Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 4009078, 13 pages
https://doi.org/10.1155/2022/4009078

Research Article

Blockchain and UAV-Enabled Signal Source Identification with Edge Computing and Wireless Signal-Aerial Image Fusion

Jian Xiao,[1,2] **Peng Liu**,[1,2] **Huaming Lin**,[3] **Hangxiang Fang**,[4] **Jiayi Xu**,[1] **Hangguan Shan**,[4] **Haoji Hu**,[4] **Yi Huang**,[3] **and Huijuan Lu**[2]

[1]*School of Computer Science and Technology, Hangzhou Dianzi University, Hangzhou, China 310018*
[2]*Key Laboratory of Electromagnetic Wave Information Technology and Metrology of Zhejiang Province, College of Information Engineering, China Jiliang University, Hangzhou 310018, China*
[3]*Hangzhou Security and Technology Evaluation Center, Hangzhou, China 310020*
[4]*College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou, China 310027*

Correspondence should be addressed to Huaming Lin; lhm18@live.cn

Received 10 January 2022; Accepted 8 March 2022; Published 24 March 2022

Academic Editor: Celimuge Wu

Copyright © 2022 Jian Xiao et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This paper proposes a novel signal source identification system composed of unmanned aerial vehicles (UAVs) and a blockchain, in which the identification method makes full use of binocular camera data and received signal strength. The UAV tasks are organized by using blockchain technology and smart contracts. To tackle the challenge that the transmit power of the object and the channel path loss coefficient are unknown to the UAV, a maximum likelihood estimation method is developed to estimate the parameters in the path loss log-normal shadowing model. Then, the mean squared error is used as the metric to distinguish the signalling object. The simulation results show that the proposed method can effectively complete the task. Also, a mobile edge computing- (MEC-) enabled UAV testbed system is designed and implemented in real environment. The system works accurately where the number of candidate objects is 3.

1. Introduction

Radio signal source identification provides essential support in many applications [1–3]. However, except the basic information of the object (such as shape and outline), the parameters of the signal are usually unknown. Therefore, in a complex electromagnetic environment, it needs to first screen out the potential targets and then identify the one which is sending signals. The traditional ways of object detection and radio direction finding are easily constrained by their own mobility and rely on manual operation and control. Therefore, to improve the efficiency, accuracy, and reliability of the identification, as well as reduce the cost, an integrated and shareable aerial platform is required.

Technology advances in unmanned aerial vehicles (UAVs, also known as drones) have enabled them to carry multiple types of onboard sensors. Cameras are one kind of sensors that have been commonly used. A UAV carrying cameras can provide a clearer view from the air than ground while allowing flexible movement. Cameras carried on UAVs can be classified into many types, such as single camera [4], multiple cameras [5], and spectral cameras [6]. A binocular camera is a single camera with two lenses and is capable of outputting both graphs and depth information, thus arousing interest in UAV applications, such as UAV navigation [7], obstacle avoidance [8], and localization [9]. Furthermore, road detection [10] and photogrammetric measurements [11] can be also solved with UAV binocular vision.

Meanwhile, the reduced cost and weight of Software-Defined Radio (SDR) equipment make it feasible for UAVs to carry an SDR onboard. The application fields of UAVs carrying SDRs can then be extended to wildlife tracking, search, rescue, etc. For example, in [12], two SDR-based UAV-assisted wildlife tracking methods are presented: one is based on four single-stage antennas using the Doppler effect and the other one using Yagi omnidirectional antennas for

signal reach angle. Ref. [13] presents a UAV system carrying VHF telemetry equipment that includes a hexacopter UAV, an onboard computer, an SDR receiver, a directional antenna, and a control laptop on the ground. In paper [14], to search for survivors after a disaster, the authors use the UAV carrying an SDR as a GSM base station to receive signals sent by the target's GSM device and locate the target by the received signal strength and UAV coordinates.

As UAVs are getting more powerful and smarter nowadays [15], automatic UAV-assisted radio source detection becomes a potential solution and a hot research topic. An automatic UAV trajectory planning method for ground object localization is proposed in [16]. The solution locates ground objects by received signal strength and automatically finds paths with high localization accuracy and low energy consumption by reinforcement learning. A method for locating illegal base stations via received signal power in the case of unknown channel model and unknown noise model is proposed in [17]. It takes advantage of directional antennas and controls the UAV by Q-learning algorithms. However, all the above methods have only been validated in numerical simulations. In reality, the real-time performance of the system, due to heavy data transmission stress and computation demands, can be a major challenge to be settled in field experiments.

Considering a practical commercial application scenario, a user may not afford such a UAV fleet and it is also not necessary. Therefore, UAVs may be from a heterogeneous origin and form a computing paradigm of multiple autonomous agents. In the meantime, the air-ground integrated edge computing system has been put into practice [18]. In such an architecture, how to ensure secure communication and cooperation between multiple parties becomes a key problem. Blockchain [19, 20] has been proven to be very useful in various IoT applications. In literature [21], the authors describe a method of organizing the communication protocol, which allows agents of the multiagent system (MAS) to make decisions about their actions. The paper shows how to implement an autonomous economic system with UAVs and organize a communication system among agents in a peer-to-peer network using the decentralized Ethereum blockchain technology and smart contracts. "BUS" proposed in [22] is a UAV swarm-assisted data acquisition scheme in which data is collected from IoT devices via a UAV swarm and then stored in the nearest server with the assistance of blockchain. A smart contract is employed to handle the IoT devices and missions in BUS. In another work, the selection of the UAV for the desired quality of network coverage and the development of a distributed and autonomous real-time monitoring framework for the enforcement of service-level agreement (SLA) are introduced [23]. It builds a novel blockchain architecture that relies on machine learning techniques to monitor and penalize UAVs that violate SLA. In [24], the authors propose a new type of blockchain to resolve critical message dissemination issues in a vehicular ad hoc network (VANET), which can be used as a reference in our work.

In this paper, partly motivated by [25], we design and implement a mobile edge computing- (MEC-) enabled UAV system equipped with onboard SDR and binocular camera, one for each. A signal source identification algorithm that fuses the visual depth information and received power strength is proposed. The organization of tasks of UAVs is enabled by blockchain. Our method can work in situations where the objects' transmit power and channel parameters are unknown.

The rest of this paper is organized as follows. Section 2 briefly introduces the overall architecture of the system. Blockchain preliminaries are presented in Section 3. In Section 4, the system model, the four major parts, the formulation of the problem, and the design of the algorithm are described in detail. Section 5 gives the experimental results, including the results of the semiphysical simulation and the real-world experiment. Finally, Section 6 concludes the paper.

2. System Architecture

The proposed scenario consists of a target area, a hiding signal source, various UAVs, some users, a ground access point, edge computing servers, network services, and a blockchain, as shown in Figure 1. A user would like to make an order for signal source identification. With the help of the servers, a smart contract is generated with the order data (the purpose of the order, attribute data, participators, etc.) and then transferred to the blockchain. Any unoccupied UAVs can accept the contract which contains information about the task.

Then, the UAV makes a scheduled flight and informs the user about the result of the task. During the flight, the data collected by the UAV will be sent to the edge servers for analysis. After returning to the base, the UAV notifies the servers that the order is completed. This ensures the security and reliability of the proposed system.

