Combat drone swarm system (CDSS) based on Solana blockchain technology

Sviatoslav Vasylyshyn[1*†], Ivan Opirskyy[1†]

[1] *Lviv Polytechnic National University, 12 Stepana Bandery str, Lviv, 79000, Ukraine*

Abstract

This paper examines the application of Solana blockchain technology in managing combat drone swarms, focusing on its ability to enhance security, reliability, and transparency in military and disaster relief operations. We present a model, UAV Swarm Net, which leverages the high throughput and low latency of Solana to ensure real-time decision-making and robust communication among UAVs. Our analysis includes a comparative study with traditional systems, emphasizing the advantages of blockchain in scalability and security. We conclude with real-world applicability, regulatory challenges, and future directions for integrating emerging technologies. Blockchain Swarm Management can help register each drone on the blockchain platform. Digitally signed transactions, data provenance, and a consensus mechanism can immediately identify and nullify data that has been corrupted between drones. Survivability and overall combat effectiveness enable it to complete difficult tasks such as swarm confrontation and forest firefighting.

Keywords

Blockchain, combat, Solana, drones, network, security

1. Introduction

In the context of cooperative operations of UAV clusters, information connection channels must be established between UAVs to form a mobile self-organizing (ad hoc) UAV network. Compared to traditional mobile ad hoc networks, the drone network features fast node movement, strong interference from the working environment, long working hours, and robust real-time performance. These characteristics introduce more complex security issues to the cooperative operations of the drone cluster. Data can easily become a target of hacker attacks. Once hackers intercept communication or hijack drones, it can impact the swarm combat environment and even result in serious consequences, such as leaking state secrets and disrupting social order [1]. For example, in January 2021 the incident of hundreds of drones falling in Chaotianmen the U.S. Department of Justice's update of the drone safety law indicates that drone safety plays an important role in future security risks, and the safety protection of drones is imperative [2].

The Seventh International Workshop on Computer Modeling and Intelligent Systems (CMIS-2024), May 3, 2024, Zaporizhzhia, Ukraine

sviatoslav.i.vasylyshyn@lpnu.ua (S. Vasylyshyn); iopirsky@gmail.com (I. Opirskyy)
0000-0003-1944-2979 (S. Vasylyshyn); 0000-0002-8461-8996 (I. Opirskyy)

To enhance the robustness and security of UAV systems, in recent years, researchers have begun to try to use blockchain technology to solve the information security problem of UAV collaborative operations. Blockchain is an emerging technology that originated from Bitcoin. It connects data blocks in chronological order to form a distributed ledger that cannot be tampered with or forged. According to the degree of openness, blockchain can be divided into three types: public chain, alliance chain, and private chain. Among them, only the private chain limited to private members has both high transaction throughput performance and a high degree of decentralization if we compare it with UAVs in warfare. Compared with public and alliance chains, it is more suitable for integration with drones to create a safe and reliable communication network [3].

This article using the private chain Solana as the basic framework, explores solutions for applying the core technologies of blockchain (such as peer-to-peer networks, distributed ledgers, smart contracts, etc.) to drone cluster systems to help drones achieve collaborative operations. The data sharing and collaborative decision-making functions in the blockchain are used, and the security features of the blockchain itself are used to deal with the security issues of drone collaboration so that the drone cluster can operate normally in confrontational airspace and enhance the security of the drone system.

Section 2 of this article introduces related work, including the security issues faced by drone systems, the working principle of the private chain Solana, and existing solutions that combine blockchain and drones. Section 3 introduces the model UAV-Swarm Net proposed in this article, including network structure and transaction process. Section 4 explains how the UAV-Swarm Net model responds to the security challenges of UAV systems from three aspects: data confidentiality, integrity, and availability. The final summary discusses the limitations caused by the combination of the two technologies and the issues that need to be further studied in the future.

2. Related work

2.1. UAV system safety

A typical UAV swarm system (Unmanned Aircraft System, UAS) is mainly composed of a UAV swarm, a ground control base station (Ground Control Station, GCS), and a communication network used to exchange information between them. It is a complex system [4]. In combat, the increasing complexity of tasks and the improvement of the intelligence level of UAVs have led to the development of UAV system control methods from traditional radio remote control and automatic program control to autonomous collaborative control of UAV clusters. The difference between automatic control and autonomous control is that automatic control involves the system performing tasks according to instructions, whereas autonomous control requires the drone itself to make decisions at critical moments. Compared with simple UAS, UAV systems are facing major challenges in terms of safety, swarm intelligence, and cluster complexity. The complexity and practicality of UAV systems have also triggered a research boom in both corporate and academic circles. According to statistics, in 2020 alone, close to 20,000 papers were published with the keyword "UAV" [6]. Safety is one of the main concerns of UAS. Computers and GCS can communicate and share information in real time, and the information sent and received must be reliable to make further real-time and effective decisions and secure collaboration. The National Institute of Standards and Technology (NIST) has formulated the data security policy [7] it is specified as "CIA", which is the system's requirements for confidentiality (Confidentiality, C), integrity (Integrity, I), and availability

