Blockchain-based Secure Data Transmission for UAV Swarm using Modified Particle Swarm Optimization Path Planning Algorithm

M.Kayalvizhi[1]
Research Scholar: Computing Technologies Department
SRM Institute of Science and Technology
Chennai, India

Dr.S.Ramamoorthy[2]
Associate Professor: Computing Technologies Department
SRM Institute of Science and Technology
Chennai, India

***Abstract*—With the rapid development of unmanned aerial vehicles assisted applications enabled with a communication system, they are open to various malicious attacks. As a new form of flying things, they can access the network for better communication via the aerial base station. Most of the Unmanned aerial vehicles assisted flying objects' optimal path selection schemes does not consider the path deviation. In path deviation attacks, secure data transmission are not addressed in existing works. The secure communication process between Unmanned aerial vehicles and base station are exploited through security-based attacks. Moreover, path loss issue leads to multicast packet loss and unsecured broadcast. The existing network architecture setup does not fulfill the secure data communication and privacy issues. In this paper, Blockchain is utilized to investigate the secure communication between Unmanned aerial vehicles to Wireless Unmanned aerial vehicles Base stations. Since the destination information is dynamic under an uncertain environment, it will cause a delay in data communication. Unmanned aerial vehicles are more vulnerable to security attacks. The proposed blockchain-based architecture supports secure data communication in Unmanned aerial vehicles uncertain environments. To improve network security, this paper designs a modified particle swarm optimization method for better path selection. Through these experimental results, a blockchain-based data communication scheme is outer performed concerning network security.**

Keywords*—Unmanned aerial vehicles; path planning; swarm optimization; denial of service attack; blockchain; security and privacy; data communication

I. INTRODUCTION

Unmanned aerial vehicles (UAV) can be enabled with high flexibility based on harsh environment data communications. The major harsh environments are landscape country border monitoring, deep-sea monitoring, Industrial Monitoring, IoT agricultural monitoring, and UAV-based thermal tracking tool. UAV is one such potential communication field. The harsh environments can be monitored through UAV in large-scale integration with network security aspects. The UAVs are moving randomly across the environments with controller specifications to collect the information about network moving objects as well static ones. A UAV-enabled communication system is considered which will be a better one in between terrestrial and air medium. However, the available routing path up-gradation of the unmanned aerial vehicle is not enough to complete the data communication. Assuming the ideal path up-gradation is to determine the specifically targeted place of UAV or sink of the network that the UAV can carry the sensing details to reach them out. The UAV sensing data relay communication will face interrupt, distortion, and path selection issues. The analysis of relay network communication will affect the quality of data and communication time delay. The UAV data communication is defined with routing path state and data relay state. In such routing path up-gradation, the data can be broadcast via radio propagation. Once the jamming attacker enters into the UAV communication network it will remove the controller of the ground node from the attacker. The UAV network is controlled by the attacker and the UAV remote wireless sensor control ground node will be disconnected. The communication between the UAVs which are participating in the network needs to be secured since the data can be interpreted by a malicious attacker and the total mission can be compromised. The UAV device can also be compromised and it can be used against the UAV swarm. Most attacks focus on draining the resources which lead to the failure of the UAV mission. And to mitigate attacks on the modified swarm of UAVs, a secure authentication mechanism needs to be followed that identifies the participating UAVs identity and confirms that it is not malicious. The existing routing path selection process is updated through the conventional anti-jamming technique which focused only on transmit power functions with beamforming. The routing path selection should be highly controllable in the proposed algorithm. In UAV-based data communication facing optimal path selection in the wireless network and one of the recent experimental studies is conventional OSPF protocol-based path selection. The existing conventional scheme doesn't consider the successful data communication, time delay, and quality of the data. Due to the conventional path selection scheme implementing the trajectory planning didn't restrict the jammers' attack. The movements of UAVs like climbing angles and turnings are not restricted in the conventional method. However, the UAV's behaviour will affect the performance of the system.

The UAV's movements are reducing the higher risk of collision. The updated routing path will provide the ideal climbing angle to do the relay state communication. To handle these issues, UAV's multi-path selection is proposed and introducing successful data communication to improve the

performance of the UAV system. Routing path up-gradation is considered in the UAV communication process which is a novel proposal to remove the constraints. The constraints of path selection are identified as a research gap and the novel multi-path flashing meta-heuristic optimization algorithm is the proposed solution. To overcome such difficulties, a multipath flashing meta-heuristic algorithm is proposed to solve the path selection and up-gradation. The experimental numerical results show that the proposed algorithm can improve the UAV data communication process via optimized path selection design especially when there is high mobile traffic in the wireless network.