3. Blockchain Preliminaries

The blockchain is essentially a distributed public ledger, where each transaction is recorded in a block. Each block is identified by its hash. Each block not only contains the content of the transaction and timestamp but also references the hash of its previous block. These blocks are linked by reference hash and then superimposed into a "chain" in chronological order to create a blockchain. A blockchain network is a peer-to-peer network composed of a group of nodes. Each node operates the same blockchain through its own copy. The blockchain is a distributed data structure that is copied and shared among network members. We assume that each user conducts transactions on the network through miners (i.e., nodes). The literature [26] summarizes that the operations of nodes in a blockchain network follow the below steps:

(1) The user interacts with the blockchain through a pair of private/public keys. When initiating a transaction, the transaction initiator needs to sign the transaction with a private key, and those transactions are addressable on the network through the initiator's public key. When a new transaction is generated, it

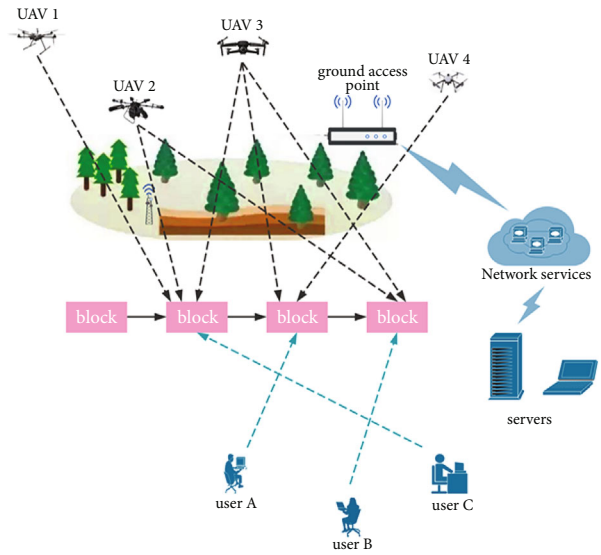


Figure 1: System architecture.

will be broadcast to other participating nodes in the blockchain network

(2) After the transaction is broadcast to the entire network, within an agreed time interval, each node will collect several unverified transactions and hash them into a time-stamped block. Each block can contain hundreds or thousands of transactions

(3) Each node performs a Proof-of-Work (PoW) calculation equivalent to solving a mathematical problem to determine who can verify the transaction. Letting the fastest node in calculation do the job is the way to achieve consensus. The node with the fastest PoW calculation will propagate its own block to other nodes. This calculation process is a "mining" process to derive the effective hash of the new block

(4) The node that obtained the verification right broadcasts the block to all nodes, and other nodes will confirm whether the transactions contained in this block are valid. If valid, add this block to the blockchain and apply the transactions it contains to update the world view of all nodes. Otherwise, this block will be discarded. Once the block is accepted by the blockchain, the transactions contained in the block are part of the blockchain and cannot be changed in any way

(5) Once all nodes accept the block, the blocks that have not previously completed the PoW work will be invalidated, and each node will reestablish a block to continue the next PoW calculation work

In essence, a smart contract refers to a piece of conditional statement code that runs on the blockchain. When two parties of a smart contract generate an asset transaction on the blockchain, this piece of code is triggered to automatically complete the specific transaction process. Smart contracts are special accounts on the blockchain, which contain addresses, balances, status, and codes. The address is a unique identifier for the account, just like a regular user account. The smart contract works as follows:

(1) Construction of smart contracts: smart contracts are jointly formulated by multiple users in the blockchain and can be used for any transaction behavior between any users. A contract clearly stipulates the rights and obligations of both parties to the transaction electronically. The code contains conditions that will trigger the automatic execution of the contract. All possible results of the contract should be described in the smart contract

(2) Storage smart contracts: once the coding is completed, the smart contract is uploaded to the blockchain network; that is, all nodes on the entire network can receive the contract

(3) Executing smart contracts: the smart contract will periodically check whether there are related events and trigger conditions and push the events that meet the conditions to the queue to be verified. The verification node on the blockchain first performs signature verification on the event. After most nodes reach a consensus on the event, the smart contract will be successfully executed and the users will be notified. The execution result of a smart contract must be deterministic; that is, the same input always produces the same output. Because all interactions with the contract are performed through signed messages on the blockchain, all network participants can obtain the cryptographically verifiable trace of the contract's operations

4. System Model

The architecture of the proposed blockchain-based signal source identification system is shown in Figure 2. There are three roles: miners, initiators, and participants. In the system, participants have backbone ground edge units to support UAV manipulating, data processing, negotiating with miners, and transmitting data to initiators.

Miner: the *miner* is a trusted and authenticated node that has multiple roles. First, it acts as a broker between initiators and participants. It accepts requests from initiators and matches them with participants. Second, it is a maintainer of the stable operations in the blockchain system which packages all kinds of data and smart contracts onto the blockchain. There could be a few miners, such as servers of the different public third-party platforms, in a real scenario.

Initiator: the *initiator* refers to the users in Section 2. The object detection or signal source identification task is launched by the initiator. Then, the initiator sends this task to the miner and waits for the assignment and draft smart contract. Smart contract and data related to the transaction will be handed to the miner to write onto the blockchain. Detection data will be returned by participants directly.

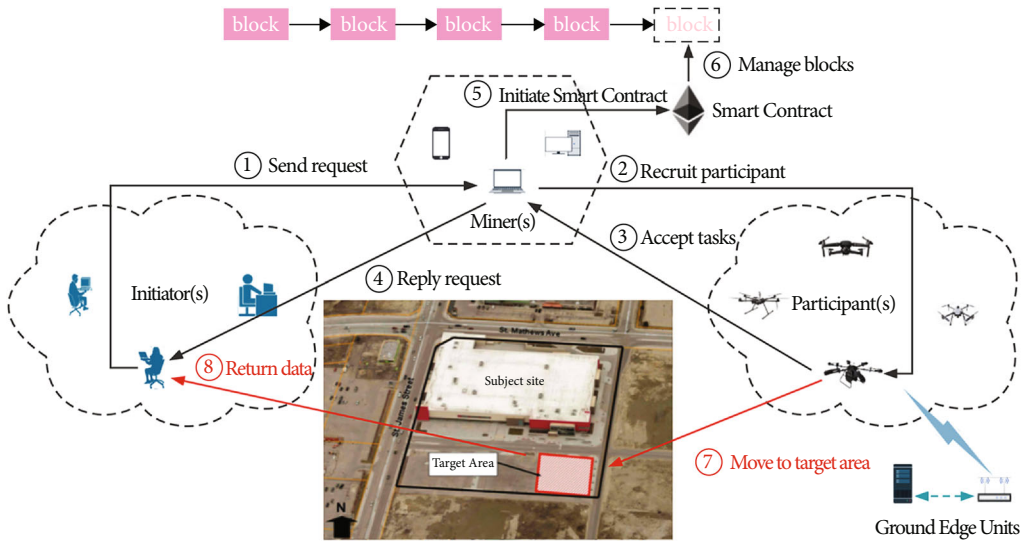


Figure 2: The proposed system model.