(Availability, A). Among them, confidentiality refers to the protection of data. Humans and machines must not disclose sensitive information to any unauthorized person, entity, or process; integrity refers to the reliability of data, and the drone system should have the ability to resist hackers from modifying or damaging data; availability refers to data and services Accessibility should ensure that the UAV system can access and use information timely and reliably [8]. A complete UAV security protection solution should combine active and passive protection methods. Active protection refers to the use of various information encryption Technology eliminates security threats and increases the difficulty of hacker intrusion. For example, literature [9] applies security encryption methods to the WiFi 802.11 access point in the drone telemetry box and the entire communication path to improve the confidentiality of data transmission. Passive protection refers to making appropriate responses after detecting security threats to avoid continued adverse effects. For example, the literature [10] uses Bayesian game theory to detect drone network intrusions and improve drone network performance. At the same time, security detection is implemented; literature [11] uses middleware to construct an encrypted channel to detect DoS intrusions by anonymous attackers to interrupt the hacker attack channel.

However, the above studies are all based on the underlying defense of the physical layer or link layer, only focus on the local security protection of drones, and lack consideration of the overall network architecture. To this end, this article will use the blockchain and drone networks to integrate multiple security technologies such as member authentication, encrypted channels, and asymmetric encryption algorithms, to establish a safe and reliable communication network for drone collaboration and effectively respond to the "CIA" security challenges.

2.2. Solana blockchain network

Solana is an open-source blockchain platform that focuses on scalability, speed, and security, while maintaining low transaction costs. Its architecture facilitates the creation of smart contracts and decentralized applications. According to the project's white paper, the network's throughput can reach up to 710,000 transactions per second (TPS). Due to its affordability, Solana has gained popularity among users in the DeFi sector. In December 2023, analysts estimated that the number of active addresses in the network exceeded 15.6 million [12]. As of January 4, 2024, the total value of funds locked in smart contracts (TVL) of the project exceeded $1.3 billion, according to DeFiLlama. At the time of writing, Solana ranks among the top five blockchains by this indicator. The Solana project aims to address the blockchain trilemma, which involves balancing scalability, security, and decentralization. It is built on a hybrid consensus mechanism that theoretically allows the network to operate rapidly while maintaining a high level of decentralization and reliability.

Before we understand how Solana works, let's look at the technologies that support the operational operation of the network:

- the Proof-of-History blockchain synchronization concept;
- Tower BFT is an optimized version of the PBFT algorithm;
- Turbine is a mechanism for transferring data about a block to broadcast records to all nodes;
- Gulf Stream — protocol for transferring transactions without mempool;
- Sealevel — parallel execution of smart contracts;
- Pipelining — transaction processing to optimize the block confirmation process;
- Cloudbreak is a horizontally scalable database of accounts;
- Archivers is a distributed registry repository.

The main feature of Solana is the PoH technology, which functions as a cryptographic clock. Normally, to verify transactions, nodes need to communicate with each other to calculate timestamps and confirm the transaction. The speed of transaction processing depends on the speed of node synchronization.

With the implementation of PoH, the synchronization process is greatly simplified. Nodes do not need to wait for transaction confirmation from each node. Instead, they rely on a cryptographic clock to track events on the blockchain. Turbine breaks the block information into smaller data packets and distributes them randomly to different nodes. With this approach, you can reach up to 40,000 validators. The speed of the blockchain is also increased by Sealevel, a technology used to optimize resources. Transactions scale horizontally across GPUs and SSDs, which should meet the growing needs of the project.

The SHA-256 hashing algorithm is implemented in Solana for cryptographic data protection.

Since the Solana protocol runs on DPoS, validators block SOL to provide a consensus mechanism. There is no hard requirement for the number of coins to run a node, but the cost of confirming blocks can cost up to 1.1 SOL per day. At the same time, powerful equipment is required to participate in the project as a validator. However, DPoS allows you to delegate assets, i.e. to transfer them under the control of a validator. You can see the list of the latest ones here. At the time of preparation of the material, almost 2,000 nodes are working in the network Profit from staking depends on many factors, including inflation and the total number of "frozen" coins in the network. Digital assets can be withdrawn at any time, but the process takes about three days.

As of January 8, 2024, about 378.5 million SOLs are locked in the protocol deposit contract. Solana's annual percentage rate of return (APY) is 7.2%. The Solana ecosystem also includes liquid staking services such as Lido Finance, Marinade, and Jito. They issue tokens instead of locked cryptocurrency. Assets can be used in DeFi applications.

