2023 IEEE/CIC International Conference on Communications in China (ICCC Workshops) | 979-8-3503-4540-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICCCWorkshops57813.2023.10233835

Blockchain-based Collision Avoidance Access Protocol for UAV Swarm

Gongming Lin*, Wei Wang*, Mengying Wang*, Qiang Ye†, Qihui Wu*
*College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing, China, 211106.
†Department of Computer Science, Memorial University of Newfoundland, Canada
Email:{lgm, wei_wang, mengying_w}@nuaa.edu.cn, qiangy@mun.ca, wuqihui2014@sina.com

***Abstract*—The explosive growth of unmanned aerial vehicles (UAVs) pose more and more aerial and communication resources, making efficient spectrum access control a key bottleneck for UAV swarm applications. Conventionally, the absence of a centralized authority may cause lots of spectrum collisions among UAVs, which not only wastes the spectrum resources, but also causes long access delay. To address this challenge, we propose a blockchain-based access protocol that can effectively mitigate the access collisions among a distributed UAV swarm in high dynamic scenarios. Specifically, we design a collision avoidance access mechanism by leveraging blockchain and hash access. We also analyze the performance of the proposed protocol and compare it with the slot multi-channel Aloha protocol. Simulation results demonstrate that the proposed protocol can effectively reduce the spectrum access collisions and is superior to slot multi-channel Aloha in access success rate, throughput, and average access delay.**

***Index Terms*—multiple access, Blockchain, UAV swarm, collision avoidance.**

I. Introduction

Unmanned aerial vehicles (UAVs) are capable of performing increasingly complex tasks, such as assisting in communication, search and rescue, security, exploration, agriculture, and military operations, benefited from the continuously improving transistor density and battery energy density [1]. Multiple UAVs may operate in the same area simultaneously, either as part of the same swarm or belonging to different organizations. However, due to the increasing scarcity of frequency resources, these UAVs often work in the same frequency band, leading to inevitable collisions and interference.

In scenarios where a centralized role, such as a base station, exists to coordinate the access of spectrum resources, collisions and interference among UAVs can be easily resolved [2]. The base station can make decisions on which UAVs are allowed to access the spectrum resources, or set up conditions for access based on certain criteria. With such a "parental role" managing the frequency usage of UAVs, the spectrum utilization in the area can be well-organized. However, in many situations, unmanned aerial vehicles operate in areas where centralized management is lacking. The unrestricted usage of limited spectrum resources by selfish UAVs can lead to the "Tragedy of the Commons" in game theory [3], which refers to the depletion of shared resources due to selfish behaviors that harm the common interest of the community.

The main cause of the "Tragedy of the Commons" is distrust. In a situation where the majority of individuals are well-behaved, selfish behavior can enable an individual to obtain more benefits. Conversely, in a situation where the majority of individuals are selfish, honest behavior will result in individual interests being compromised [4]. Clearly, in an environment of distrust, selfish behavior is the optimal strategy for all participants, even if it may lead to congestion or depletion of spectrum resources. Establishing trust is not an easy task, and without effective mechanisms, it is difficult to ensure that others comply with the agreed-upon spectrum access rules. As the underlying technology of cryptocurrencies, blockchain seems to be able to solve this trust dilemma.

Blockchain utilizes a blockchain-based data structure to verify and store data, uses distributed node consensus algorithms to generate and update data, ensures data security through cryptography, and programs and operates data through smart contracts, making it suitable for establishing trust mechanisms in decentralized systems [5], [6]. Moreover, the full traceability and tamper-proof features of blockchain are highly advantageous for regulatory oversight, this also encourages ones in the UAV swarm to regulate their own behavior.

Many scholars have studied the applications of blockchain in the fields of spectrum access and allocation. An access protocol for blockchain-based radio access networks (B-RAN) was proposed in [7], which utilizes the characteristics of hash functions to constrain devices to comply with access rules, thereby establishing trust between user devices. Using blockchain technology, [8] established trust between general authorized access (GAA) users and priority access (PA) users in citizens broadband radio service (CBRS) scenarios, resulting in improved spectrum management efficiency and service quality. In [9], blockchain is used to ensure fair and equitable transactions of spectrum resources between mobile network operators (MNOs). However, these spectrum allocation and access methods are not suitable for highly dynamic and decentralized UAV swarms with rapidly changing topologies.

