for the various CH selection algorithms. The number of UAVs is fixed at 6. From Fig. 4, it can be seen that our proposed strategy achieves the minimal energy consumption compared with the other existing CH algorithms. Meanwhile, as the number of IoT devices increases, the gaps between our proposed algorithm and the other existing algorithms become larger. This gap enlargement occurs because the average distance between the IoT devices and the UAVs is small and the uplink transmission between the IoT devices and the UAV CHs can take advantage of the LoS channel environment in our proposed algorithm. Therefore, our proposed algorithm incurs significantly less energy consumption for communication than the other schemes do. Moreover, compared with the typical random selection algorithms LEACH and HEED, which select CHs by means of multiple votes and therefore cause the IoT devices to consume more energy, our proposed algorithm needs each device to vote only once; hence, the energy consumed to reach consensus within an IoT cluster is reduced.



▲**Figure 4. Energy consumption versus the number of IoT devices**

4.3 Analysis of Average Secrecy Rate

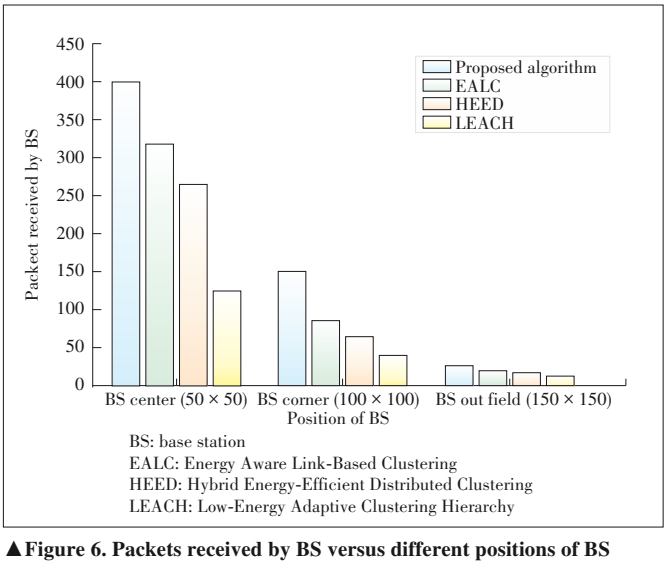
Fig. 5 shows the average secrecy rates achieved with the different CH selection algorithms versus the number of eavesdroppers. The number of UAVs is fixed at 6, and the number of IoT devices is 50. The figure shows that as the number of eavesdroppers increases, the average secrecy rate decreases. The presence of more eavesdroppers will cause the eavesdropping rate for an IoT cluster to increase, Hence, the secrecy rate of the IoT cluster will inevitably decrease. As shown in Fig. 5, the average secrecy rate of our proposed algorithm is significantly better than those of the other existing CH algorithms. This is because the distance and transmit power of each UAV are considered in our proposed algorithm. In this way, both the legitimate transmission rate and the secrecy rate of the IoT clusters can be increased.



▲**Figure 5. Average secrecy rate versus the number of eavesdroppers**

4.4 Analysis of the Maximal Number of Packets Received by BS

For 150 IoT devices and 6 UAVs, **Fig. 6** analyzes the number of data packets sent by the IoT devices and received by the BS. We compare the maximal numbers of data packets that the BS can receive at three typical locations: the center of the IoT network, the corner of the IoT network, and the outside of the IoT network. Our proposed algorithm performs significantly better than the other algorithms in terms of this metric. This is because the maximal number of data packets received at the BS strongly depends on the energy of the CHs and IoT devices. Less energy consumption of the IoT clusters will lead to a longer lifetime of the IoT network, and hence, more data packets can be transmitted in the system. Our proposed algorithm can reduce the energy consumed by the IoT devices for communications, including data transmission, data reception,



▲**Figure 6. Packets received by BS versus different positions of BS**

and data processing. Moreover, the remaining energy of the UAVs is also considered in our proposed CH selection algorithm. Consequently, the proposed algorithm can prolong the lifetime of the system by reducing the probability of UAV CH breakdown. Thus, the number of data packets received by the BS increases.

5 Conclusions

In this paper, we propose a novel UAV CH selection algorithm for IoT clusters based on blockchain technology. Our proposed algorithm considers the combined effect of the distances between the IoT devices and the UAVs, the distances between the UAVs and the BS, the maximal transmission power of the UAVs, and the remaining energy of the UAVs; it has the flexibility to assign different weights to these different contributing factors. Each IoT device votes for its optimal UAV through our proposed CH selection algorithm, and then, all IoT devices in a cluster use blockchain technology to achieve consensus to ensure the correctness and security of the vote data. The UAV with the most votes among the devices in an IoT cluster will act as the CH to serve the IoT cluster. Simulation results illustrate the system performance that are compared with corresponding results of the existing algorithms, such as LEACH, HEED and EALC. The simulation results show that our proposed algorithm outperforms the existing algorithms in terms of the energy consumption of the IoT clusters, the average secrecy rate of the IoT clusters and the maximal number of data packets received by the BS.