Terms and APY vary depending on the project:

1. Lido Finance — Lido DAO members choose validators and decide how much cryptocurrency to delegate to them. As a rule, coins are transferred to validators who are long-standing partners of the project. Annual percentage return from staking — 7.5%, according to Solana Compass;
2. Marinade - the project team evaluates the decentralization and performance of validators on its scale and selects the 100 best. They are delegated 60%, and the remaining 40% are distributed according to the results of the community vote. APY is 6.6%;
3. Jito — to interact with the project, validators must apply through the Jito Foundation. The project promises its customers 7% APY.

This article will make full use of these functions to establish a peer-to-peer network UAV-Swarm Net based on Solana to meet the security requirements of UAV systems for data confidentiality, integrity, and availability.

2.3. Existing solutions

The report highlighted that as the autonomous capabilities of drones improve, trust will become a critical focus, and blockchain technology can enhance the integrity and trust of UAS through policies and protocols. The study incorporates the integration of blockchain and drones to provide a framework for commercial drone use. Blockchain technology ensures security, offers identity management, and supports UAS conflict management and flight authorization. Additionally, it aids in air traffic management, addresses data storage challenges, and resolves the trust issues related to big data in drone cloud systems. Currently, many companies globally are engaged in research and development on the application of blockchain technology in drones. For instance, in August 2018, Boeing partnered with AI provider SparkCognition to develop a drone tracking system and an air traffic management solution based on blockchain technology. In September 2018, IBM applied for a patent that details how blockchain technology can be used to store data related to drone flights, with solutions aimed at facilitating the commercialization of drone applications.

Compared with the industry's exploration of blockchain in the commercial field of drones, the academic community is more focused on using blockchain to solve the security issues of drone systems. In terms of data confidentiality, the [13] proposed a blockchain-based system that protects drones from transmitting location data and prevents line-of-sight obstruction. [14] proposes an intelligent framework based on blockchain technology to defend against leak attacks by establishing an account and a unique identification code for each device. Data integrity In terms of data availability. [15] proposes a distributed solution that uses blockchain technology and cloud servers to ensure UAV communication and data integrity. In terms of data availability [16] uses certificates issued by a central authority to help UAVs resist DoS. Attack; [17] regards each drone in the drone cluster as a node of the blockchain, and each drone saves a copy of the data, effectively preventing blocking attacks.

Among the existing solutions, the applications in the corporate world are oriented to the commercial field and mainly use the traceability of blockchain to supervise drones. However, the academic research on the Solana blockchain in drone collaboration is only at the theoretical level and lacks an understanding of the situation. Exploration of specific technical routes. Therefore, this article will focus on the specific implementation of the integration of the Solana blockchain and drones, defining the network structure designing the transaction process, and providing a complete solution to solve the safety and security issues of drone collaboration.

3. Model establishment

3.1. UAV-Swarm Net network structure

UAV-Swarm Net consists of three roles: Ground Control Base Station (GCS), Master UAV (MasterUAV), and FollowerUAV. GCS is the combat command center in the traditional sense of UAS, which is responsible for controlling UAVs, flight process and trajectory, distributing combat tasks, maintaining [18] the normal operation of communication links, etc. The master drone and its submissive drones form a small drone cluster, and multiple small drone clusters are formed on demand Large UAV clusters. With the improvement of UAV autonomy, more and more control tasks are delegated from the GCS to the master UAV. The master UAV is responsible for controlling the submissive UAVs in its cluster and interacts with the GCS communicates in real-time with the master drones of other clusters and participates in collaborative decision-making while the submissive drones can only perform tasks under the command of the GCS [19] and the master drone, collect intelligence information and report to superiors.

UAV-Swarm Net is built on the blockchain using the network Solana. Its basic network structure is shown in Figure 1. Organization R1 is composed of multiple GCS from different theaters and assumes the responsibility of the network administrator. The initial structure of the network is determined by the network configuration NC1 pre-established by organization R1, and it is started and managed by the administrator of R1. The small drone cluster participates in the network as an organization (R2, R3, and R4 in the figure represent different clusters respectively) [20]. To identify the identity of the organization members, the certificate is assigned to organization administrators and other network nodes and matches the certificate with the organization of the Solana blockchain network, effectively preventing illegal access to the UAV-Swarm Net network from the outside world.