While blockchain can enable trust among UAVs, without proper coordination mechanisms, collisions in channel selection can still occur among UAVs even if they fully trust each other [10]. Some wireless access networks adopt polling to allocate spectrum resources, which is obviously not suitable for UAV swarms with rapidly changing topology and large working areas. In [11], devices in mobile ad hoc networks coordinate channel allocation with neighboring nodes in the next time slot by broadcasting a reservation signal, but this method requires strict synchronization and is limited to TDMA. In [12], devices use gossip algorithms to broadcast access requests, thus achieving consensus on access order among all nodes in the network. Obviously, the overhead of controlling the channel and the negative benefits of long delays make this method not worth the cost when the number of devices is large.

In order to reduce access collisions in a decentralized and highly dynamic case, this paper proposes a blockchain-based collision avoidance access protocol (BCAA).The main contributions of this work are described as follows:

- To achieve efficient and collision-free access for a UAV swarm, we build a blockchain-enabled distributed access framework, where each UAV can access the spectrum through dedicated calculation and thus potential collisions are avoided. A trusted environment built through blockchain allows spectrum resources to be used efficiently and in an orderly manner by UAV swarm.
- We analyze the access success rate, the access delay, and the total throughput of the proposed BCAA scheme, with the Markov chain model, and closed-form results are obtained.
- We evaluate the performance of BCAA and compare it with the slot multi-channel Aloha protocol with selfish behavior. The simulation results show that BCAA outperforms slot multi-channel Aloha in access success rate, throughput, and average access delay.

The remainder of this paper is organized as follows. In Section II, we present a UAV swarm spectrum access system using BCAA. In Section III, we describe the BCAA protocol in detail and analyze the performance of BCAA. Section IV provides the simulation and analysis results. Finally, conclusions are given in Section V.

II. System Model

In this section, we present a specific system for spectrum access in a UAV swarm where all UAVs access according to the BCAA protocol.

A. Scenario

As shown in Fig.1, assuming that all UAVs in the swarm are active, UAV n_a can judge the UAVs that may compete with it for channels in the next slot by relative position and pre-stored information of other UAVs, and record these UAVs and n_a itself in the “collision set”, denote as $\mathcal{N} = \{n_1, n_2, \cdots, n_N\}$. Assuming that the frequency band available for the UAV swarm is evenly divided into M non-interfering channels, denoted as $\mathcal{M} = \{m_1, m_2, \cdots, m_M\}$, each UAV can have at most one channel usage right in a slot. In addition to the working channel, there is also an independent control channel for the interaction of control information and blockchain information. In perspective of n_a, the N UAVs in the collision set $\mathcal{N}$ will compete for these M channels. It is worth noting that since the position of the UAVs will change, the collision set may change over time, and since the positions of each UAV are different, their respective collision sets are also different. After obtaining the collision set, n_a will combine the blockchain information, UAV ID, slot number and other information to calculate the access strategy of all UAVs in the $\mathcal{N}$ set at T_S time, and decide whether to access according to the rules. In the working area of the UAV swarm, there are patrol UAVs belong to the regulatory authorities, who can sense and identify the signals of the UAVs in the area.

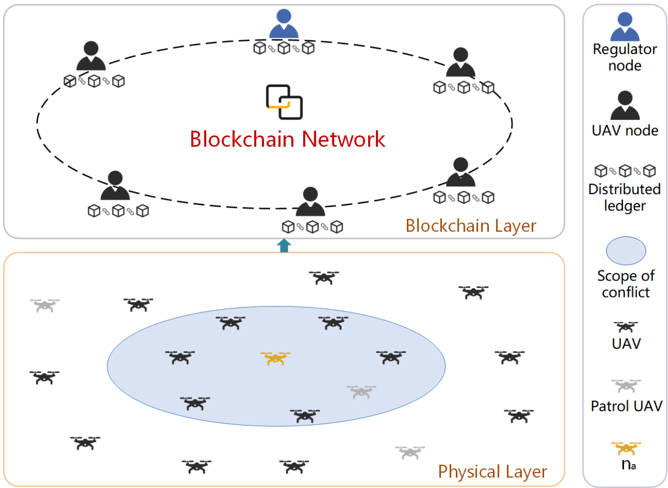

Fig. 1. UAV swarm spectrum access scenario.