Finally, the initiators make payment through the blockchain by using digital currency.

Participant: the *participant* refers to the UAV. It is controlled by a ground edge unit. The participant can evaluate the recruitment from the miner and accept the task. It reads the parameters related to the object identification task and the smart contract from the blockchain. Then, it flies to the target area and sends the computation results to the initiator.

After matching and agreement on the smart contract, the object detection and signal source identification task is technically carried out in three major steps, i.e., visual-based object detection and tracking, binocular depth estimation, and wireless signal-aerial image fusion-based signal source identification. The flow chart of the method is shown in Figure 3.

4.1. Blockchain and Smart Contract. The design goals of introducing blockchain and smart contract lie in two aspects:

4.1.1. Reliable Collaboration. We need to ensure the authenticity and reliability of initiators and participants. To this end, the blockchain guarantees that the synchronization and consistency of quality of service (QoS) of each UAV, and the payment is correctly made by the user.

4.1.2. Security and Privacy. We assume that the initiator and participants are all semihonest nodes who obey the agreement and honestly execute the tasks. However, they may want to probe into others' data, either individually or collusively. On the other hand, both sides do not want to expose their identities. Therefore, the proposed blockchain-based architecture combines secure schemes such as asymmetric key cryptography, ring signature, and consensus mechanism. All the operations are performed in a privacy-preserving manner.

According to Figure 2, there are totally eight steps for the whole process.

Step 1. The initiator sends its task requirement and remuneration offering to the miner which is encrypted by its private key and with ring signature.

Step 2. The miner decrypts the requirement and recruits the participant with an optimal matching algorithm according to predefined conditions. The offer is sent with the encryption of the miner's private key.

Step 3. The participant decrypts the offer and chooses to accept or deny it in his own interest. If accepted, its parameters and the public key will be encrypted with the miner's public key and then sent back to the miner.

Step 4. The miner then answers the initiator with the information of the participant in an encryption manner.

Step 5. Then, a smart contract between the initiator and the participant is created in both parties' confirmation.

Step 6. The smart contract is deployed in the blockchain framework. The miner also builds a secure channel and provides a pair of keys for data exchange of both parties.

Step 7. After receiving the parameters of the task from the initiator (a user) via the secure channel, the participant (a UAV) flies to the target area and performs the identification task.

Step 8. When the task is completed, the result will be returned to and validated by the initiator via the secure channel. Finally, the payment is made using digital currency according to the smart contract.

4.2. Object Detection and Object Tracking. The visual target detection and tracking part mainly complete the subtask of tracking and identification of specific types of targets within the UAV field of view. Target detection is one of the key technologies to improve the perception capability of UAVs and is of great significance. Compared with the traditional methods based on manual features, the deep learning methods based on convolutional neural networks have powerful feature learning and expression capabilities and become the mainstream algorithms for target detection tasks at present [27].

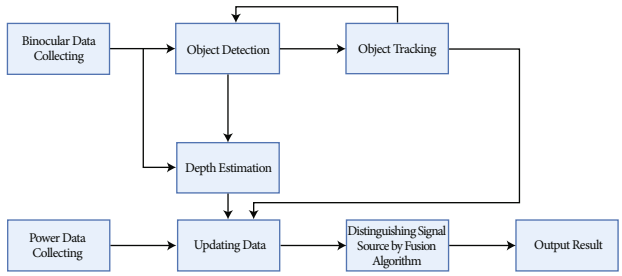


FIGURE 3: The flow chart of the wireless signal-aerial image fusion-based signal source identification.

Aerial photography generally has the following characteristics because the imaging perspective is different from natural scene images.

(i) Complex background

(ii) Small targets

(iii) Large field of view

(iv) Rotation

Inspired by [27], the visual target detection part adopts the YOLO-based target detection framework [28], and on this basis, the algorithm is optimized and adjusted based on the characteristics of UAV data collection and the difficulties of recognition, via the drone vehicle datasets [29] and DOTA datasets [30], as shown in Figure 4. For the target tracking part, the Deep SORT algorithm [31] is used to predict the movement probability of the object and calculate the difference between the front and back frame features of the object and then complete the continuous tracking of the target.

We perform data augmentation for both datasets of images. Data augmentation is a technique that artificially extends the training dataset by allowing limited data to produce more equivalent data. It is an effective means to overcome the shortage of training data. We mainly use random rotation, color transformation, blurring, noise injection, and hybrid image processing to enhance the diversity of the input data. Then, the YOLO pretraining network is trained using the enhanced data to fine-tune the weights of the convolutional layer parameters and migrate the object recognition task from the ground view to the object recognition task in the UAV view.

In the overall system, the signal source identification algorithm needs to take the visual detection result and the corresponding object ID as input; thus, we add a tracking algorithm in addition to YOLO's object recognition to ensure that each detected object corresponds to its ID. As an algorithm commonly used in Multiobject Tracking (MOT), Deep SORT is a detection-based tracking method of good performance and high industrial interest. The main process of the MOT algorithm is as follows:

(1) Given the original video frame, run a target detector such as YOLO for detection and obtain target detection frames

(2) Take out the interested targets in all target frames and perform feature extraction (including apparent features and motion features)

(3) Perform similarity calculation to calculate the matching degree between the targets in the front and back frames (the distance between the features belonging to the same target before and after is relatively small, and the distance between different targets is large)

(4) Associate the data, and assign the ID of the target to each object

4.3. Binocular Depth Estimate. The binocular depth estimate part is to complete the subtask of estimating the depth to the identified object, i.e., the distance of a UAV equipped with a binocular camera to the identified target object.

In this work, we choose the SGBM algorithm to estimate the depth between objects and the camera [32]. Firstly, the binocular disparity d measures the horizontal disparity of the surface point on the target object between the video frame taken by the left camera x_L and the right camera x_R is estimated by energy optimization [33] as shown in