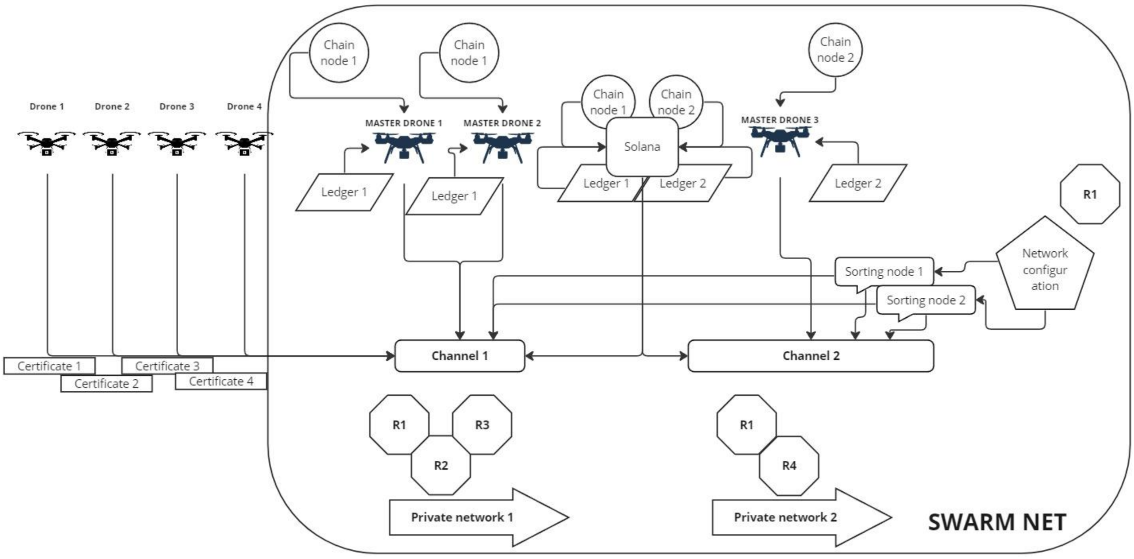


Figure 1: Network structure of UAV Swarm Net

According to the actual needs of drone operations, drone cluster organizations are added to different private networks. Organization R1 joins each private network and monitors the behavior of each drone cluster in real-time as the private network administrator. Internal communication and business isolation rely on channels, and communication between different private networks and different channels is completed through cross-chain channels. Each channel maintains a blockchain ledger, and only organizations that join the channel have the right to access and deploy the ledger and chain code of the channel. In the network shown in Figure 1, organizations R1, R2, and R3 belong to private network 1 and participate in channel 1, and organizations R1 and R4 belong to private network 2 and participate in channel 2. Therefore, organizations R1, R2, and R3 are internal network nodes that have the right to access the ledger and chain code of channel 1, and can also access the ledger data of other channels (such as channel 2) by registering cross-chain services [21]. The master drone participates in the network as a peer node in the organization. All master drones in the channel are deployed with a copy of the ledger. This multi-copy approach effectively avoids single points caused by the hijacking of the drone. Submissive drones participate in the network as blockchain users. They have the certificates of the cluster organizations to which they belong. They access the chain code and ledger deployed on their master drone through the client [22]. The query results of the ledger will be returned quickly to the submissive drone, but the update of the ledger will go through more complex processes such as endorsement and sorting. In addition to the master drone, GCS also assumes the responsibility of a peer node. It participates in multiple channels at the same time, so it deploys multiple Ledger and chain codes. The ordering node from R1 supports multiple channels at the same time to order transactions and distribute blocks.