The high-speed increase of technologies in the wireless network has also simultaneously increased many challenges in data security. The data shared via networks need to be secured by strong encryption and cryptography mechanisms. The data are broken down into blocks in which each block consist of the data such as time, and the hash of the previous block. Blockchain plays a vital role to address the data security challenges and in preventing cyber-attacks. It ensures that the data available in the network cannot be tampered with or removed by any external users, who are not authenticated. The data can be added to the network only if its authenticity is verified by the peer nodes in the network. And if any malicious user tries to alter the data, the attacker needs to alter every block of the data, since the data blocks are interlinked and carries the hash of the previous block. So it will be a tedious task for the attacker to alter every consecutive block and gain access to the network.

The rest of the research paper is constructed with the following sections. In Section II, Existing works, analysis of existing objectives and results is discussed. Section III discusses the evaluation of path deciding factors for path planning. Further in Section IV, how blockchain secures UAV swarm and Section V UAV network-level Denial of Service Attack scenario further implementing blockchain settings, respectively. Section VI. The experimental level simulation settings and results are presented, further validating the blockchain performance in security and privacy in terms of data communication. Section VII discussions on simulation results and in Section VIII, the conclusion work is presented.

II. Existing Work

In this section, brief review details on the network security and path selection problem for UAV are discussed. The various path selection approaches are applied to find optimal path selection for UAV data communication.

T. Zhao, X. Pan and Q. He [1], the author proposed a dynamic Ant colony algorithm for path planning in UAV where the proposed algorithm is applied in the scenario of UAV reconnaissance. The main drawback of the Ant colony algorithm is that it will be effective in only a confined space. Optimal results are not guaranteed when the distance is increased. And the authors applied the algorithm on the UAV's which are deployed in a pre-planned location. This algorithm cannot be optimal when the UAV's target location is undefined and will not be feasible in an uncertain dynamic environment where the search space can be extended.

Li, Z., & Han, R. [2], the author studied the UAV flight path planning where the ant colony algorithm is used and a digital signal map is derived. The UAV movements are tracked in both vertical and horizontal directions, which will help to stimulate the UAV flight path. The proposed algorithm is not feasible when the threat area is dynamic and can't be optimal in real-time complex scenarios.

Bai, X., Wang, P., Wang, Z., & Zhang, L. [3], the author proposed a hybrid algorithm of an artificial bee colony and A* and studied on an iterative selection of arrival time where the UAV select the arrival time which is shortest and enhances the multiple UAV sequential arrival time. The proposed algorithm will not be suitable for the complex mission where the multiple UAVs needs to operate simultaneously to complete a task and the task offloading is not possible in this case.

Muntasha, G., Karna, N., & Shin, S. Y. [4], the author designed an algorithm anti-collision algorithm using an artificial bee colony where it optimizes the velocity of the UAV to reach the target. And an alternate path is designed if obstacles are detected. The proposed algorithm will be effective when the population size is increased. And it has a high computational cost.

Priyadarsini, P. L. K. [5], the author proposed an area partitioning algorithm and the area is partitioned as rectangles and midpoints are calculated for each partitioned rectangle which is further used for optimal path planning. And a graph is constructed by joining the midpoints and the optimal path is found using firefly and particle swarm optimization algorithm, where the results show that the particle swarm optimization algorithm is better than the firefly algorithm. But the proposed algorithm is not suitable for environments with dynamic obstacles.

Wei, Y., Wang, B., Liu, W., & Zhang, L. [6] the author focused on using an improved firefly algorithm for hierarchical task assignment. The author used the Metropolis criterion to avoid local optimum. And the firefly algorithm uses a multi-neighbour search algorithm to discretize the problem. The main problem in the proposed algorithm the defined parameters do not change over time and its not optimal in an uncertain environment where the targets are obstacles are dynamic.

