Development of Algorithm for Blockchain and Artificial Intelligence Collaboration to Identify Travel Path of UAVs

Dr Hitesh kumar Nimbark
Professor, Gyanmanjari Institute of Technology,
Gujarat, India

Abstract

Computational intelligence is the backbone of the next generation applications like unmanned aerial vehicle, man less missions; and aerospace research. Blockchain technology and artificial intelligence can be collaborated to achieve secure executions. This paper presents the new algorithm “UAV Path Predictor” which intends to predict the optimum secure path coordinates. It is necessary to pre-define the travel path of the UAV based on surveillance target geographical territory. In case of existing flight path availability, it is important to store possible shortest path coordinates as a historic dataset which can be referred for future flight of UAVs. Also, if multiple UAVs flights are scheduled concurrently, there is a possibility of collision hence, for improved security proposed method suggests the CNN module which recurrently analyzes the multiple paths which gets stored in blockchain blocks. Thus, blockchain provides fast processing with the collaboration of CNN module collaboration.

Keywords: UAVs, CNN, Artificial Intelligence, Blockchain, Machine Learning, Recognition Algorithms, Decision-making Algorithms.

1. Introduction

In the past two decades, there has been a rapid development in the drone industry known as Unmanned Aerial Vehicles (UAVs). Currently, the use of commercial UAVs has increased a lot due to their affordability, but lack of security implementations has introduced many threats and vulnerabilities in UAVs [1]. Due to some illegal users and malicious interference, the electromagnetic environment (EME) for UAVs is increasingly complex. As an airborne electronic system, the data link is easy to be interfered by external electromagnetic interference (EMI), resulting in an abnormal communication, an interruption or even a damage [2]. A variety of measures can be used to protect critical infrastructure from UAV threats, including physical barriers, security drones, UAV detection and defense systems, and airspace management systems. It is also important to develop technologies for detecting and intercepting UAVs in order to quickly respond to threats and prevent possible attacks [3].

Recently emerging technology blockchain could be one of promising ways to enhance data security and user privacy in peer-to-peer UAV networks. Borrowing the superiorities of blockchain, multiple entities can communicate securely, decentralized, and equitably. This article comprehensively overviews privacy and security integration in blockchain-assisted UAV communication. For this goal, we present a set of fundamental analyses and critical requirements that can help build privacy and security models for blockchain and help manage and support decentralized data storage systems [4]. Refer Fig.1 for aerospace application layers to be secured. Refer Fig. 1 for possible application layer utilities.

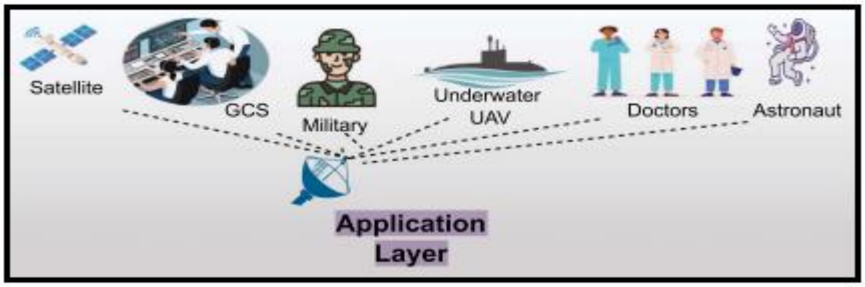

Fig.1: Application layer for aerospace security (Hafeez, S., Khan et al, 2023)

Pentatope elliptic curve encryption is used to protect data in the cloud in the context of the proposed system. Drones and other UAVs have a distributed design in terms of data communication. The distributed design in drones and other UAVs refers to the way data are communicated among different components of the drone. Instead of having a centralized system that processes and stores all data, the information is distributed across multiple units, each responsible for a specific task. For example, the flight control system, the sensors, and the communication module can all be separate units that communicate with each other using a network. This enables each component to process data in real time, leading to faster decision making and improved overall performance. Additionally, the distributed design can also improve reliability and safety by reducing the impact of a single component failure. If one unit fails, the other components can continue to operate, maintaining control of the drone and preventing a catastrophic failure [5].