3.2. Transaction process

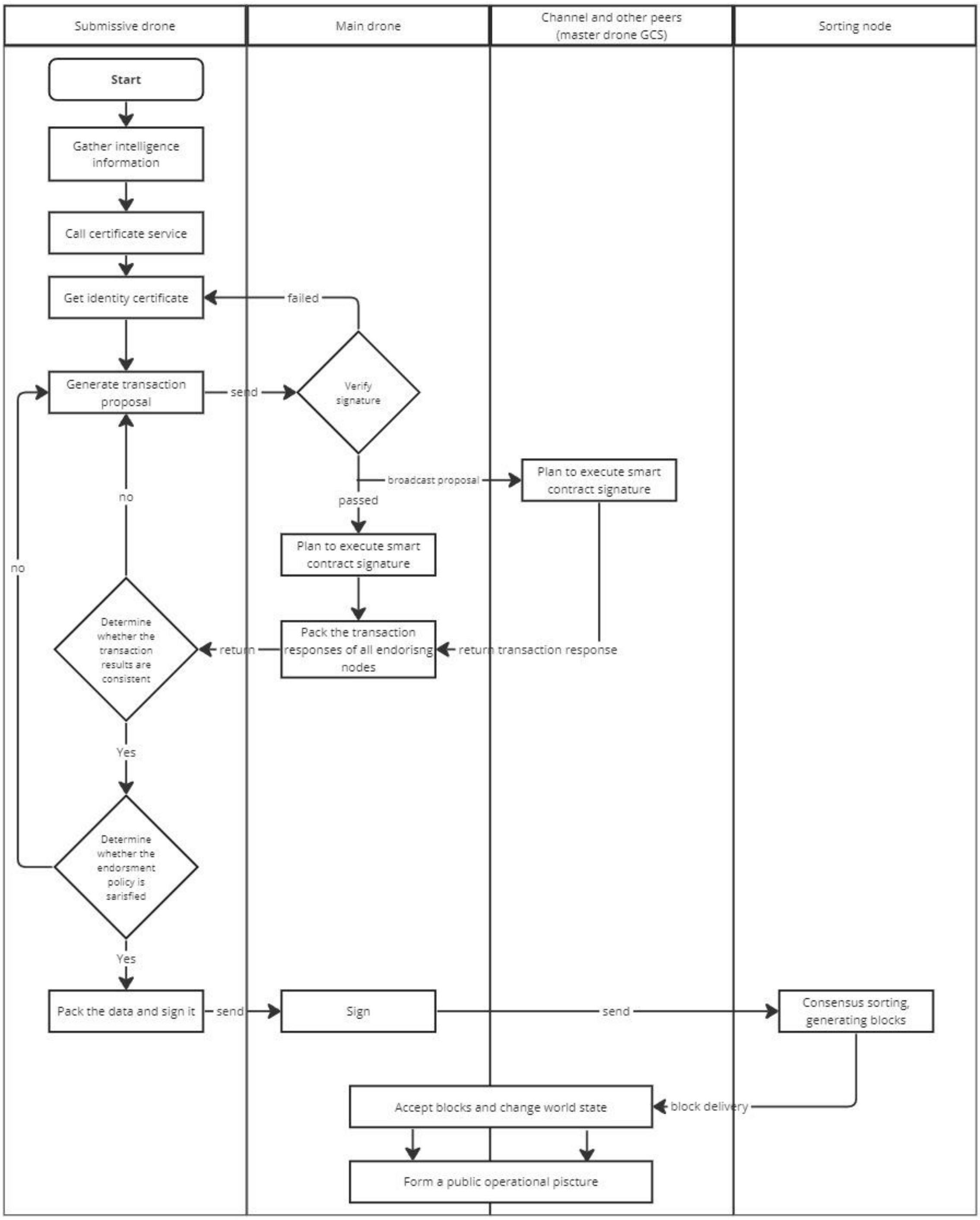
The ledger and chain code together form the core of UAV-Swarm Net. The ledger records all the intelligence information collected by the drone cluster from the start of the network; the chain code [23] is used for data sharing and collaborative decision-making between drones. The cooperative operation process of the UAV cluster is divided into the reconnaissance stage, the decision-making stage, and the execution stage. In the reconnaissance stage, each submissive UAV writes the collected local intelligence information into the account book by accessing the chain code on its master UAV and then distributes it to other peer nodes in the channel, and a shared public operational map is formed. In the decision-making phase, the main drone generates decision proposals based on the target status and real-time situation, and executes its own deployed decision chain code, allowing other nodes in the same channel to participate in collaborative decision-making through endorsement [24]; verified decisions are released to submissive drones through chain code events. The final execution phase is implemented.

The specific transaction process of the reconnaissance phase is shown in Figure 2. The local intelligence information collected from the drone through sensors or cameras is stored in the local database in the form of key-value. Before uploading the information, the drone must first pass the client's CA service to register and obtain the certificate. Subsequently, the submissive drone initiates a transaction proposal to the master drone to which it belongs [25]. The proposal contains the contract identifier to be called, the contract method, and all the intelligence collected from the drone within a period. The master drone after verifying the signature - the proposal is broadcast to other peer nodes in the channel. Through the endorsement of the node, the UAV-SwarmNet network conducts a security appraisal of the intelligence from the drone.

The endorsement node will verify the following contents of the proposal:

1. Verify whether the format of the transaction proposal is complete to prevent information data from being tampered with;
2. Verify whether the transaction proposal has been submitted before to prevent replay attacks;
3. Use MSP to verify whether the submissive drone's signature is valid and determine whether the submissive drone has been invaded;
4. Verify whether the submissive drone is authorized to operate on the channel.
5. After the verification is passed, the endorsement node will input the transaction proposal as a call the parameters of the chain code function are intended to execute the chain code and generate transaction results. Then the transaction results and the signature of the endorsing node will be returned to the master drone as a "proposal response", and finally packaged and sent to the submissive drone. The submissive drone verifies the signature of the endorsement node and compares the proposal results. If the proposal results are consistent and the signature of the endorsement node meets the endorsement policy, the submissive drone will package the data and send it to the ordering node through the master drone. The ordering node sorts the transactions and generates a zone [26]. The block is delivered to the peer nodes in the channel. Eventually, all peer nodes in the channel receive the block and change the world state. The UAV clusters then share intelligence information through the channel to form a

common public operational map, which is the intelligence foundation laid for subsequent decision-making stages.