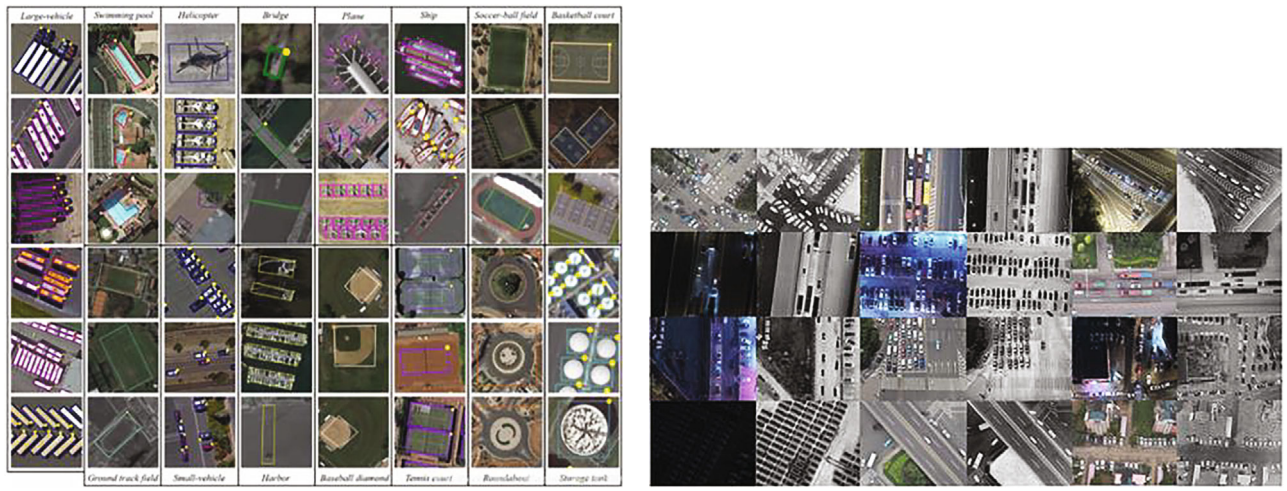
$$d = |x_L - x_R|. \tag{1}$$

Then, the obtained disparity map is converted into a depth map based on the relationship between disparity and depth. Finally, the distance from the target to the camera is extracted from the depth map. More specifically, the disparity value of each pixel is calculated with respect to the right eye view using the left eye view as the reference. We construct an energy function $E(D)$ to estimate the optimal disparity image D by minimizing the energy value using the following equation:

$$E(D) = \sum_p C(p, D_p) + \sum_{q \in N_p} P_1 I\left[\left|D_p - D_q\right| = 1\right] + \sum_{q \in N_p} P_2 I\left[\left|D_p - D_q\right| > 1\right]. \tag{2}$$

The first term is the sum of matching cost for every pixel in the disparity image D corresponding to the captured left video frame. $C(p, D_p)$ is the pixel-wise matching cost function with disparity D_p corresponding to the minimum cost for pixel p. In the current implementation, the matching cost value is calculated based on Mutual Information (MI) [34]. The second term adds a constant penalty P_1 for all pixels q in the neighborhood N_p of p, if the disparity between p and q is 1, while the third term adds a larger constant penalty P_2 if the disparity between p and q is larger than 1. Operator $I[X]$ equals 1 if event X occurs; otherwise, it equals 0. Constant P_2 is chosen larger than P_1.

Based on the mapping between disparity and depth value, the depth image according to the left-view video frame can be evaluated. The depth information of the surface point on the target object using disparity value is computed as follows:



(a) (b)

Figure 4: Two datasets for UAV object detection: (a) from drone vehicle datasets; (b) from DOTA datasets.

$$Z = \frac{b \cdot f}{d}, \tag{3}$$

where b is the baseline of the binocular camera and f is the camera focal length.

To obtain the distance between the target object and the camera, the bounding box of the object in the video frame needs to be computed based on the object detection and tracking algorithm. The pixels within the bounding box are sampled at an interval of 2 to 5 pixels, and the depth value is indexed from the corresponding depth map. The average depth value of the sampled pixels is then used to represent the actual distance from the object to the camera.

4.4. Fusion Object Detection. So far, we have found a number of suspicious objects distributed in the area, which are similar in appearance. Suppose that only one of them is the real object which is communicating with the outside world at a fixed wireless frequency band, and we need to identify it. Some existing works utilize a wireless network between UAVs and objects to help localization [35, 36]. However, in both cases, the information of the target is known beforehand. The wireless connection is only used to transmit data, power, and arrival of time for distance calculation. To this end, the proposed method utilizes a UAV equipped with a binocular camera to obtain the distances between the object and the UAV at some measurement points of the trajectory, by applying binocular depth estimation after using deep learning-based target detection. At the same time, the received power is obtained utilizing the UAV onboard SDR. As shown in Figure 5, the UAV moves simultaneously along the path until the desired data has been collected.

Let S denote the set of objects that the UAV detected in the flight area. Arbitrarily select an object $s \in S$ and take it as the source target sending signals. Then, let the received power p_n measured by the UAV at position n be as same as p_{sn} (assume that only s is the transmitting signal and note that s is anonymous to the UAV) and the distance estimated

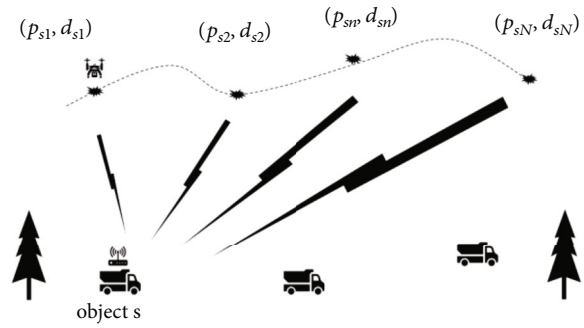


Figure 5: Problem formulation of signal source identification.

by binocular depth estimation at position n be d_{sn}. The two types of data collected during the flight have a correspondence such that the received power from the object s measured at N positions constitutes a vector $\mathbf{p}_s$, and the binocular depth estimated distance of the object s measured at N positions constitutes a vector $\mathbf{d}_s$, as shown in

$$\mathbf{d}_s = [d_{s1}, d_{s2}, \cdots, d_{si}, \cdots, d_{sN}]^T, \tag{4}$$

$$\mathbf{p}_s = [p_{s1}, p_{s2}, \cdots, p_{si}, \cdots, p_{sN}]^T. \tag{5}$$

Consider that the received wireless signal power satisfies the path loss log-normal shadowing model [37].

$$p = p_0 - 10\alpha \lg \frac{d}{d_0} + X_\sigma, \tag{6}$$

where p is the received power in dB at distance d from the object, p_0 is the received power in dB at distance d_0 from the object, α is the path loss exponent, and X_σ is the environment-dependent shadow fading coefficient which obeys the Gaussian distribution with zero mean and variance σ^2.

To determine whether object s is sending signals, the distance vector $\mathbf{d}_s$ and power vector $\mathbf{p}_s$ of object s can be substituted into the path loss log-normal shadowing model

to determine if they match the model well. In the case that the parameters p_0 and α in the log-normal model are unknown, they (when s is assumed to be the target object) need to be calculated first. By utilizing maximum likelihood estimation, the procedure for evaluating the parameters of the path loss log-normal shadowing model for object s is as follows.

Let the reference distance d_0 in the path loss log-normal shadowing model be equal to 1 m, implying that p_0 is the received power at a reference distance of 1 m. Since p is subject to Gaussian distribution with mean $p_0 - 10\alpha \lg d$ and variance σ^2, we can define the following likelihood function:

$$L(p_0, \alpha, \sigma^2) = \prod_{n=1}^{N} \frac{1}{\sqrt{2\pi}\sigma} \exp\left\{ -\frac{[p_{sn} - (p_0 - 10\alpha \lg d_{sn})]^2}{2\sigma^2} \right\}. \tag{7}$$

Taking the likelihood function logarithmically, we can obtain

$$\ln L(p_0, \alpha, \sigma^2) = N \ln \frac{1}{\sqrt{2\pi}\sigma} - \sum_{n=1}^{N} \frac{[p_{sn} - (p_0 - 10\alpha \lg d_{sn})]^2}{2\sigma^2}. \tag{8}$$