Artificial intelligence (AI) is the science used to develop techniques that can think like humans or even beyond humans' intelligence. One of the critical features addressed by AI is the ability to learn and adapt. Therefore, AI techniques are a suitable candidate to apply to UAV networks with their fluid technology and other challenging characteristics. Many network researchers are currently exploring AI applications in UAV network domains. AI-based security solutions are being suggested for various cyber-attacks, including cyber-physical attacks. The authors have proposed using convolutional neural networks (CNNs) and recurrent neural networks (RNNs) to identify and classify high-risk areas and various motion characteristics of UAVs [6]. Deep Learning (DL), a subset of machine learning (ML) based on artificial neural networks, has experienced significant advancements in recent years. While it has demonstrated remarkable capabilities in various domains, the true potential of DL shines when it is applied to real-world problems [7].

Computational intelligence assists the UAVs and set ups to comprehend the humane practices themselves and consequently respond in a manner that is managed effectively towards the end user of that individual program, model, etc. Several distinctive learning computations are utilized to accomplish the idea where the vital development starts training and validation at each application and network layer of data which can be processed through blockchain. Hence, in Section 2 we provided existing literature studies, Section 3 discusses the proposed algorithm and model whereas Section 4 concludes the paper with future development aspects.

2. Literature Review

Author's objective is to develop an innovative and AI-driven automation system that leverages state-of-the-art perceptive technologies for creating an ideal self-regulating video surveillance model. The system is designed to optimize real-time monitoring and enhance threat detection capabilities through advanced AI algorithms and cutting-edge computer vision techniques. By harnessing machine learning and deep learning methodologies, the model aims to achieve unparalleled accuracy in detecting and analyzing potential security breaches and anomalies [8]. This further can be enhanced by means of UAV path finder using blockchain network analysis.

According to the author, navigation, the lifeblood of autonomous systems, has also undergone a seismic shift due to AI integration. Path planning and control algorithms, powered by AI, enable autonomous vehicles, drones, and robots to chart safe and efficient courses through intricate and unpredictable terrain. Adaptive control strategies provide the necessary flexibility to navigate rapidly changing environments, ensuring not only safety but also optimal performance. Collision avoidance algorithms, with their real-time detection and response mechanisms, act as a crucial safety net, preventing accidents and ensuring the well-being of passengers, operators, and bystanders [9]. For blockchain architecture refer following Fig.2.

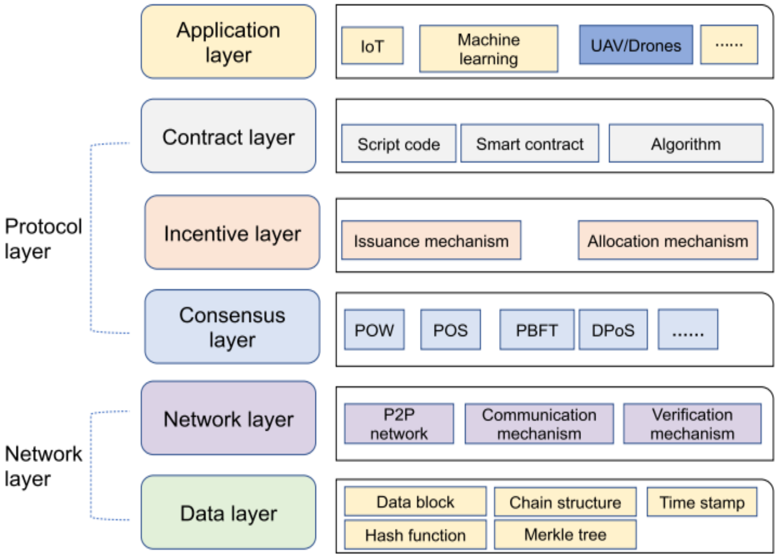

Fig. 2: Blockchain Architecture (Zhu, C.,et al., 2022)

More recently, the concept of federal learning (FL) has been set up to protect mobile user data privacy. Compared to traditional machine learning, federated learning requires a decentralized distribution system to enhance trust for UAVs. Blockchain technology provides a secure and reliable solution for FL settings between multiple untrusted parties with anonymous, immutable, and distributed features. Therefore, blockchain-enabled FL provides both theories and techniques to improve the performance of intelligent UAV edge computing networks from various perspectives. Author’s survey discussed the current state of research on blockchain and FL and compared the leading technologies and limitations. Also, author discussed how to integrate blockchain and FL into UAV edge computing networks and the associated challenges and solutions [10].