Submissive drone
Main drone
Channel and other peers
(master drone GCS)
Sorting node
Start
Gather intelligence information
Call certificate service
Get identity certificate
failed
Generate transaction proposal
send
Verify signature
broadcast proposal
Plan to execute smart contract signature
passed
Plan to execute smart contract signature
no
no
Determine whether the transaction results are consistent
return
Pack the transaction responses of all endorisng nodes
return transaction response
Yes
Determine whether the endorsment policy is sarisfied
Yes
Pack the data and sign it
send
Sign
send
Consensus sorting, generating blocks
Accept blocks and change world state
block delivery
Form a public operational piscture

Figure 2: Transaction flowchart in the UAV reconnaissance phase

The chain code for uploading intelligence information contains a judgment on the authenticity of the intelligence. Once the judgment is wrong, UAV-Swarm Net will trace the responsibility based on the signature of the endorsement node, and adopt different punitive measures according to the intelligence level. If the intelligence level is higher, the uploader of the information the submissive drone, its master drone, and other peer nodes endorsing the transaction will be considered spy nodes, removed from the trust list of UAV-Swarm Net, and submitted to GCS for review and recycling. If a drone cluster If the main drone has deactivated its identity due to being implicated or suspended its work due to being invaded, one of the following two methods will be used to maintain the normal operation of the system:

1. GCS will assign a new main drone to take over the submissive drone;
2. The submissive drone with the most votes in the cluster is selected through the election and promoted to the master drone, becoming the new peer node of UAV-Swarm Net and taking over the task of controlling the cluster.

The transaction process in the decision-making phase and execution phase is roughly the same as that in the reconnaissance phase. The main difference is that the transaction proposal carrying the decision is initiated by the master drone and executed by the submissive drone. After discovering the mission target, the master drone conducts the transaction according to the current evaluation of the effectiveness of intelligence information and generates a combat plan. To avoid serious accidents caused by the main drone's decision-making errors, the UAS will assess the security level of the combat plan. Different security levels correspond to different endorsement strategies. For example, the plan to apply for a weapons strike adopts the highest security level and requires the endorsement of all master drones and GCS in the channel. When the decision is determined, the master drone releases a chain code event to the submissive drone. From none, the master drone registers these event types in advance, and when receiving notification of the occurrence of the event, it will immediately execute the corresponding command.

4. Model security analysis

First of all, UAV-Swarm Net provides a good guarantee for the confidentiality of data. UAV-Swarm Net sets network access restrictions based on the Public Key Infrastructure (PKI). Only issued by a specific organization CA can be obtained. Only users with certificates can obtain access to the channel through the verification of the MSP component, which lays a good foundation for the communication environment of the drone. In addition, UAV-Swarm Net uses the TLS transport layer for secure communication between communication nodes, through two-way verification ensuring the identity of both communicating parties and establishing a two-way encrypted channel. Intelligence data is converted into ciphertext using the encryption function when uploading to the chain. Only nodes with the key can interpret the intelligence information, effectively avoiding illegal intrusion into sensitive data.

Secondly, the immutability and multiple copies of the blockchain ledger ensure the integrity of the data, enabling the UAV system to resist improper modification and destruction of data by the outside world. Each main UAV and GCS in UAV-Swarm Net are deployed with an intelligence ledger of the channel to which it belongs, even if a master drone is hacked, the data can be restored by downloading the ledgers of other nodes. Both the intelligence upload of the submissive drone and the decision-making of the master drone require much time. GCS sites are endorsed by other master drones, and large GCS are usually difficult to hack, which greatly improves the reliability and credibility of intelligence and decision-making. The immutability of the ledger means that it is impossible to modify a certain block of intelligence information to change the current state database. Each block on the blockchain saves the on-chain data and the hash value of the previous block. If the data of the block is tampered with by hackers, it will cause the hash of the current block. The hash value does not match the hash value recorded in the next block so that security threats can be detected and alarms triggered. The traceability of the blockchain also establishes a monitoring mechanism for the drone system, through block transaction information and endorsement Signatures can quickly locate the compromised node and remove it from the trust list to avoid greater losses.

Finally, the decentralized nature of the UAV-Swarm Net network ensures the availability of the UAV system, allowing the UAV to access data information timely and reliably. As long as most nodes in the network do not encounter hacker attacks, the normal operation of the entire system can be ensured. In addition, the UAV-Swarm Net network also has high scalability.

By modifying the network configuration and adding channels, the establishment of small UAV clusters and the formation of large UAV clusters can be flexibly realized. The use of endorsement strategies can meet different levels of security requirements in actual combat missions.