B. Blockchain Model

The blockchain layer describes a consortium blockchain maintained by all UAVs, and each UAV is a node in the blockchain. The nodes are divided into peer nodes, consensus nodes and bookkeeping nodes. Peer nodes participate in the synchronization of blocks and the execution of smart contracts, but do not participate in consensus voting. Consensus nodes participate in consensus voting and select one bookkeeping node among them to generate new blocks.

The specific steps are as follows:

1. Identity registration: A UAV needs to upload its device information before it can join the consortium blockchain. After approval, the UAV will be assigned a unique and unchangeable ID by the blockchain system. The device information and ID of the newly joined UAV will be published to all UAVs in the form of on-chain information. After all UAVs synchronize the block containing this information, which is $\mathcal{T}_{sync}$ seconds after the block is generated, the new UAV can participate in the competition for the channel.

2. Upload access information: After a UAV successfully accesses a channel at a certain time slot, it needs to upload the access information to the blockchain network, otherwise, upload the access failure information to the blockchain network.

3. Upload regulatory information: The regulatory patrol UAV, which is dispatched by the regulatory authority, will also access this blockchain and can compare its monitoring results with the information on the chain to infer whether there is any dishonest behavior. The patrol UAV can impose penalties on the involved UAVs after discovering illegal frequency usage and dishonest behavior. The penalty information will also be uploaded to the blockchain network, which will affect the success rate of accessing for the involved UAVs.

4. Pack and sync blocks: The access and regulatory information is stored in the blockchain ledger after being validated and packaged through consensus. Assuming that it can be ensured that the blocks generated by the blockchain will be synchronized by all UAV nodes after $\mathcal{T}_{sync}$ seconds.

III. Proposed BCAA Protocol and Performance Analysis

In this section, we provide a detailed description of the BCAA protocol. Then, we will analyze the theoretical performance of BCAA at Poisson traffic. For the convenience of the analysis, we restrict the scenario to be more specific: in each time slot, the UAV generates packets at the supply rate λ. After the UAV accesses the channel in a time slot, it can send one packet. The unsent packets will exist in the buffer of the UAV. We will analyze the performance of BCAA in terms of three metrics: access success rate, throughput and average access delay.

A. BCAA Protocol

After constructing a system that meets the above standards for UAV swarm, the BCAA protocol can be used for spectrum access. To avoid unnecessary collisions, UAVs participating in channel contention use shared prior information to determine the channel allocation scheme for each time slot. The steps are as follows:

1. Generate the collision set: At the beginning of the T_S-1 time slot, the UAV n_a determines the UAVs that may compete with it for channels in the T_S time slot by their relative positions and the pre-stored information about other UAVs, and records these UAVs with n_a itself in the collision set $\mathcal{N}$:

$$\mathcal{N} = \{n_1, n_2, \cdots, n_N\}, n_a \in \mathcal{N}. \tag{1}$$

2. Compute the pre-allocation plan: After obtaining the collision set $\mathcal{N}$, the UAV n_a calculates the pre-allocation plans of all UAVs in $\mathcal{N}$:

$$p_{n_i} = (\textbf{hash}(ID_{n_i}, Info_{T_S-\mathcal{T}_{sync}}, T_S) \bmod M) + 1, \tag{2}$$

where p_{n_i} represents the pre-allocation plan of the UAV n_i, $n_i \in \mathcal{N}$, hash($\bullet$) represents the hash function whose result is integer and uniformly distributed on the interval $[LE, RE]$ and the endpoints of the interval satisfy $RE \gg RE - LE \gg M$, ID_{n_i} is the ID of the UAV n_i, $Info_{T_S-T_{sync}}$ is the on-chain information of the latest generated block before $\mathcal{T}_{sync}$ seconds of the start moment of the time slot T_S.