Then, to calculate the maximum likelihood estimate of the parameters, we can derive equation (8) and find p_0, α, and σ^2, such that the partial derivatives are zero, i.e.,

$$\frac{\partial \ln L}{\partial p_0} = -\sum_{n=1}^{N} \frac{[p_{sn} - (p_0 - 10\alpha \lg d_{sn})]}{\sigma^2} = 0, \tag{9}$$

$$\frac{\partial \ln L}{\partial \alpha} = \lg d_n \sum_{n=1}^{N} \frac{[p_{sn} - (p_0 - 10\alpha \lg d_{sn})]}{\sigma^2} = 0, \tag{10}$$

$$\frac{\partial \ln L}{\partial \sigma^2} = -\frac{1}{2} N \frac{1}{\sigma^2} + \frac{1}{2} \frac{1}{\sigma^4} \sum_{n=1}^{N} [p_{sn} - (p_0 - 10\alpha \lg d_{sn})]^2 = 0. \tag{11}$$

After calculation, we can obtain the following estimates for p_0, α, and σ^2:

$$\widehat{p}_0 = \bar{p} + 10\widehat{\alpha}\bar{d}_{sn}, \tag{12}$$

$$\widehat{\alpha} = \frac{\sum_{n=1}^{N} -1/10(\lg d_{sn} - \bar{d}_{sn})(p_{sn} - \bar{p})}{\sum_{n=1}^{N} (\lg d_{sn} - \bar{d}_{sn})^2}, \tag{13}$$

$$\widehat{\sigma^2} = \frac{1}{N} \sum_{n=1}^{N} [p_{sn} - (\widehat{p}_0 - 10\widehat{\alpha} \lg d_{sn})]^2, \tag{14}$$

where

$$\bar{p} = \frac{1}{N} \sum_{n=1}^{N} p_{sn}, \tag{15}$$

$$\bar{d}_{sn} = \frac{1}{N} \sum_{n=1}^{N} \lg d_{sn}. \tag{16}$$

Using the parameters obtained from the maximum likelihood estimation $\widehat{p}_0$ and $\widehat{\alpha}$, we can obtain the fitted value of the received power $\widehat{p}_{sn}$ according to equation (6) as

$$\widehat{p}_{sn} = \widehat{p}_0 - 10\widehat{\alpha} \lg d_{sn}. \tag{17}$$

To measure the extent to which object s conforms to the path loss log-normal shadowing model, we choose the mean squared error (MSE) of the fitted received power and the measured received power as the metric. Then, the MSE of object s is defined as

$$\mathrm{MSE}_s = \frac{1}{N} \sum_{n=1}^{N} (\widehat{p}_{sn} - p_{sn})^2. \tag{18}$$

After the UAV detects all objects in the flight area, it compares the MSE of all objects and identifies the object with the smallest MSE as the source target, i.e.,

$$\text{Source target} = \arg \min_{s \in S} \mathrm{MSE}_s. \tag{19}$$

In summary, the fusion-based signal source identification algorithm is shown in Algorithm 1.

4.5. Hardware Implementation. We also build a testbed to evaluate the system performance. The hardware component list is described in Table 1.

The experiment system consists of two major parts, the air system and the ground system, as seen in Figure 6. The air system contains various UAVs (in our case, hexacopter UAVs loaded with Raspberry 4Pi B model, which links the binocular camera and the SDR by a USB cable and communicates with the ground system through Wi-Fi). The ground system includes a laptop with a discrete GPU, in which the costly computations are conducted, and a Wi-Fi AP to connect all devices through wireless communications. The laptop is also responsible for simulating the miner in the blockchain network. We use smartphones to play the role of the initiator. All tasks are launched from smartphones. The UAV system is shown in Figure 7. The Raspberry Pi 4 and SDR are mounted in the UAV, and the camera is tied in angle to the ground.

5. Result and Analysis

We used semiphysical simulation to verify the effectiveness of the fusion algorithm. First, we used SDR on the ground to collect power data at different positions, and then, we calculated the path loss coefficient of the actual channel and the received power at a reference distance of 1 m by linear regression. As shown in Figure 8, the object was a USRP B210 device from Ettus Corp, and diagrams for transmitting were written in GNU Radio software. The waveform of the signal was a periodic sine waveform, and the transmitter frequency was set to 907 MHz-927 MHz, the power was set

Input: objects set S=Ø, initiate corresponding distance data vector d_s=Ø, power data vector p_s=Ø
Output: signal source target
1. while UAV keeps flying do
2. if new object *s'* is detected then
3. do S = S ∪{*s'*}
4. end if
5. obtain current power *p* from SDR measurement
6. for *s* in S do
7. obtain current distance *d* of object *s* from binocular depth estimate
8. if *d* and *p* is valid then
9. update *d* and *p* to the end of d_s and p_s
10. end if
11. end for
12. if data achieves certain amounts then
13. target = *None*
14. for *s* in S do
15. calculate $\hat{p}_0$ and $\hat{\alpha}$ of object *s*
16. calculate MSE_s
17. update target by comparing *MSE*
18. end for
19. end if
20. end while

Algorithm 1: Fusion-based signal source identification.

Table 1: Hardware components.

Component		Parameter
UAV air system	Computer	Raspberry Pi 4B
	Camera	Metoak binocular camera
	UAV	Hexacopter Tarot UAV
	SDR	Hackrf One
Ground MEC system	Laptop	Lenovo Legion 7
	Wi-Fi	TP-LINK war1200

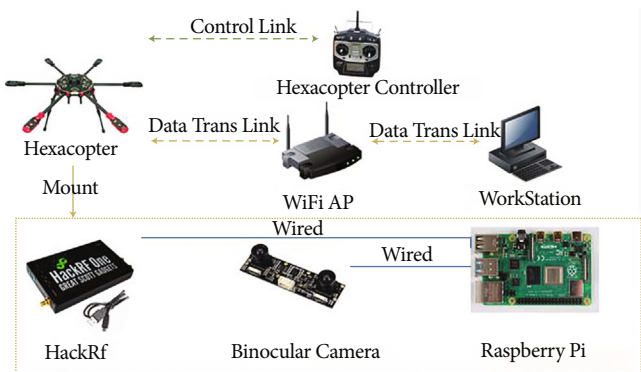


Figure 6: Experiment system architecture. The dashed double arrow lines show the communications between devices.

to 1 W, and the transmitting gain of the antenna was 50 dB. The object was placed at 1.7 m from the ground to simulate the signal propagation in the air as high as possible. We measured the data at each 1 m interval on the ground, and the distance range from the source was from 1 m to 30 m. The experiment was repeated 10 times, and the total received power values were obtained for 300 locations. Figure 9 shows the measured power and distance. After calculation, we obtained $p_0 = -28.91$ dBm, $\alpha = 3.581$, and $\sigma^2 = 23.49$.

5.1. Security Analysis. In our system, all participants and initiators are assumed to be semihonest nodes. Based on this assumption, we are going to analyze the security objectives in this section.