5. Advantages and implementation challenges of the CDSS

The CDSS, leveraging Solana blockchain technology, introduces several groundbreaking advantages over traditional UAV management models. Primarily, the integration of blockchain ensures a decentralized, tamper-proof system that enhances data integrity, confidentiality, and availability. This decentralized approach mitigates the risks associated with centralized control, where a single point of failure could compromise the entire operation. Moreover, the Solana blockchain's capability for high transaction throughput and low latency underpins a responsive and scalable system, capable of handling dynamic, complex swarm operations without sacrificing operational tempo or security.

Advantages:

1. Enhanced Security and Robustness: The use of blockchain technology ensures that data shared across the network is immutable and transparent. This significantly reduces the risk of fraudulent activities and enhances the trustworthiness of communication among drones.
2. Decentralized Control: Unlike traditional systems that rely on a centralized command structure, the CDSS employs a distributed architecture. This ensures that the system is more resilient to attacks and failures, as there is no single point of failure that could bring down the entire network.
3. Improved Scalability: The Solana blockchain's high throughput capabilities enable the CDSS to scale efficiently, accommodating a large number of drones without compromising performance. This is critical for expanding operations and integrating new drones into the swarm without significant overheads.
4. Real-time Decision Making: Blockchain's inherent data integrity and the speed of Solana's consensus mechanism facilitate real-time decision making. This allows for rapid responses to changing operational scenarios, significantly enhancing the effectiveness of drone swarm operations.

Despite these advantages, implementing a CDSS based on blockchain technologies is not without its challenges. These include:

1. Technical Complexity: The integration of blockchain technology into UAV operations introduces a layer of complexity in terms of system design, development, and maintenance. Ensuring that all components work seamlessly together requires a high level of expertise and resources.

2. Energy Consumption: Blockchain operations, particularly those involving consensus mechanisms, can be energy-intensive. This might impact the energy efficiency of drones, reducing operational endurance and necessitating more frequent recharging or refueling stops.
3. Regulatory and Legal Challenges: The deployment of blockchain-based drone systems faces regulatory scrutiny, especially concerning airspace regulations, drone operation standards, and data protection laws. Navigating these legal frameworks and obtaining necessary approvals can be a lengthy and complex process.
4. Adoption Barriers: Resistance to change and skepticism about new technologies can pose significant barriers to the adoption of blockchain-based drone management systems. Overcoming these requires extensive stakeholder engagement, demonstrations of efficacy, and addressing concerns regarding safety, privacy, and cost.

6. Conclusions

This article defines the UAV-Swarm Net network structure based on the private chain Solana, explores the method of integrating blockchain technology with drones, and establishes a complete security protection solution for the collaborative operations of drone clusters. Blockchain technology is playing an important role while the UAV system improves robustness, security, and scalability, it also has many limitations. For example, the main UAV needs to maintain chain codes and ledgers, which will occupy a lot of memory; the main UAV is responsible for decision-making, endorsement, and controlling multiple tasks such as submissive drones will have an impact on its combat performance; GCS has weak control rights over submissive drones and cannot convey commands promptly. Future research will explore the integration of artificial intelligence to automate decision-making processes within the UAV-Swarm Net, potentially reducing human oversight requirements and enhancing response times. Additionally, advancements in quantum-resistant cryptography are identified as crucial to safeguarding against evolving cyber threats.

References

[1] S. Cohen, W. Nutt, Y. Sagic, Deciding equivalances among conjunctive aggregate queries, J. ACM 54 (2007). doi:10.1145/1219092.1219093.

[2] J. Cohen (Ed.), Special issue: Digital Libraries, volume 39, 1996.

[3] D. Kosiur, Understanding Policy-Based Networking, 2nd. ed., Wiley, New York, NY, 2001.

[4] D. Harel, First-Order Dynamic Logic, volume 68 of Lecture Notes in Computer Science, Springer-Verlag, New York, NY, 1979. doi:10.1007/3-540-09237-4.

[5] A. Z. Spector, Achieving application requirements, in: S. Mullender (Ed.), Distributed Systems, 2nd. ed., ACM Press, New York, NY, 1990, pp. 19–33. doi:10.1145/90417.90738.

[6] B. P. Douglass, D. Harel, M. B. Trakhtenbrot, Statecarts in use: structured analysis and object-orientation, in: G. Rozenberg, F. W. Vaandrager (Eds.), Lectures on Embedded Systems, volume 1494 of Lecture Notes in Computer Science, Springer-Verlag, London, 1998, pp. 368–394. doi:10.1007/3-540-65193-4_29.

[7] D. E. Knuth, The Art of Computer Programming, Vol. 1: Fundamental Algorithms (3rd. ed.), Addison Wesley Longman Publishing Co., Inc., 1997.

[8] S. Andler, Predicate path expressions, in: Proceedings of the 6th. ACM SIGACT-SIGPLAN symposium on Principles of Programming Languages, POPL '79, ACM Press, New York, NY, 1979, pp. 226–236. doi:10.1145/567752.567774.