Aliwi, M., Aslan, S., & Demirci, S. [7], the author used the firefly algorithm to find the best coverage area for the UAV placement for better communication and to reduce the consumption of energy. But this proposed work focuses only on one UAV and doesn't concentrate on multiple UAV environments. The optimal usage of battery power of the UAV is essential for effective communication. And since the firefly algorithm has a slow convergence rate and it can easily fall into local optimum.

Wang, S., Bai, Y., & Zhou, C. [8], the author proposed a method that focuses on yaw angle and height for mapping UAV devised on particle swarm optimization. Here the algorithm calculates the fitness value of each particle and the position of each particle is updated which outputs the optimal position. The main gap in the particle swarm optimization

algorithm is that the iterations don't guarantee the optimal result and it can easily fall into local optimum.

Aggarwal, K., & Goyal, A. [9], the author used particle swarm optimization algorithm to coordinate multiple UAVs for disaster management. The work focuses on locating humans in the disaster management site. The main gap in the particle swarm optimization algorithm is that it is influenced by the inertia weight and has low flexibility.

Evs¸en Yanmaz, Robert Kuschnig, Markus Quaritsch, Christian Bettstetter, and Bernhard Rinner., [10] discussed deterministic and probabilistic path planning algorithms, its drawback and benefits. They studied that the deterministic approach takes more time in deciding the action plan and probabilistic approaches can only give probabilistic guarantees in any task.

TarunRana, Achyut Shankar, Mohd Kamran Sultan, RizwanPatan, [11] Authors highlighting drones are controlled remotely via radio frequency and it makes the signal jamming in a susceptible manner. Radiofrequency jamming is a very frequent attempt from attackers. There are so many existing techniques that easily hack the drones and disconnect the communication channel. The UAV timestamp is a time log system that provides more security to the UAV. The timestamp follows the block which contains the hash value. The attacker changes the hash values and it creates a communication problem.

Jiyang Chen1, Zhiwei Feng2,1, Jen-Yang Wen1, Bo Liu, and LuiSha.,[12] author referring defending against UAV network internal Denial service of attack requires continuous tracking of all aspect running the system which creates huge overhead for the system. The real-time difficulties like system memory size, hardware capability, power consumption and reliability are hard to maintain the system functionality.

The above all related works in the optimal path planning in Unmanned Aerial Vehicle focuses on the coverage space which is already pre-defined and only finds an optimal solution in that defined coverage space. And the existing swarm algorithms such as Firefly, Ant colony, Artificial bee colony and Particle Swarm optimization algorithm all are capable of finding an optimal path in a search space where the target and the obstacle positions are pre-planned. It doesn't focus on dynamic targets and obstacles with the factor of uncertainty. When it comes to uncertainty, the navigation of UAVs is affected by many external factors. And the UAV system should be able to continue the mission when it is affected by external factors such as heavy gusts of wind, changing temperature, high altitude and moving obstacles. And another main security gap observed is secure communication. The data and the parameters defined should be securely communicated to the UAVs for a mission. And compromise of the data can lead to mission failure.

From the existing works, the optimal path algorithms such as Firefly algorithm, Iterative algorithm, Deterministic & Probabilistic Algorithm, GNSS and m-TSP mostly focus on the path selection in a static network environment. So, when these optimal algorithms are in an uncertain high mobility dynamic network, data loss and path deviation attacks are expected which compromises the successful data communication among the UAVs. The most frequently used optimal path algorithms and their limitations are listed out in Table I. The main research objective is to allow authenticated UAVs to operate in a high mobility dynamic environment and despite the uncertain factors and the path selection and the data transmission should happen securely and successfully. So based on these factors, a Meta-Heuristic optimization-based path planning model is proposed for path up-gradation aided with secure data communication.

TABLE I. COMPARISON OF EXISTING ALGORITHMS

Algorithm	**Comparisons of Existing Algorithms**			
	Advantages	***Limitations***	***Performance in a dynamic environment***	***Proposed Solution***
Firefly	Low UAV Energy Consumption	Limited Coverage	Partial environment	Need high coverage
M-TSP	Multi-Target	Not in Dynamic	Trilateration Method.	Dynamic Coverage
Genetic	Easy Target Access	Small Scale coverage	Limited	Need high coverage

III. PATH DECIDING FACTOR EVALUATION IN PATH PLANNING

The heuristic optimization system installed on an unmanned aerial vehicle network can provide a lot of changes in the uncertain environment from not only static UAV network secure data communication but also in high mobility UAV network. The features can be highlighted into two different levels of improvements, heuristic optimization path planning and secure data communication.