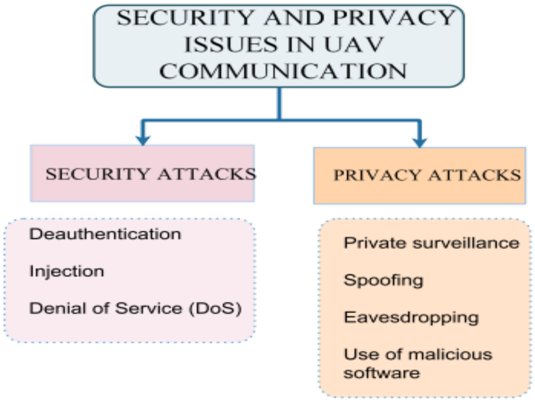

Fig.3: UAV Security Areas (Saraswat, D.et al., 2022)

UAVs are resource-constrained, with limited power and battery, and thus centralized cloud-centric models are not suitable. Moreover, as exchanged data is through open channels, privacy and security issues exist (refer Fig. 3 above). Federated learning (FL) allows data to be trained on local nodes, preserving privacy and improving network communication. However, sharing of local updates is required through a trusted consensus mechanism [11]. Employing UAVs in the Aviation 4.0 era will minimize the human dependency level of the aviation management systems. Embedding UAVs with Blockchain technology (BCT) might become an increasing phenomenon since the UAVs should be operated in an environment with many obstacles and possibilities of cyber-attacks. If UAVs are used in multi-agent systems that smart contracts have been prepared and planned for them, UAVs can be programmed to make decisions on their own. One of the notable cases in this regard is the use of UAVs in BCT systems related to the category of Atrium BCT [12].

However, the untrusted party's misuse of the UAV may violate the security and even demolish the critical operation in the IoMT system. In addition, data manipulation and falsification using unauthorized access are the significant challenges of the Internet-of-military-things (IoMT) system. In response to this problem, author suggested a blockchain integrated convolution neural network (CNN)-based intelligent framework named IoMT-Net for identification and tracking illegal UAV in the IoMT system. Blockchain technology prevents illicit access, data manipulation, and illegal intrusions, as well as stored data on the central control server (CCS) [13].

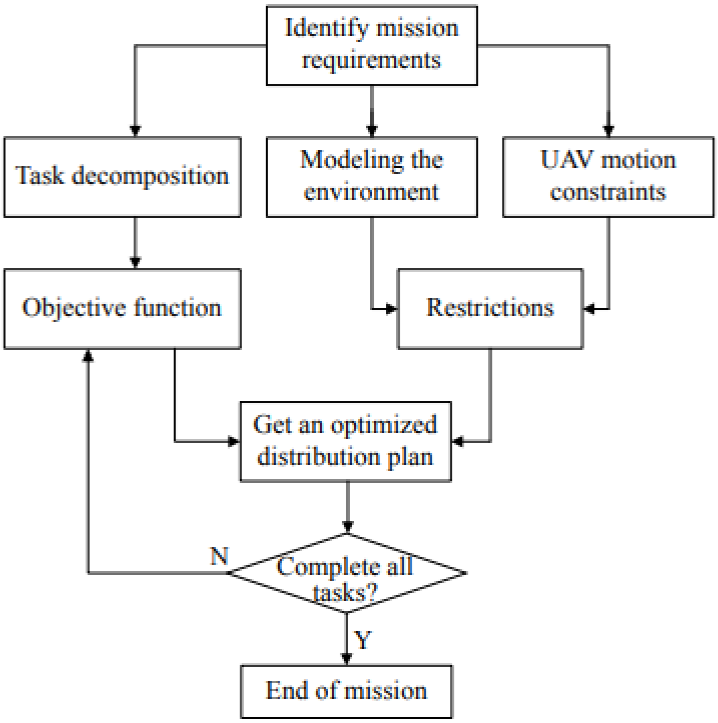

Fig. 4: UAV swarm task allocation process (Husheng, W. U. et al., 2021)

With reference to Fig.4 above, it is difficult for the double suppression division algorithm of bee colony to solve the spatio-temporal coupling or have higher dimensional attributes and undertake sudden tasks. Using the idea of clustering, after clustering tasks according to spatio-temporal attributes, the clustered groups are linked into task sub-chains according to similarity. Then, based on the correlation between clusters, the child chains are connected to form a task chain. Therefore, the limitation is solved that the task chain in the bee colony algorithm can only be connected according to one dimension [14].