[9] S. W. Smith, An experiment in bibliographic mark-up: Parsing metadata for xml export, in: R. N. Smythe, A. Noble (Eds.), Proceedings of the 3rd. annual workshop on Librarians and Computers, volume 3 of LAC '10, Paparazzi Press, Milan Italy, 2010, pp. 422–431. doi:99.9999/woot07-S422.

[10] D. Harel, LOGICS of Programs: AXIOMATICS and DESCRIPTIVE POWER, MIT Research Lab Technical Report TR-200, Massachusetts Institute of Technology, Cambridge, MA, 1978.

[11] K. L. Clarkson, Algorithms for Closest-Point Problems (Computational Geometry), Ph.D. thesis, Stanford University, Palo Alto, CA, 1985. UMI Order Number: AAT 8506171.

[12] D. A. Anisi, Optimal Motion Control of a Ground Vehicle, Master's thesis, Royal Institute of Technology (KTH), Stockholm, Sweden, 2003.

[13] H. Thornburg, Introduction to bayesian statistics, 2001. URL: http://ccrma.stanford.edu/jos/bayes/bayes.html.

[14] Poker-Edge.Com, Stats and analysis, 2006. URL: http://www.pkredge.com/statsYYFWWQ.php.

[15] B. Obama, A more perfect union, Video, 2008. URL: http://video.google.com/videoplay?docid=6528042696351994555.

[16] D. Novak, Solder man, in: ACM SIGGRAPH 2003 Video Review on Animation theater Program: Part I - Vol. 145 (July 27–27, 2003), ACM Press, New York, NY, 2003, p. 4. URL: http://video.google.com/videoplay?docid=6528042696351994555. doi:99.9999/woot07-S422.

[17] R. Yang, F. R. Yu, P. Si, Z. Yang, Y. Zhang, Integrated blockchain and edge computing systems: a survey, some research issues and challenges, IEEE Commun. Surv. Tutorials, 21 (2019), 1508– 1532. http://doi.org/10.1109/COMST.2019.2894727

[18] T. Ma, H. Wang, L. Zhang, Y. Tian, N. Al-Nabhan, Graph classification based on structural features of significant nodes and spatial convolutional neural networks, Neurocomputing, 423 (2021), 639–650. https://doi.org/10.1016/j.neucom.2020.10.060

[19] Y. Tian, B. Song, M. Murad, N. Al-Nabhan, Trustworthy collaborative trajectory scheme for continuous LBS, Int. J. Sens. Networks, 38 (2022), 58–69. http://doi.org/10.1504/IJSNET.2022.120275

[20] L. Fu, Z. Li, Q. Ye, H. Yin, Q. Liu, X. Chen, et al., Learning robust discriminant subspace based on joint L2,p- and L2,s-norm distance metrics, IEEE Trans. Neural Networks Learn. Syst., 33 (2022), 130–144. https://doi.org/10.1109/TNNLS.2020.3027588

[21] Q. Ye, P. Huang, Z. Zhang, Y. Zheng, L. Fu, W. Yang, Multiview learning with robust doublesided twin SVM, IEEE Trans. Cybern., 2021 (2021). https://doi.org/10.1109/TCYB.2021.3088519

[22] Q. Ye, Z. Li, L. Fu, Z. Zhang, W. Yang, G. Yang, Nonpeaked discriminant analysis for data representation, IEEE Trans. Neural Networks Learn. Syst., 30 (2019), 3818–3832. https://doi.org/10.1109/TNNLS.2019.2944869

[23] Z. Tong, F. Ye, M. Yan, H. Liu, S. Basodi, A survey on algorithms for intelligent computing and smart city applications, Big Data Mining Anal., 4 (2021), 155–172. https://doi.org/10.26599/BDMA.2020.9020029

[24] J. H. Anajemba, T. Yue, C. Iwendi, M. Alenezi, M. Mittal, Optimal cooperative offloading scheme for energy efficient multi-access edge computation, IEEE Access, 8 (2020), 53931–53941. https://doi.org/10.1109/ACCESS.2020.2980196

[25] S. Guo, X. Hu, S. Guo, X. Qiu, F. Qi, Blockchain meets edge computing: a distributed and trusted authentication system, IEEE Trans. Ind. Inf., 16 (2020), 1972–1983. https://doi.org/10.1109/TII.2019.2938001

[26] P. Zhang, C. Tian, T. Shang, L. Liu, L. Li, W. Wang, et al., Dynamic access control technology based on zero-trust light verification network model, in 2021 International Conference on Communications, Information System and Computer Engineering (CISCE), (2021), 712–715. https://doi.org/10.1109/CISCE52179.2021.9445896