In this step, for each UAV n_i in $\mathcal{N}$, an integer between $[1, m]$ is generated, representing that in the time slot T_S, the UAV n_i will only compete for the channel $m_{p_{n_i}}$.

3. Direct access: Let the subset $\mathcal{N}_\alpha \subseteq \mathcal{N}$ represent the set of all UAVs whose result in the second step is equal to m_α, $m_\alpha \in \mathcal{M}$.

If $n_a \in \mathcal{N}_\alpha$ and $|\mathcal{N}_\alpha| = 1$, it means that no other UAV competes with n_a for channel m_α at the T_S time slot and n_a can access the m_α channel at the beginning of the T_S time slot.

4. Compete for channel $\mathbf{m}_\alpha$: If $n_a \in \mathcal{N}_\alpha$ and $|\mathcal{N}_\alpha| > 1$, it means that UAV n_a needs to compete with other UAVs for the channel m_α. Only one UAV can access the channel m_α, and the UAV n_a needs to satisfy the following equation to win the channel competition:

$$n_a = \underset{n_i \in \mathcal{N}\alpha}{\arg\max}(\textbf{hash}(ID_{n_i}, Info_{T_S-\mathcal{T}_{sync}}, T_S) \cdot \frac{\varphi_{n_i}}{\xi_{n_i}}), \tag{3}$$

where φ_{n_i} is the class weight factor of UAV n_i and ξ_{n_i} is the penalty factor of UAV n_i. If n_a wins the competition, it can access channel m_α at the beginning of the T_S time slot, otherwise n_a will forgo to access any channel in the T_S time slot.

5. Upload access messages: If n_a successfully accesses m_α channel in the T_S time slot, it needs to upload an access message to the blockchain network:

$$MSG = \{ID_{n_a}, T_S, m_\alpha, \mathcal{N}\}. \tag{4}$$

If n_a fails to access any chnnel, it needs to upload a failure message to the blockchain network:

$$MSG_f = \{ID_{n_a}, T_S, \mathcal{N}\}. \tag{5}$$

B. Access Success Rate

Since the result of the hash function obeys uniform distribution in a large interval [13] and the lower limit of the interval is much larger than the amount of channels M , it is easy to prove that the result of Eq. (2) is an integer uniformly distributed on $[1, M]$.

Assuming that the pre-allocation result of n_a is calculated to be m_α, the probability that the pre-allocation result is the same as n_a is $1/M$ for each UAV in $\mathcal{N}$. The probability that UAV n_a directly accesses channel m_α without competing with other UAVs is:

$$\begin{aligned} P_d &= \binom{N-1}{0} \frac{1}{M} (1 - \frac{1}{M})^{N-1} \\ &= (1 - \frac{1}{M})^{N-1}. \end{aligned} \tag{6}$$

Assuming that all UAVs in $\mathcal{N}$ have the same class factor and penalty factor during channel access at time slot T_S, all UAVs competing for the same channel have the same probability of winning. With k UAVs competing for the ma channel, the access success rate of n_a is:

$$\begin{aligned} P_{win} &= \sum_{k=0}^{N-1} \frac{1}{k+1} \binom{N-1}{k} (\frac{1}{M})^k (1 - \frac{1}{M})^{N-k-1} \\ &= \sum_{k=0}^{N-1} \frac{(M-1)^{N-k-1}(N-1)!}{M^k (k+1) k! (N-k-1)!}. \end{aligned} \tag{7}$$

