Enhancing UAV Network Reliability through Blockchain-Based Information Sharing

Seoeun Choi
School of Electrical Engineering
Korea University
Seoul, Republic of Korea
magchoi@korea.ac.kr

Seunghwan Lee
Department of Smart Convergence
Korea University
Seoul, Republic of Korea
longkid1@korea.ac.kr

Hwangnam Kim
School of Electrical Engineering
Korea University
Seoul, Republic of Korea
hnkim@korea.ac.kr

***Abstract*— Unmanned aerial vehicles have been used in various fields in addition to their first military purposes, and in most cases, several UAVs should work together to perform the task. For this, each UAV belongs to a network and exchanges data with each other. However, malicious nodes can often break into the network and attempt to intercept or change the exchanged data, which can adversely affect UAV performance. In this paper, we propose a methodology in which UAVs exchange data through blockchain-based validation and consensus to prevent the invasion of these malicious nodes and enable safer and more stable data exchange.**

Keywords—UAV network; Blockchain; security; Proof of Work;

I. Introduction

Unmanned Aerial Vehicles (UAVs), also known as drones, were used in the past for military purposes to reduce the casualties of air force pilots when infiltrating enemy bases [1]. In addition, over the past few decades, the uses of UAVs have expanded beyond military purposes to industrial and academia. [2]. In most cases, several UAVs form a fleet and perform missions in cooperation with each other, which is called UAV swarm. UAVs in the swarm form a network and communicate with each other to exchange data for task performance. This allows UAVs in the swarm to cooperate each other to successfully perform complex tasks [3]. However, malicious nodes often break into the UAV swarm network and attempt to intercept or change the data exchanged by UAVs. Such data may contain various security-sensitive contents such as military information and personal information, etc. Therefore, data intercept or change by malicious nodes can have an adverse effect on the performance of tasks performed by UAVs. For example, in 2008, "Shi'ite" militants in Iraq hacked live video footage from U.S. UAVs after they discovered that the video was not encrypted. This video footage was obtained through a cyberattack on the UAVs' software [4].

The exchange of data by UAVs through blockchain-based consensus can be an excellent defense against these threats. Blockchain is a technology proposed by Nagamoto that allows only data that has gone through participants' validation and consensus to be added to the chain in the form of blocks [5]. In addition, participants share the same information by recording the information of the chain in distributed ledgers [6]. This property of the blockchain enables data protection by blocking attempts by malicious nodes to access data.

In this paper, we propose a system in which UAV nodes in the network exchange data and protect it from external intrusion through blockchain-based validation and consensus processes. In the system, each UAV node can participate in the network through mutual validation, generate data into blocks, and share it with other nodes by adding it to the chain through the consensus process. In addition, we evaluate the performance of the system based on the time and difficulty required for consensus.

II. System Design

A. System Architecture

The system architecture is shown in Fig. 1. We assume that all UAVs in the swarm are always connected. We also assumed each UAV had the computing power to execute consensus algorithm. The data collected by UAVs in a swarm can be combined into a single block in our proposed structure.

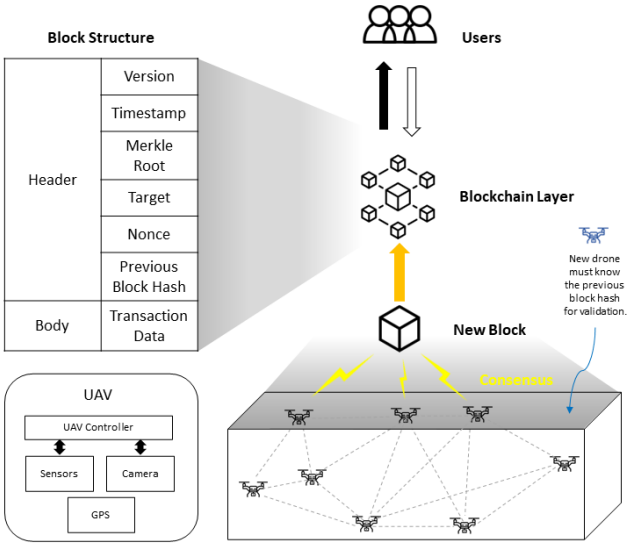

Fig. 1. System Architecture of Blockchain-based UAV network

This new block is added to the blockchain. It is impossible to modify the block because the block hash of the previous block is stored in each block. The block hash is formed from the version, the time, the merkle root, the destination, the nonce, and the previous block hash that belongs to the block header.

For example, suppose there is a malicious attempt to intercept or tamper with data from a UAV network. If an attacker manipulates the transaction data recorded in the n^{th} block, the transaction hash value changes and the merkle root of the n^{th} block changes. When the merkle root hash changes, the corresponding block hash also changes. Therefore, it does not match the previous block hash, which is in the $n + 1^{\text{th}}$ block. As a result, malicious attempts to manipulate UAV network data cannot be successful. The protocol of the proposed system is detailed in Algorithm 1.