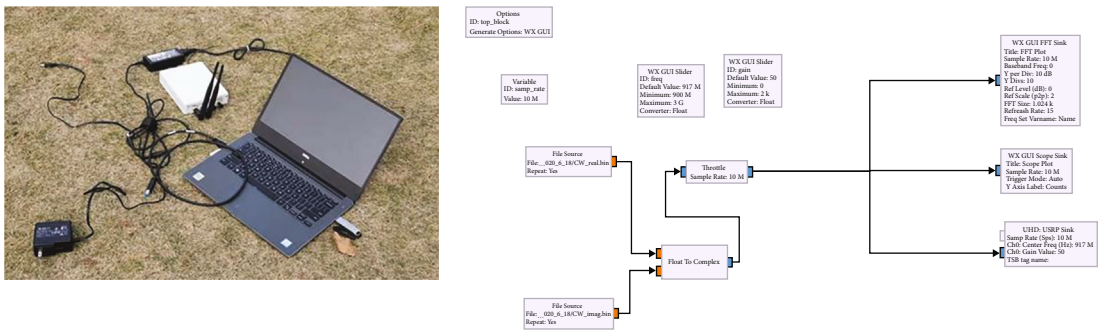
5.1.1. Anonymity between Initiators and Participants. To hide the identities of both the initiator and participants, we use the ring signature proposed by Rivest et al. [38]. The ring signature can hide the real signer. And if the asymmetric encryption function is used in the signature, the security of the signature can be enhanced. The ring signature in our system is based on the asymmetric encryption function.

5.1.2. Data Security. All data segments are encrypted with the receiver's public key; without the receiver's private key, the attacker cannot crack the cryptosystem and obtain the encrypted data segments. At the same time, the key exchange and data communication are through the secure channel created by the miner, which enhances the security.

5.2. Performance of Semiphysical Simulation. We first placed the objects randomly in an area with the size of 30 m × 40 m, generated the coordinates of the objects, and selected an object as the source target. After that, we generated a sequence of N coordinates at uniform intervals of 1 m according to the distance to the object. This sequence is the coordinate sequence of the simulated flight path of the UAV. Then, according to the measured channel parameters, the source distance was substituted into the path loss log-

(a) (b)

Figure 7: The proposed UAV system: (a) the assembled UAV; (b) the ground MEC system.



(a) (b)

Figure 8: Experiment system implementation: (a) USRP B210; (b) GNU radio block diagrams.

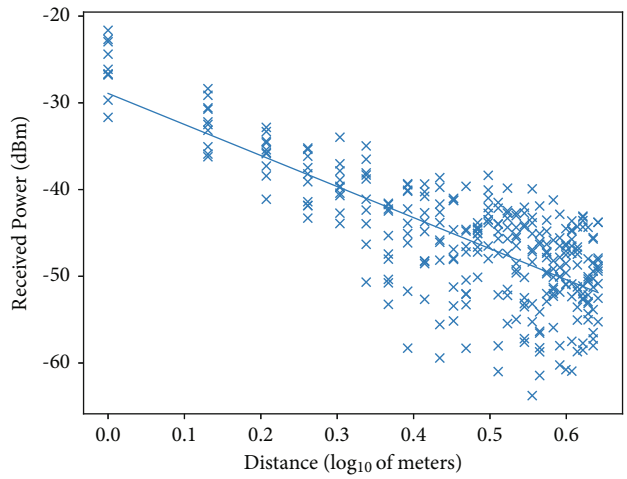


Figure 9: Distance versus power.

normal shadowing model to generate the corresponding measured power value. Next, for all objects, the distance was calculated based on the coordinates of the UAV flight path and the distance of the object coordinates. Noting that the UAV flight passed through N points, we set up an object distance vector with a size of N, as well as a power vector. Figure 10 shows the identification accuracy of the proposed fusion method under different numbers of potential objects. When the number of objects is 2, the accuracy decreases slightly with the increase in experimental rounds and finally reaches a stable value about 70%. When the number of objects is 3, the accuracy also decreases slightly with the increase in experimental rounds and then increases gradually until it is stable at about 53%. We attribute this small fluctuation to the influence of random factors. In the above, we mentioned that objects were randomly placed in the area, and the signal source was randomly selected; a Gaussian noise would also be added when using the log-normal shadowing model to generate the received power at different distances, which would affect the discrimination of objects and then the accuracy. The reason for the decrease in accuracy against the number of objects is that, within the limited

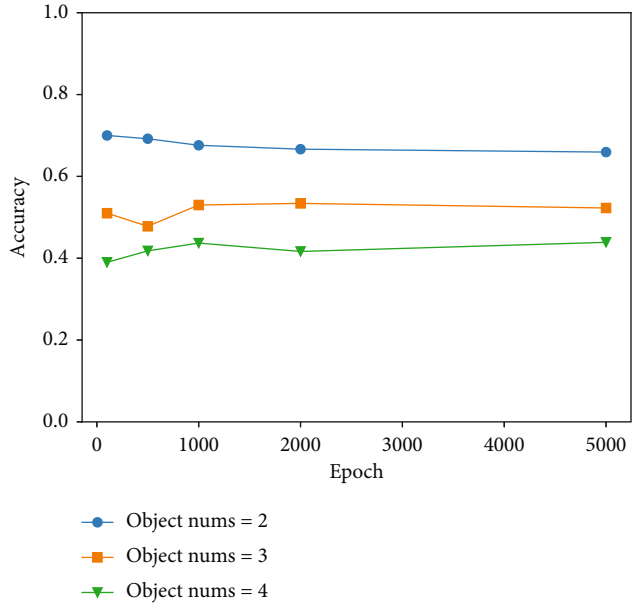


Figure 10: Accuracy under different numbers of objects.

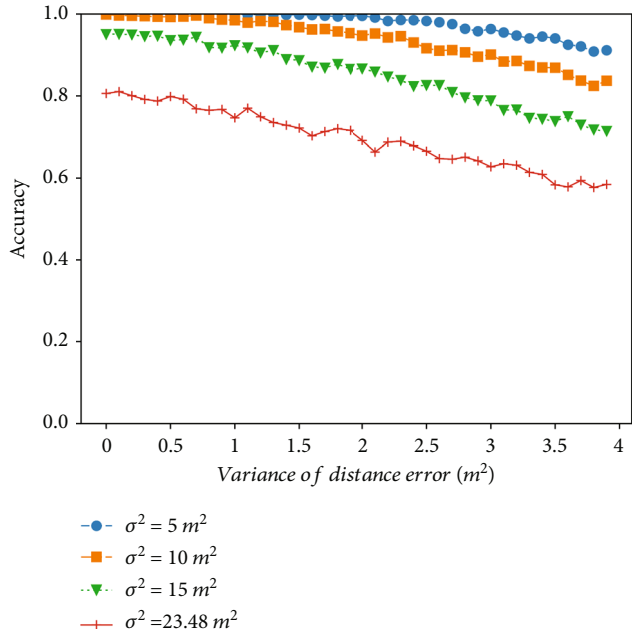
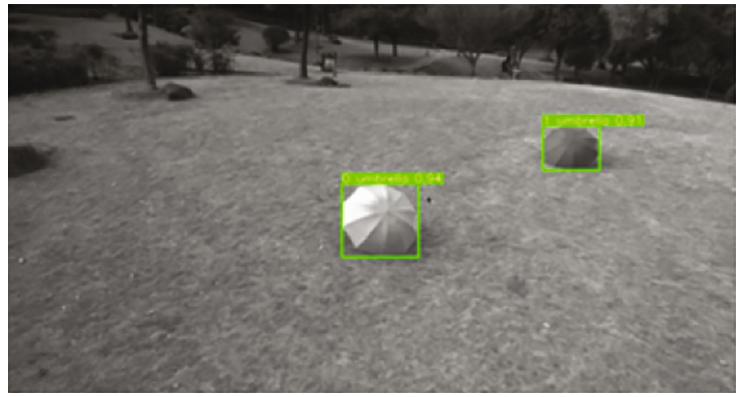