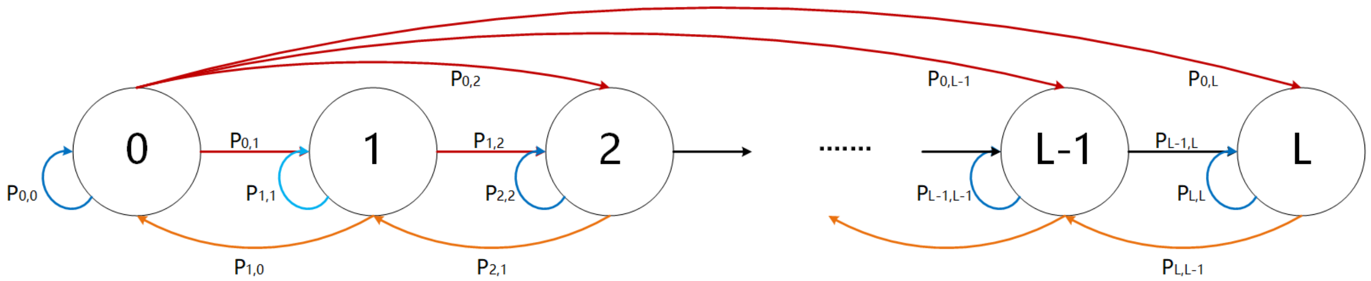

Fig. 2. State transition diagram of UAV buffer.

C. Markov Model

The queue length variation of the UAV buffer can be considered as a Markov process, and for the next analysis, we need to build a Markov model.

Let the states of Markov represent the queue length in the buffer of the UAV. By setting the maximum buffer queue length of the buffer to L, the state space of the Markov process is represented as:

$$\mathcal{Q} = \{0, 1, 2, \cdots, j, \cdots, L\}. \tag{8}$$

Define η_j as the steady-state probability of the system when the buffer queue length is j, and $p_{u,v}$ denotes the state transfer probability of the buffer transfer from $\mathcal{Q} = u$ to $\mathcal{Q} = v$. Then the state transition diagram of the buffer is shown in Fig. 2,and the state transition matrix of the buffer is:

$$\mathcal{P} = \begin{bmatrix} p_{0,0} & p_{0,1} & \cdots & p_{0,L-1} & p_{0,L} \\ p_{1,0} & p_{1,1} & \cdots & p_{1,L-1} & p_{1,L} \\ 0 & p_{2,1} & \cdots & p_{2,L-1} & p_{2,L} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & p_{L,L-1} & p_{L,L} \end{bmatrix}. \tag{9}$$

Define b_l as the probability that l packets arrive in a time slot, b_l obeys a Poisson distribution with parameter λ:

$$b_l = \frac{\lambda^l}{l!} e^{-\lambda}, \ l \in [0, L]. \tag{10}$$

Then the one-step transition probability of the buffer can be expressed as:

$$\begin{cases} p_{u,u+l} = b_l, & u = 0, 0 \leqslant l \leqslant L \\ p_{u,u+l} = b_l \cdot (1 - P_{win}) + b_{l+1} \cdot P_{win}, & 1 \leqslant l \leqslant L - u, \\ & 1 \leqslant u \leqslant L - 1 \\ p_{u,u-l} = b_0 \cdot P_{win}, & 1 \leqslant u \leqslant L \\ p_{u,u} = b_1 \cdot P_{win} + b_0 \cdot (1 - P_{win}). & 1 \leqslant u \leqslant L \end{cases} \tag{11}$$

Let vector $\boldsymbol{\eta} = \{\eta_0, \eta_1, \cdots, \eta_L\}$, and since η_j represents the steady-state probability when the buffer is of queue length j, the following equation is given:

$$\boldsymbol{\eta} \cdot \mathcal{P} = \boldsymbol{\eta}. \tag{12}$$

$$\sum_{j=0}^{L} \eta_j = 1. \tag{13}$$

According to Eq. (8) to (13), the steady-state solution of the buffer length can be obtained.

D. Throughput and Average Access Delay

Throughput is defined as the average number of packets that can be successfully transmitted per time slot in the swarm and can be obtained by multiplying the probability of successful access by the amount of UAVs ready to send packets per time slot. The UAV sends the packet when the buffer is not empty, so the throughput $\mathbb{T}$ can be expressed as:

$$\mathbb{T} = P_{win} \cdot N \cdot (1 - \eta_0). \tag{14}$$

According to Little's law [14], in a stable system, the average access delay is equal to the ratio of the average length of the buffer queue to the throughput. The average length of the buffer queue is:

$$\overline{L} = \sum_{l=0}^{L} \eta_l \cdot l. \tag{15}$$

The average access delay can be expressed as:

$$\mathcal{D} = \frac{\overline{L}}{\mathbb{T}} = \frac{\sum_{l=0}^{L} \eta_l \cdot l}{P_{win} \cdot N \cdot (1 - \eta_0)}. \tag{16}$$

IV. Simulation Results and Discussions

In this section, we use Python to simulate the above modeling and analysis and give the simulation data about the performance of BCAA and compare it with the time slot multi-channel Aloha protocol where selfish behavior exists. Finally, we discuss the effect of class factor φ and penalty factor ξ on the UAV access success rate.