The system can also be used for communication between UAVs. It is possible to share data for performing tasks between UAVs by posting the swarm UAVs' data on blocks and uploading them to the blockchain network. In other words, it allows UAVs to communicate with each other without third party. For example, there is a centralized system such as composite multi-UAV control. There is no need to rely on a central authority such as the UAV leader or Airborne Control Center (ACC) when using the proposed protocol.

B. Enhanced Information Sharing Protocol

All nodes in the UAV network know the block hash of the last block. There are two steps to protect shared data from malicious nodes. First, it is possible to prevent nodes suspected of having malicious intent from participating in the network. A new node needs to know the block hash value of the genesis block in the network when it wants to join a UAV network. If the node does not know the value, it will not be able to join the network. Next, you can take advantage of the integrity of the blockchain to trust the data that is shared on the network. This paper assumes that blocks are created by consensus based on Proof of Work (PoW). The UAV uses GPS and a variety of sensors to collect information and record it as a transaction. The transaction data will be in the transaction pool and will be awaiting the creation of a new block. A new block is created by calculating a hash value that is less than the target value. The target value is specified in the header of the previous block. The number of leading zeros attached to the front of the target value refers to the difficulty, and the higher the number of zeros, the more difficult it is to generate a hash value less than the target value, so the difficulty of the consensus increases. If the hash value calculation is successful, it means consensus, and a new block is created. Finally, the new block is attached to the end of the chain.

The blocks need to be generated more frequently when a network problem occurs that causes delays or when time-sensitive data needs to be transmitted. In this case, reducing the difficulty of consensus can reduce the time required to generate a block. The adjusted consensus difficulty reverts to the general consensus difficulty when the special situation is over. The data in the transaction pool will be collected and recorded in the new block. There is no risk of tampering with the data which has been recorded in the chain because the hash value of the previous block is stored in each of the blocks.

***Algorithm 1**: Enhanced Information Sharing Protocol*

Input: *UAV swarm* ü = {u_1, u_2, …, u_n}
data set ***tx*** = {tx_1, tx_2, …, tx_n}
tval = *target for consensus*
nonce = *number of hash value calculation*
difficulty = *difficulty for consensus*
norm_diff = *difficulty for normal traffic*
event = *events that require low network delay*

Output: $\mathbf{B}_i$ = i^{th} *Block in Blockchain layer*
BC = *current state of the chain*

```
function generate_transactions(u, tx)
    for each u get sensor, camera, GPS data
        tx ← data
    return tx
function share_information_in_blocks(ü, tx)
    while block_hash > tval do
        block_hash ← compute_hash()
        nonce += 1
    for every tx in ü
        B_i ← tx = {tx_1, tx_2, …, tx_n}
        B_i.hash ← block_hash
        BC.add(B_i)
    return B_i
while UAV network running do
    difficulty ← norm_diff
    if event occurs then
        difficulty -= 1
return BC
```

C. Security Strength

In the proposed system, a new UAV needs to be verified based on the key value to join the network. For the key value, we recommend using a hash value for security reasons. Our proposed system uses SHA-256. It has security strengths for collision resistance, preimage resistance, and second preimage resistance [7]. It is computationally impossible to find two different inputs where $\text{sha256}(m_1) = \text{sha256}(m_2)$ because it has 128 bits of collision resistance strength. It is also computationally impossible to find an input message with a random hash value because it has 256 bits of preimage resistance strength. The second preimage resistance strength of SHA-256 hash function is 256 - $L(m)$ bits. $L(m)$ is defined as:

$$L(m) = \log_2 \frac{len(m)}{block\ size} \tag{1}$$

where $len(m)$ is the length of message m bits. For example, if $m = 2^{33}$, $L(m) = \log_2(2^{33}/2^9) = 24$, then finding a second preimage requires 2^{232} times of work. The hash function can be

used to defend against major hacking attacks such as brute force attack.

III. Performance Evaluation

We implemented the validation and consensus process described in Section 2 and simulated it. In the system proposed, nodes in the UAV network must create it in the form of blocks to transmit data. In the proposed system, the time required to make data in the form of blocks accounts for most of the delay, and the delay of the network itself during transmission is a relatively small value. Therefore, in this paper, we assume that the delay of the UAV network is equal to the block generation time for data transmission and sharing.