References

[1] BUTUN I, ÖSTERBERG P, SONG H B. Security of the Internet of Things: vulnerabilities, attacks, and countermeasures [J]. IEEE communications surveys & tutorials, 2020, 22(1): 616 – 644. DOI: 10.1109/COMST.2019.2953364
[2] AGIWAL M, ROY A, SAXENA N. Next generation 5G wireless networks: a comprehensive survey [J]. IEEE communications surveys & tutorials, 2016, 18 (3): 1617 – 1655. DOI: 10.1109/COMST.2016.2532458
[3] XU L N, COLLIER R, O'HARE G M P. A survey of clustering techniques in WSNs and consideration of the challenges of applying such to 5G IoT scenarios [J]. IEEE Internet of Things journal, 2017, 4(5): 1229 – 1249. DOI: 10.1109/JIOT.2017.2726014
[4] BEHERA T M, MOHAPATRA S K, SAMAL U C, et al. Residual energy-based cluster-head selection in WSNs for IoT application [J]. IEEE Internet of Things journal, 2019, 6(3): 5132 – 5139. DOI: 10.1109/JIOT.2019.2897119
[5] ALI M S, VECCHIO M, PINCHEIRA M, et al. Applications of blockchains in the Internet of Things: a comprehensive survey [J]. IEEE communications surveys & tutorials, 2019, 21(2): 1676 – 1717. DOI: 10.1109/COMST.2018.2886932
[6] HEINZELMAN W B, CHANDRAKASAN A P, BALAKRISHNAN H. An application-specific protocol architecture for wireless microsensor networks [J]. IEEE transactions on wireless communications, 2002, 1(4): 660 – 670. DOI: 10.1109/TWC.2002.804190
[7] YOUNIS O, FAHMY S. HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks [J]. IEEE transactions on mobile computing, 2004, 3(4): 366 – 379. DOI: 10.1109/TMC.2004.41
[8] AADIL F, KHAN M F, MAQSOOD M, et al. Energy aware cluster-based routing in flying ad-hoc networks [J]. Sensors, 2018, 18(5): 1413. DOI: 10.3390/s18051413
[9] MOZAFFARI M, SAAD W, BENNIS M, et al. A tutorial on UAVs for wireless networks: applications, challenges, and open problems [J]. IEEE communications surveys & tutorials, 2019, 21(3): 2334 – 2360. DOI: 10.1109/COMST.2019.2902862
[10] SUN Y, DONGFANG X, NG D W K, et al. Optimal 3D-trajectory design and resource allocation for solar-powered UAV communication systems [J]. IEEE transactions on communications, 2019, 67(6): 4281 – 4298. DOI: 10.1109/TCOMM.2019.2900630
[11] GUPTA L, JAIN R, VASZKUN G. Survey of important issues in UAV communication networks [EB/OL]. (2016-03-28)[2020-10-16]. https://arxiv.org/abs/1603.08462
[12] MAO G, FIDAN B, ANDERSON B D O. Wireless sensor network localization techniques [J]. Computer networks, 2007, 51(10): 2529 – 2553. DOI: 10.1016/j.comnet.2006.11.018
[13] FERNÁNDEZ-CARAMÉS T M, FRAGA-LAMAS P. A review on the use of blockchain for the Internet of Things [J]. IEEE access, 2018, 6: 32979 – 33001. DOI: 10.1109/ACCESS.2018.2842685
[14] ARAFAT M Y, MOH S. Localization and clustering based on swarm intelligence in UAV networks for emergency communications [J]. IEEE Internet of Things journal, 2019, 6(5): 8958 – 8976. DOI: 10.1109/JIOT.2019.2925567
[15] WU Q Q, MEI W D, ZHANG R. Safeguarding wireless network with UAVs: a physical layer security perspective [EB/OL]. (2019-07-24)[2020-10-16]. https://arxiv.org/abs/1902.02472
[16] ZENG Y, XU J, ZHANG R. Energy minimization for wireless communication with rotary-wing UAV [EB/OL]. (2018-04-06)[2020-10-16]. https://arxiv.org/abs/1804.02238

Biographies

LIN Xinhua is a graduate student of Huazhong University of Science and Technology, China. His main research interests include UAV communications, blockchain technology and IoT networks.

ZHANG Jing (zhangjing@hust.edu.cn) received the M.S. and Ph.D. degrees in electronics and information engineering from Huazhong University of Science and Technology (HUST), China in 2002 and 2010, respectively. He is currently an associate professor with HUST. He has conducted research in the areas of multiple-input multiple-output, CoMP, beamforming, and next-generation mobile communications. His current research interests include HetNet in 5G, green communications, energy harvesting, IoT network, optimization and performance analysis in networks.

LI Qiang received the Ph.D. degree in electrical and electronic engineering from Nanyang Technological University (NTU), Singapore in 2011. He is currently an associate professor with Huazhong University of Science and Technology (HUST), China. His current research interests include next generation mobile communications, fog computing, edge caching, cognitive radios/spectrum sharing, wireless cooperative communications, full-duplex techniques, simultaneous wireless information and power transfer.