A. Access Success Rate

The variation of the success rate of access with N with different amount of channels is shown in Fig. 3. According to Eq. (7), the access success is only related to the amount N of UAVs in the collision set $\mathcal{N}$ and the amount of channels M, when the class factor of all UAVs and with the penalty factor are equal.

The comparison of the access success rate of BCAA with that of slot multi-channel Aloha is shown in Fig. 4, which shows that the access success rate of BCAA is higher compared with time slot multi-channel Aloha. This is because in

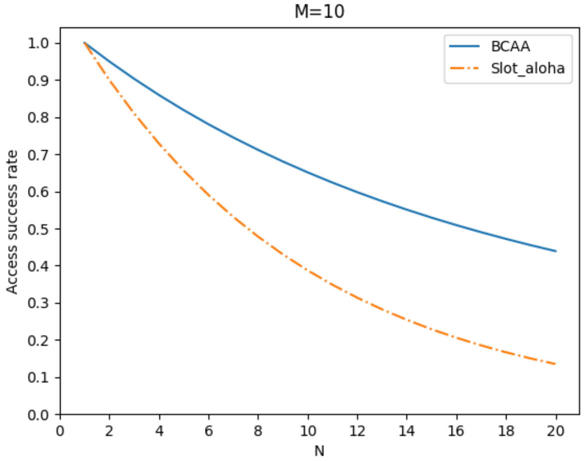

Fig. 3. Access success rate comparison under different number of UAVs, where M=10.

BCAA, the UAV has a chance to access the channel when the randomly selected channel "collides" with other UAVs, while the time slot multi-channel Aloha fails to access the channel for all UAVs after the collision.

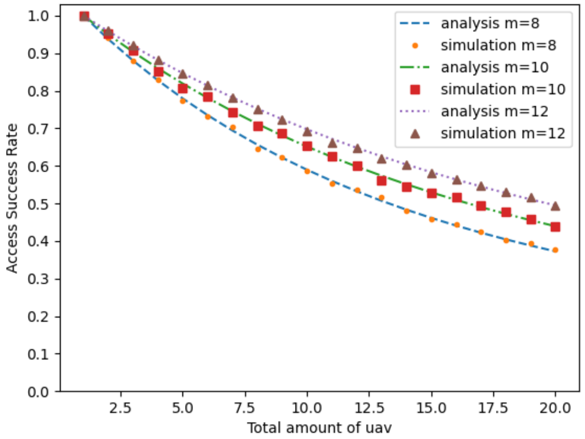

Fig. 4. Access success rate of the proposed BCAA scheme.

B. Throughput and Average Access Delay

In Fig. 5, we can observe the trend of throughput with the supply rate λ. Under the constraints of the amount of channels in $\mathcal{M}$ and the access success rate P_{win}, the throughput remains basically constant after growing to its peak.

In Fig. 6, we can see that the slot multi-channel time Aloha decreases when the supply rate reaches a certain value, which is the negative effect of channel collision caused by selfish behavior. In contrast, BCAA can maintain a high throughput rate during collision, this is because there is always one UAV that will able to access the contested channel when a "collision" happens compared to Aloha's total failure, therefore, UAVs using BCAA can obtain a high access success rate simply by accessing on demand, without being caught in a "prisoner's dilemma" due to selfish behavior.