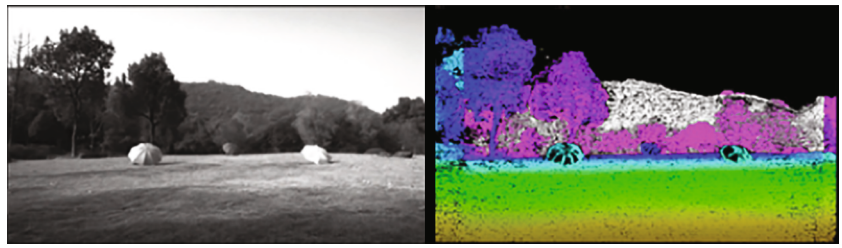
Figure 11: Sensitivity under different distance errors.

area, the increase in the number of objects will also increase the possibility that they have similar distance to the UAV, and thus, the trend of distance versus power change between them tends to be similar.

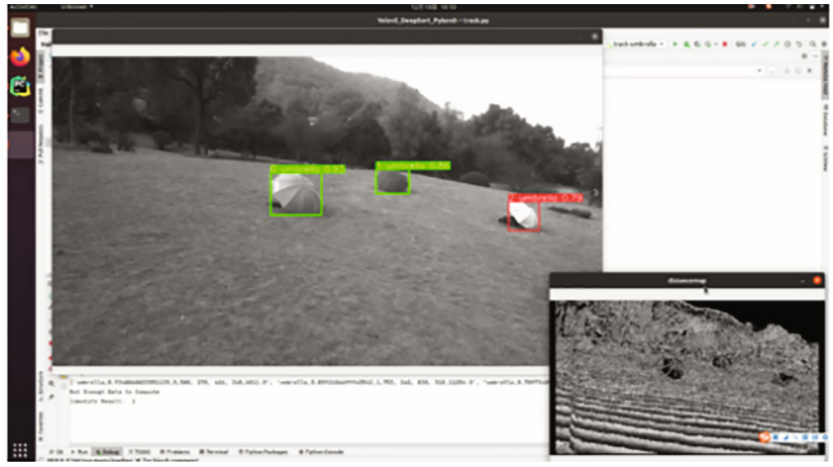
5.3. System Sensitivity Analysis. Figure 11 shows the sensitivity of the fusion method regarding the change of parameters and the depth distance error obtained by the binocular vision in the log-normal model. σ^2 is the variance of the noise mentioned above. The variance indicates the stability of the channel or the received signal-to-noise ratio to a certain extent. To explore the influence of variance on the accuracy of the method, we selected three synthetic and one measured values for experimental simulation. Here, the number of objects was set to 3, the distance between objects was 5 m, the number of experiments was 2000, and the number of distance-received power pairs collected for each experiment was 30. The horizontal coordinate was the variance of the distance error for each measurement in square meter. The four curves indicate the detection accuracy of the fusion



(a)



(b)



(c)

Figure 12: Experiment results: (a) two umbrellas detected; (b) the depth graph; (c) successfully distinguishing the signal source (see the red anchor box).

algorithm when the variance of the shadow fading is set to 5, 10, 15, and 23.48, respectively, while the distance error increases from 0 to 4.0 meters.

When the variance is small, in another word, when the signal-to-noise ratio is high, the discrimination accuracy of the method is high. When σ^2 is equal to 5, the channel is ideal and the accuracy is close to 1.0. With the gradual increase in variance, the accuracy also begins to decline. When σ^2 exceeds 15, the accuracy begins to decline significantly. It is preliminarily inferred that the value of 15 should be a critical point of the method. Also, when the distance error increases, the accuracy decreases gradually. The calculation shows that when the distance error is 4, it will be 2 m different from the real distance in extreme cases. When the object spacing is 5 m, the error will greatly reduce the accuracy. In practice, the distance error estimated by binocular vision is around 1 m, so the accuracy of this method is high enough in real-world applications.

5.4. Physical Experiment. We also launched the UAV to the air to verify our system. The experiment was held on a lawn, and the objects were simply 3 umbrellas, each was placed 3 m away from the other. The whole system worked well, when the 3 umbrellas were in the sight of the camera. By controlling the moving path of the UAV, we got some data. Despite those limitations, the accuracy was very close to the simulation result. Figure 12 shows the setup of the experiment and the real-time output of the system.

6. Conclusion

In this paper, we proposed a signal source identification algorithm to distinguish the target by a blockchain and UAV-enabled system. We used binocular cameras to detect candidate objects and corresponding distances. With the measuring of the received signal strength and mobile edge computing, finally, we used fused object identification techniques to determine the real target object. Blockchain and smart contract technologies were adopted to organize UAVs and users, aimed at providing reliability and security. The accuracy of discrimination could reach 70% for 2 objects and 53% for 3 objects in a semiphysical simulation. The real-world experiment showed the feasibility of the system, and the performance was close to that in the semiphysical simulation.

Regarding future directions for this work, first, satellite positioning (such as GPS and BeiDou) can be utilized to give precise location information of the signal source after identification. Second, only one signal source is considered in this paper; the method will be extended to support multiple signal sources in the future work.

Data Availability

Data is available on request; please contact the corresponding author Huaming Lin (lhm18@live.cn).

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Authors' Contributions

Jian Xiao, Peng Liu, and Huijuan Lu contribute to implementation of wireless signal-aerial image fusion. Huaming Lin and Yi Huang contribute to system architecture design. Hangxiang Fang, Hangguan Shan, and Haoji Hu contribute to object detection and object tracking. Jiayi Xu contributes to binocular depth estimate.

Acknowledgments

This work was supported in part by the Open Project Funding of the Key Laboratory of Electromagnetic Wave Information Technology and Metrology of Zhejiang Province (No. 2020KF0001) and the Natural Science Foundation of China (Grant Nos. 62172134 and 62102125).

References

[1] K. M. Almgren, A. Olofsson, and S. Magnusson, *Radio Signal Source Identification System*, EP, 2001.

[2] Z. Li, A. Giorgetti, and S. Kandeepan, "Multiple radio transmitter localization via UAV-based mapping," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 9, pp. 8811–8822, 2021.

[3] Y. Li, F. Shu, B. Shi, X. Cheng, Y. Song, and J. Wang, "Enhanced RSS-based UAV localization via trajectory and multi-base stations," *IEEE Communications Letters*, vol. 25, no. 6, pp. 1881–1885, 2021.

[4] M. Calì and R. Ambu, "Advanced 3D photogrammetric surface reconstruction of extensive objects by UAV camera image acquisition," *Sensors*, vol. 18, no. 9, p. 2815, 2018.