Author aimed to enhance the performance of UAVs with a decentralized machine learning framework based on blockchain. The suggested framework has the potential to significantly enhance the integrity and storage of data for intelligent decision making among multiple UAVs. Author also presented the use of blockchain to achieve decentralized predictive analytics and present a framework that can successfully apply and share machine learning models in a decentralized manner. Further, author evaluated the system using collaborative intrusion detection as a case-study in order to highlight the feasibility and effectiveness of using blockchain based decentralized machine learning approach in UAVs and other similar applications [15].

3. Research Methodology

Although AI-based UAV network structure is a continual study area, we have to target on several crucial elements, incorporating security and privacy, network design, localization and trajectory, and standard uses of UAVs that are required for the effective structure and deployment of next-generation UAV networks.

Non-collision of UAVs with one another and no dysfunction in the data system and transmission by UAVs is among the very important factors. These kinds of challenges significantly and cautiously need to be analyzed, and the presence of all these preferences in any network of UAVs needs to be verified. Various features of UAV network shown in Fig.5 below.

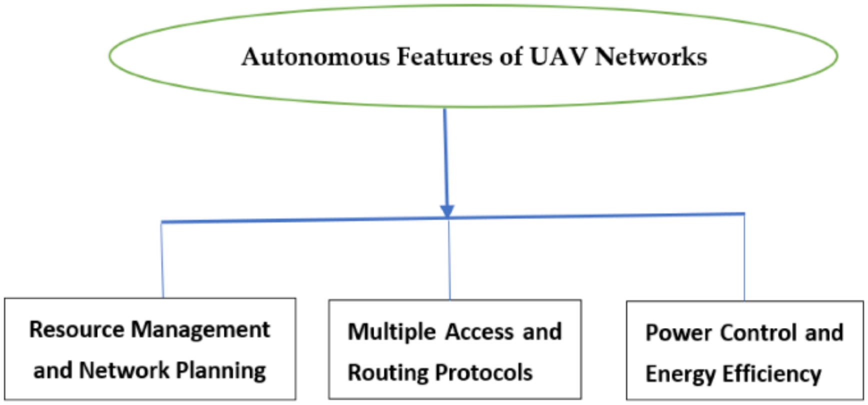
Autonomous Features of UAV Networks
Resource Management and Network Planning
Multiple Access and Routing Protocols
Power Control and Energy Efficiency

Fig.5: Autonomous features classification for UAV networks (Sarkar, N. I. et al., 2023)

Also, to track the UAV with possible shortest paths it is necessary to store the UAV coordinates as a dataset. The CNN classifier can classify the shortest and secure path whereas blockchain blocks will forward coordinates to UAV for further travel plan. If any obstacle is mapped as per the graph theory, blocks will store the previous information. The proposed algorithm is presented as:

Algorithm 1 UAV PathPredictor

Input: UAV’s launching_region and destination _region blocks

launching_region = Block_X

destination _region = Block_Y

```
Block_N=array travel_path[n]   // Store pre-defined travel point coordinates to block
Block_M=array travel_path_history[m] // Store existing travel point coordinates to block
if (Block_N != null)
then record time elapsed between Block_X & Block_Y
Store path coordinates to Block_M
else  apply AI_classifier to make route decision for future flight
if  (max_pooling !=0 && Block_M !==0)
then apply convolution neural network (CNNPredictor)  //suggest optimum travel path
else UAVs flight ==On_hold  // No permission to fly on existing  travel path
end if
```

As the decision-making procedure for UAV path, which is the decision of an alternate choice between several possibilities, is a binary path points with zero or one, UAVs designate zero or one to each one of these possibilities subsequent to path planning for every decision. To select the ideal option involving many alternatives, the one with the maximum number of factors is chosen and executed.

4. Conclusion

In this paper new UAV PathFinder algorithm is presented based on the research gaps identified. The collaborative execution of artificial intelligence and blockchain is feasible for real-time data capture and storage as a historical travel path for almost any aerospace object. The study focused on surveillance UAVs travel path to avoid the collision as well as to identify shortest path using convolution neural network training. We would like to suggest the more efficient application as a future utilization of UAVs as a PeacePromoter for community in scenario of natural disaster management and emergency support. In case of natural disasters, it becomes difficult to identify geographical safe path coordinates so; using proposed research historical coordinated can be very useful.