The UAV network is a wireless network, and due to its characteristics, it has a higher frequency of network problems such as transmission errors than general wired networks. In this case, the delay value may be very high. In addition, if an event such as an accident occurs while performing a task and data must be transmitted urgently in almost real time, a very low level of delay value must be maintained. In these cases, it is necessary to lower the delay than before. In the system proposed in this paper, the delay can be lowered by lowering the consensus difficulty. The simulated result is shown in Fig. 2. The figure shows a graph measuring the aspect of delay by adjusting the difficulty according to the state of the network or traffic requirements during 50 data transmissions. In the proposed system, the difficulty of data transmission in general situations is set at 5. However, in Fig. 2, the delay rises steeply until the 15th transmission. In this case, the system recognizes that a network problem has occurred and adjusts the consensus difficulty to 4 to lower the delay. Moreover, if time-sensitive data to be transmitted urgently occurs, it keeps the delay at a very low level by lowering the consensus difficulty further, as between the 31st and 40th transmission of Fig. 2. It shows that there is an almost exponential difference in delay according to the degree of difficulty of consensus. The faster it takes to generate a block, the higher the probability that the malicious node can generate a hash value less than the target hash value, and the higher the possibility of accessing the block and damaging the integrity of information. Therefore, the adjustment to the consensus difficulty should only be made in essential situations such as the aforementioned cases.

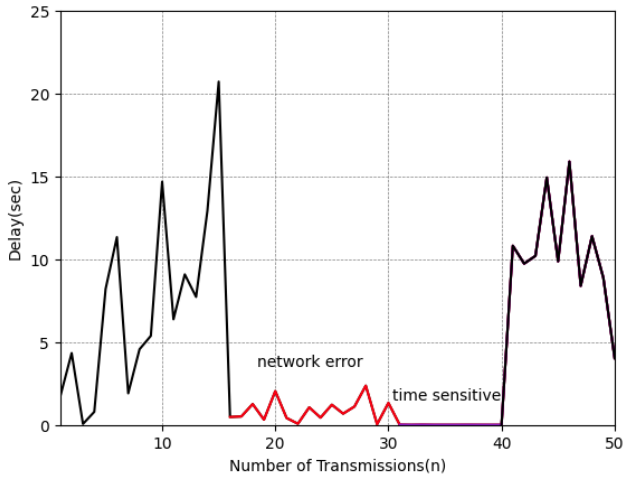

Fig. 2. Transmission delay according to the difficulty level

IV. Conclusion

In this paper, we propose a blockchain-based validation and consensus system for new node participation in UAV networks and data sharing of UAV nodes. In the proposed system, in order for new external nodes other than nodes existing in the network to participate, a validation procedure by a key value shared by existing nodes must be performed. Since this key value is a value generated by the hash function, it is virtually impossible to guess this value unless shared in advance. Therefore, this means that the access of the UAV network by the malicious node may be blocked. In addition, the system collects data from nodes in the UAV network in the form of transactions, creates them as a block, and adds them to the chain, allowing all nodes to share data. The block generated through consensus is protected by its hash value, and thus the data in the block is also protected. This means that even if there is an external malicious node that has successfully passed the validation process and accessed the UAV network with a very low probability, it is almost impossible to access and change the data shared by UAV nodes. Therefore, when utilizing the proposed system, nodes in the UAV network can share data more safely.

We have some future works. We plan to apply the system proposed in this paper by actually linking the UAV simulation program and the network simulation program. Through this, it is expected that it will be possible to verify system performance in a more realistic experimental environment.

Acknowledgment

This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2021-0-01835) supervised by the IITP (Institute of Information & Communications Technology Planning & Evaluation) and in part by the National Research Foundation (NRF) of Korea funded by the Korean Government under Grant 2020R1A2C1012389. Seoeun Choi and Seunghwan Lee contributed equally to this work.

References

[1] Y. Zeng, R. Zhang, and TJ. Lim, “Wireless communications with unmanned aerial vehicles: opportunities and challenges,” IEEE Communications Magazine, vol. 54, issue. 5, pp. 36-42, May 2016.

[2] S. Yoo, et al., “Poster: A Multi-Drone Platform for Empowering Drones’ Teamwork,” The 21st Annual International Conference on Mobile Computing and Networking (MobiCom), pp. 275-277, September, 2015.

[3] Q. Zhang, et al. “IoT Enabled UAV: Network Architecture and Routing Algorithm,” IEEE Internet of Things Journal, vol. 6, issue. 2, pp. 3727-3742, April, 2019.

[4] D. Rudinskas, Z. Goraj, and J. Stankūnas, “Security analysis of uav radio communication system,” Aviation, vol. 13, issue. 4, pp. 116-121, Nov. 2009.

[5] S. Park and H. Kim, “DAGmap: Multi-Drone SLAM via a DAG-Based Distributed Ledger,” Drones, vol. 6, issue. 2, pp. 34, Jan. 2022.

[6] S. Park, J. Lee, and H. Kim, “Efficient computation offloading for ethereum DApps,” Journal of Industrial Information Integration, Volume 31, ,100411, 2023

[7] M Bellare and P. Rogawayy, "Optimal Asymmetric Encryption How to Encrypt with RSA", Advances in Cryptology Eurocrypt 94 Proceedings, vol. 950, pp. 1-19, 1995.