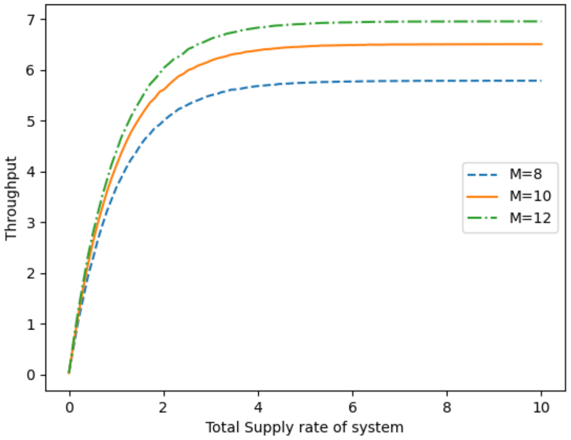

Fig. 5. Throughput of BCAA under different number of channels, where N=10.

Fig. 7 reflects the average access delays of BCAA and slot multi-channel Aloha at different total system supply rates [15]. It can be observed that the average access delay of BCAA is much lower than that of slot multi-channel Aloha in the state where the buffer is close to full capacity.

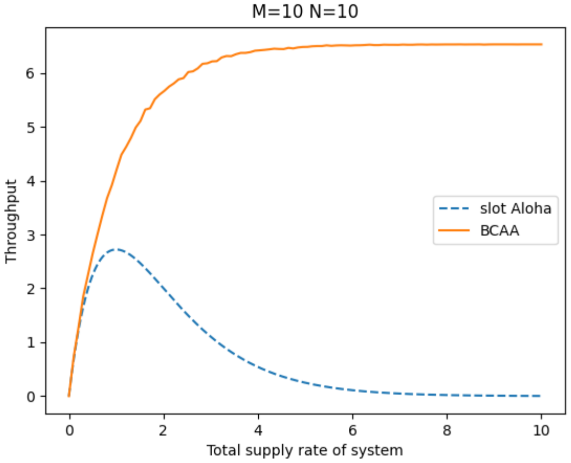

Fig. 6. Throughput comparison between BCAA and slot Aloha, with M=10, N=10.

C. Affect of φ and ξ

The class factor φ and penalty factor ξ could be analyzed together. To ensure the fairness and performance of the protocol, the majority of UAVs should have an initial class factor and penalty factor of 1. Here are two situations where the class factor and penalty factor need to be adjusted, the first is for UAVs performing important missions, where we should

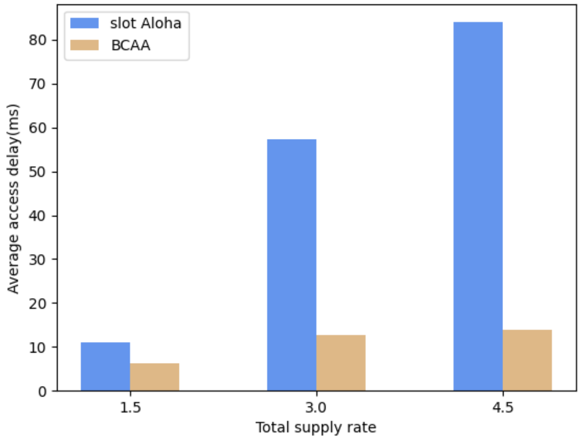

Fig. 7. Average access delay comparison between BCAA and slot Aloha, with M=10, N=10.

increase their class factor. The second scenario is that for rule violating UAVs, the regulator's patrol UAVs should be entitled to increase their penalty factor. Fig. 8 presents the effect of $\frac{\varphi}{\xi}$ on the access success rate of UAVs, it can be observed that class factor and penalty factor have obvious influence on the success rate of UAV access. It should be noted that the effect will be reduced if the $\frac{\varphi}{\xi}$ of too many UAVs are adjusted.

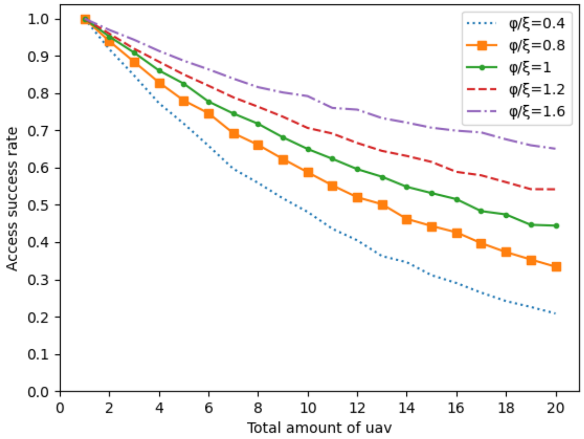

Fig. 8. Affect of class factor and penalty factor on the access success rate, where M=10.