In this section, the Meta-Heuristic optimization-based path planning model is discussed in detail. Since the proposed modified swarm optimization method is developed with dynamic UAV movement which is influenced by the nearby base station and it is also guided exact UAV position based on the entire domain. There is no restriction on range. For evaluating the optimal dynamic UAV network Metaheuristic optimization method, an evaluation method is followed which maintains the distance of intra UAV path, energy level, and throughput and packet loss. The proposed metaheuristic optimization method provides exact distance measurement of intra UAV path which reduces the UAV minimum relay link requirements between the UAV nodes. This evaluation function is proposed as the fitness sum of mentioned parameters. The parameter functions are as follows:

$$In = \alpha \text{ x } UAVm / \Sigma i=ie + \alpha 1 \text{ x } 1/\Sigma i=ie1 + \alpha 2 \text{ x } 1/Tuav (\Sigma i=n (\Sigma i=ie + \Sigma i=ie1) / Tuav) \quad (1)$$

In the above-mentioned equation $\Sigma i=ie$, $\Sigma i=ie1$ is the distance between two UAV nodes and $\Sigma i=ie$, ie is the initial node energy level of the UAV network. After deciding the destination, the assigned UAV nodes get updated with the location of the destination, energy level and distance between the UAV nodes. These are the parameters considered in the UAV assisted UAV nodes. The Heuristic optimization

collected the UAV network data from the uncertain environment. The initial step evaluates the values of each UAV node and the instructions are proposed in the optimal path based on Meta - Heuristic optimization algorithm.

The UAV network node evaluation values are derived with the following equation (2). In this equation, the distance between two UAV nodes and UAV node data collecting capacity is utilized for UAV path deciding factors.

$$Pdf = \alpha 1 \text{ x } \sum i=1 \text{ j=1}(\sum i=ie \sum i=ie1) + \alpha 1 \text{ x} \sum i=1 \text{ A dc} \quad (2)$$

$\sum i=1$ $\sum i=ie1$ are represented values of the two UAV nodes, $\sum i=1$ A dc - Average Data Collection.

Path deciding factors (Pdf) are used to indicate the distance between UAV nodes ($\sum i=1$ j=1) Pdf. The collecting data capacity is calculated from the UAV node sensing quality which is frequently evaluated for path deciding factor.

The evolution method was initiated through UAV network node deployment and implemented Meta-Heuristic optimization, multiple UAV nodes are integrated high dynamic UAV network data communication and ensure privacy and security. Based on the UAV network, multiple numbers of UAV nodes are integrated and the evolution method calculates the path deciding values. The existing localization variable structure filtering problems and computational performance calculation occasional errors issues are overcome with evolution method path deciding values. The presented values are highlighted as deciding factors among the UAV network. In meta-heuristic optimization techniques are utilized for path planning and instant path selection. Among all the path planning and path up-gradation techniques in meta-heuristic term is mathematically optimized to select the upgraded instant path through high-level mathematical procedure specifically limited computational capacity and incomplete information structure. The path planning factors are discussed in the next section.

IV. UAV Swarm and Blockchain

Blockchain is a growing technology in the cyber security area and it's a promising technology in securing data and identity. It has many impacts in a wide range of areas in inventory management, the health industry and Internet of Things (IoT) in the domain of UAV.

The management of the UAV swarm is a critical task since it involves the coordination of multiple UAVs and the data communication in UAVs needs to be secured. And the security concerns are more when multiple UAVs are operating in a surveillance operation. And the main security challenge is to secure the UAVs in the network and to prevent the UAV swarm from security attacks such as denial-of-service attacks and ground control station jamming attacks. And to address these problems, Blockchain technology will be a promising solution. The UAVs in the swarm are registered with a valid key which will make them an authorized UAV in the network as depicted in Fig. 1. The UAVs which don't have valid keys will be automatically rejected by the UAV network. The blockchain maintains a distributed ledger and tracks the activity of the UAVs in the swarm network. And the collected data in the UAV are secured and cannot be tampered with. So, once the UAVs collect and store the data, the collected information is secured and it cannot be modified. Any slight modification in the blockchain will be detected and it will be rejected by the network. So, Blockchain will be effective in securing the UAV's identity and the data collected in the UAV swarm and preventing it from malicious attacks.