[5] D. Wierzbicki, "Multi-camera imaging system for UAV photogrammetry," *Sensors*, vol. 18, no. 8, p. 2433, 2018.

[6] J. Mäkynen, C. Holmlund, H. Saari, K. Ojala, and T. Antila, "Unmanned aerial vehicle (UAV) operated megapixel spectral camera," in *Electro-Optical Remote Sensing, Photonic Technologies, and Applications*, vol. 8186, International Society for Optics and Photonics, 2011.

[7] R. J. Moore, S. Thurrowgood, D. Bland, D. Soccol, and M. V. Srinivasan, "A stereo vision system for UAV guidance," in *in 2009 IEEE/RSJ International Conference on Intelligent Robots and Systems*, pp. 3386–3391, St. Louis, MO, USA, 2009.

[8] Y. Yu, T. Wang, C. Long, and W. Zhang, "Stereovision based obstacle avoidance strategy for quadcopter UAV," in *in 2018 Chinese Control And Decision Conference (CCDC)*, Shenyang, China, 2018.

[9] Y. M. Mustafah, A. W. Azman, and F. Akbar, "Indoor UAV positioning using stereo vision sensor," *Procedia Engineering*, vol. 41, pp. 575–579, 2012.

[10] R. Fan, J. Jiao, J. Pan, H. Huang, and M. Liu, "Real-time dense stereo embedded in a UAV for road inspection," in *in 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, Long Beach, CA, USA, 2019.

[11] K. N. Tahar, A. Ahmad, and W. A. A. W. M. Akib, "UAV-based stereo vision for photogrammetric survey in aerial terrain mapping," in *in 2011 IEEE International Conference on Computer Applications and Industrial Electronics (ICCAIE)*, pp. 443–447, Penang, Malaysia, 2011.

[12] K. Vonehr, S. Hilaski, B. E. Dunne, and J. Ward, "Software defined radio for direction-finding in UAV wildlife tracking," in *in IEEE International Conference on Electro Information Technology*, Grand Forks, ND, USA, 2016.

[13] A. Torabi, M. W. Shafer, G. S. Vega, and K. M. Rothfus, "UAV-RT: an SDR based aerial platform for wildlife tracking," in *in2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, pp. 1–6, Chicago, IL, USA, 2018.

[14] S. O. Murphy, C. Sreenan, and K. N. Brown, "Autonomous unmanned aerial vehicle for search and rescue using software defined radio," in *in Vehicular Technology Conference*, Kuala Lumpur, Malaysia, 2019.

[15] Z. Du, C. Wu, T. Yoshinaga et al., "A routing protocol for UAV-assisted vehicular delay tolerant networks," *IEEE Open Journal of the Computer Society*, vol. 2, pp. 85–98, 2021.

[16] D. Ebrahimi, S. Sharafeddine, P. H. Ho, and C. Assi, "Autonomous UAV trajectory for localizing ground objects: a reinforcement learning approach," *IEEE Transactions on Mobile Computing*, vol. 20, no. 4, pp. 1312–1324, 2021.

[17] S. Wu, "Illegal radio station localization with UAV-based Q-learning," *China Communications*, vol. 15, no. 12, pp. 122–131, 2018.

[18] X. Chen, C. Wu, T. Chen et al., "Information freshness-aware task offloading in air-ground integrated edge computing systems," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 1, pp. 243–258, 2022.

[19] L. Qiao, S. Dang, B. Shihada, M. S. Alouini, and Z. Lv, "Can blockchain link the future?," *Digital Communications and Networks*, 2021.

[20] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K. K. R. Choo, "A systematic literature review of blockchain cyber security," *Digital Communications and Networks*, vol. 6, no. 2, pp. 147–156, 2020.

[21] A. Kapitonov, S. Lonshakov, A. Krupenkin, and I. Berman, "Blockchain-based protocol of autonomous business activity for multi-agent systems consisting of UAVs," in *in 2017 Workshop on research, education and development of unmanned aerial systems (RED-UAS)*, pp. 84–89, Linköping, Sweden, 2017.

[22] A. I. Abhi and S. Y. Shin, "BUS: a blockchain-enabled data acquisition scheme with the assistance of UAV swarm in Internet of things," *IEEE Access*, vol. 7, pp. 103231–103249, 2019.

[23] A. S. Khan, G. Chen, Y. R. Bschons, G. Zheng, and S. Lambotharan, "Trusted UAV network coverage using blockchain, machine learning, and auction mechanisms," *IEEE Access*, vol. 8, pp. 118219–118234, 2020.

[24] S. Rakesh, B. Rojeena, and P. S. Anish, "A new type of blockchain for secure message exchange in VANET," *Digital Communications and Networks*, vol. 6, no. 2, pp. 177–186, 2020.

[25] Z. Liu, C. Zhan, Y. Cui, C. Wu, and H. Hu, "Robust edge computing in UAV systems via scalable computing and cooperative computing," *IEEE Wireless Communications*, vol. 28, no. 5, pp. 36–42, 2021.

[26] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[27] M. H. Mughal, M. J. Khokhar, and M. Shahzad, "Assisting UAV localization via deep contextual image matching," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 4, pp. 2445–2457, 2021.

[28] A. Bochkovskiy, C.-Y. Wang, and H.-Y. M. Liao, "Yolov4: optimal speed and accuracy of object detection," 2020, arXiv preprint arXiv:2004.10934.

[29] P. Zhu, Y. Sun, L. Wen, Y. Feng, and Q. Hu, "Drone based RGBT vehicle detection and counting: a challenge," 2020, arXiv preprint arXiv:2003.02437.

[30] G. S. Xia, X. Bai, J. Ding et al., "DOTA: a large-scale dataset for object detection in aerial images," in *in 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*, Salt Lake City, UT, USA, 2018.

[31] N. Wojke, A. Bewley, and D. Paulus, "Simple online and realtime tracking with a deep association metric," in *in 2017 IEEE International Conference on Image Processing (ICIP)*, Beijing, China, 2017.

[32] H. Hirschmuller, "Stereo processing by semiglobal matching and mutual information," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 30, no. 2, pp. 328–341, 2008.

[33] Y. Boykov, O. Veksler, and R. Zabih, "Fast approximate energy minimization via graph cuts," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 23, no. 11, pp. 1222–1239, 2001.

[34] P. Viola and W. M. Wells, "Alignment by maximization of mutual information," *International Journal of Computer Vision*, vol. 24, no. 2, pp. 137–154, 1997.

[35] Y. Zhao, Z. Li, N. Cheng, B. Hao, and X. Shen, "Joint UAV position and power optimization for accurate regional localization in space-air integrated localization network," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4841–4854, 2021.

[36] M. Atif, R. Ahmad, W. Ahmad, L. Zhao, and J. J. P. C. Rodrigues, "UAV-assisted wireless localization for search and rescue," *IEEE Systems Journal*, vol. 15, no. 3, pp. 3261–3272, 2021.

[37] S. Rouhollah and Z. Hadi, "RSS localization using unknown statistical path loss exponent model," *IEEE Communications Letters*, vol. 22, 2018.

[38] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *in Proc. International Conference on the Theory and Application of Cryptology and Information Security*, pp. 552–565, 2001.