V. Conclusion

In this paper, we propose an access protocol called BCAA for UAV swarms. By introducing blockchain, the proposed protocol prevents the "tragedy of the commons" caused by selfish behavior, and uses the information on the chain as a common a priori information for collision avoidance among UAVs. Meanwhile, the traceability and immutability of blockchain makes this protocol convenient for regulation. Theoretical analysis and simulation show that the proposed protocol has good performance in terms of throughput, access success rate, and average access delay. Future work will focus on improving the utilization of idle channels to further enhance the performance of the proposed protocol.

Acknowledgment

This work was supported in part by the National Natural Science Foundation of China under Grant 62001220, the Jiangsu Provincial Key Research and Development Program under Grants BE2022068, the Natural Science Foundation of Jiangsu Province under Grants BK20200440, and the Young Elite Scientist Sponsorship Program, China Association for Science and Technology, YESS20200207

References

[1] Y. Zhou, B. Rao, and W. Wang, "UAV swarm intelligence: Recent advances and future trends," *IEEE Access*, vol. 8, pp. 183 856–183 878, 2020.

[2] Q. Zhao and B. M. Sadler, "A survey of dynamic spectrum access," *IEEE signal processing magazine*, vol. 24, no. 3, pp. 79–89, 2007.

[3] E. Ostrom, "Tragedy of the commons," *The new palgrave dictionary of economics*, vol. 2, pp. 1–4, 2008.

[4] X. Ling, Y. Le, J. Wang, and Z. Ding, "Hash access: Trustworthy grant-free IoT access enabled by blockchain radio access networks," *IEEE Network*, vol. 34, no. 1, pp. 54–61, 2020.

[5] S. Nakamoto and A. Bitcoin, "A peer-to-peer electronic cash system," *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf*, vol. 4, no. 2, 2008.

[6] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International journal of web and grid services*, vol. 14, no. 4, pp. 352–375, 2018.

[7] X. Ling, B. Zhang, H. Xie, J. Wang, and Z. Ding, "Hash access in blockchain radio access networks: Characterization and optimization," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8053–8066, 2021.

[8] Z. Li, W. Wang, J. Guo, Y. Zhu, L. Han, and Q. Wu, "Blockchain-assisted dynamic spectrum sharing in the cbrs band," in *2021 IEEE/CIC International Conference on Communications in China (ICCC)*. IEEE, 2021, pp. 864–869.

[9] Z. Li, W. Wang, Q. Wu, and X. Wang, "Multi-operator dynamic spectrum sharing for wireless communications: A consortium blockchain enabled framework," *IEEE Transactions on Cognitive Communications and Networking*, 2022.

[10] A. B. Tambawal, R. M. Noor, R. Salleh, C. Chembe, M. H. Anisi, O. Michael, and J. Lloret, "Time division multiple access scheduling strategies for emerging vehicular ad hoc network medium access control protocols: A survey," *Telecommunication Systems*, vol. 70, pp. 595–616, 2019.

[11] C. Zhu and M. S. Corson, "A five-phase reservation protocol (fprp) for mobile ad hoc networks," *Wireless networks*, vol. 7, pp. 371–384, 2001.

[12] H. Seo, J. Park, M. Bennis, and W. Choi, "Consensus-before-talk: Distributed dynamic spectrum access via distributed spectrum ledger technology," in *2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*. IEEE, 2018, pp. 1–7.

[13] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," in *Proceedings of the ninth annual ACM symposium on Theory of computing*, 1977, pp. 106–112.

[14] J. F. Shortle, J. M. Thompson, D. Gross, and C. M. Harris, *Fundamentals of queueing theory*. John Wiley & Sons, 2018, vol. 399.

[15] D. Shen and V. O. Li, "Performance analysis for a stabilized multi-channel slotted aloha algorithm," in *14th IEEE Proceedings on Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003.*, vol. 1. IEEE, 2003, pp. 249–253.