References

[1] Hadi, H. J., Cao, Y., Nisa, K. U., Jamil, A. M., & Ni, Q. (2023). A comprehensive survey on security, privacy issues and emerging defence technologies for UAVs. Journal of Network and Computer Applications, 213, 103607.

[2] Xu, T., Chen, Y., Wang, Y., Zhang, D., & Zhao, M. (2023). EMI Threat Assessment of UAV Data Link Based on Multi-Task CNN. Electronics, 12(7), 1631.

[3] Pohasii, S., Korolov, R., Dzheniuk, N., Jammine, A., Andriushchenko, T., & Milevska, T. (2023, June). Decision Making in Managing the Choice of UAV Threat Detection Systems in the Protection of Critical Infrastructure Facilities. In 2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1-6). IEEE.

[4] Hafeez, S., Khan, A. R., Al-Quraan, M., Mohjazi, L., Zoha, A., Imran, M. A., & Sun, Y. (2023). Blockchain-Assisted UAV Communication Systems: A Comprehensive Survey. IEEE Open Journal of Vehicular Technology.

[5] Aljumah, A., Ahanger, T. A., & Ullah, I. (2023). Heterogeneous Blockchain-Based Secure Framework for UAV Data. Mathematics, 11(6), 1348.

[6] Sarkar, N. I., & Gul, S. (2023). Artificial Intelligence-Based Autonomous UAV Networks: A Survey. Drones, 7(5), 322.

[7] Velayutham, V., Chhabra, G., Kumar, S., Kumar, A., Raha, S., & Saha, G. C. (2023). Analysis of Deep Learning in Real-World Applications: Challenges and Progress. Tuijin Jishu/Journal of Propulsion Technology, 44(2).

[8] Nadaf, J., Patil, T. B., kumar Lavate, R., Beldar, M., Abhang, R., Abbad, S., & Kadam, A. (2023). Innovative AI-driven Automation System Leveraging Advanced Perceptive Technologies to Establish an Ideal Self-Regulating Video Surveillance Model. Tuijin Jishu/Journal of Propulsion Technology, 44(2).

[9] Kumar, N., Chandola, D. C., Sudman, M. S. I., Hajoary, D., Singh, V., & Prakash, R. (2023). Exploring the Use of AI in Autonomous Vehicles, Drones, and Robotics for Perception, Navigation and Decision-Making. Tuijin Jishu/Journal of Propulsion Technology, 44(3), 01-09.

[10] Zhu, C., Zhu, X., Ren, J., & Qin, T. (2022). Blockchain-enabled federated learning for UAV edge computing network: Issues and solutions. Ieee Access, 10, 56591-56610.

[11] Saraswat, D., Verma, A., Bhattacharya, P., Tanwar, S., Sharma, G., Bokoro, P. N., & Sharma, R. (2022). Blockchain-based federated learning in UAVs beyond 5G networks: A solution taxonomy and future directions. IEEE Access, 10, 33154-33182.

[12] Barenji, R. V., & Nejad, M. G. (2022). Blockchain applications in UAV-towards aviation 4.0. Intelligent and Fuzzy Techniques in Aviation 4.0: Theory and Applications, Springer, 411-430.

[13] Akter, R., Golam, M., Doan, V. S., Lee, J. M., & Kim, D. S. (2022). IoMT-Net: Blockchain-Integrated Unauthorized UAV Localization Using Lightweight Convolution Neural Network for Internet of Military Things. IEEE Internet of Things Journal, 10(8), 6634-6651.

[14] Husheng, W. U., Hao, L., & Renbin, X. I. A. O. (2021). A blockchain bee colony double inhibition labor division algorithm for spatio-temporal coupling task with application to UAV swarm task allocation. Journal of Systems Engineering and Electronics, 32(5), 1180-1199.

[15] Khan, A. A., Khan, M. M., Khan, K. M., Arshad, J., & Ahmad, F. (2021). A blockchain-based decentralized machine learning framework for collaborative intrusion detection within UAVs. Computer Networks, Elsevier, 196, 108217.