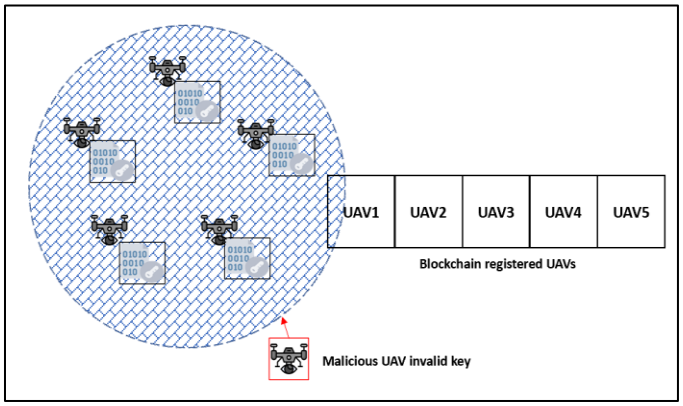

Fig. 1. A Scenario of an uncertain UAV Network.

The evolution factors are described for path planning constraint and the UAV nodes are followed updated searching state. The updated searching state is following three different segments finding the next hop duration in the assigned UAV network, UAV identity, and UAV location with the exact position. The described factors involved provide an updated routing path that ensures the security of data communication between two UAVs. UAV path planning convergence and combining matrix decomposition issues and multipath distortion errors are solved through this evolution constraints method. These three factors are updated through real-time values from the experimental part. The coordination of the factors kept maintains the updated routing table.

In such case the destination has not maintained the energy to carry over the data communication to reach the destination, the UAV communication node, exchange the data to reach the destination, the data exchange can be the safest way and the UAV network communication system should ensure the UAV node energy and threshold level. The UAV network routing table keeps the updated UAV path deciding factor parameters. To ensure the longest distance data communication between two UAV nodes, the updated parameter values are decided on the stability of the network. The local trajectory planner is applied in the decision mode which provides the current direction of motion based on parameter index. According to the current parameter values, the data communication is not suitable for direct communication then it is upgraded for indirect communication. Indirect communication is suggested if the stability of the network connection is not suited for direct communication. In this case, the routing table updates the revised path to make the indirect path.

The blockchain-based UAE server is responsible for forwarding the data. The UAV node energy details are managed through the UAV server. To improve the efficient data communication enhanced interior gateway routing protocol was implemented in the UAV mounted server

network. The high potential bandwidth creates better connectivity. This proposed blockchain-based architecture supports secure data communication in UAV uncertain environments. The enhanced interior gateway routing protocol in the UAV mounted server network is implemented which featured an advanced distance vector in x86 architecture and storage access. The secure data communication adopted asymmetric encryption and passed through meta-heuristic optimization. The enhanced interior gateway protocol updates the further position while the UAV node hovers the position in the assigned duration. So, the UAV node is prepared to move for a further position with the help of an updated routing protocol. The UAV node keeps the distributed ledger and it receives the encrypted data. The UAV node sends the encrypted data to the UAE server and the UAE server will check the encrypted data and allow meta-heuristic optimization. The meta-heuristic optimization forwards encrypted data to the UAE server and then the UAE server decrypted the data to get the actual data. The distributed ledger keeps the transaction of all the details within the UAV node and UAE server communication. The Malicious UAV node moves to the neighbour UAV nodes without following the updated routing table. The malicious UAV node exhausts the energy level due to unplanned moments in the uncertain environment.

V. Denial of Service Attack Scenario

The UAV network-level Denial of Service Attack scenario further implementing blockchain settings respectively are discussed. A scenario of Uncertain Environment UAV network is illustrated in Fig. 2. The heuristic optimization assists the system by protecting UAV network data Communication channel, memory and CPU utilization. The Implementation of this proposed system provides a secure UAV network.

A. System Model

The proposed heuristic optimization-assisted system is composed of a performance control system and security data system. The Optimization system controls the uncertain environment and maintains the performance. The controlling system provides optimized performance and advanced path planning with malicious activity avoidance. The proposed method running inside the uncertain environment UAV network is normally operated by industrial applications which have high secure architectures and update instant activities. The advanced optimization system will be practical to track the system and control the potential vulnerabilities.

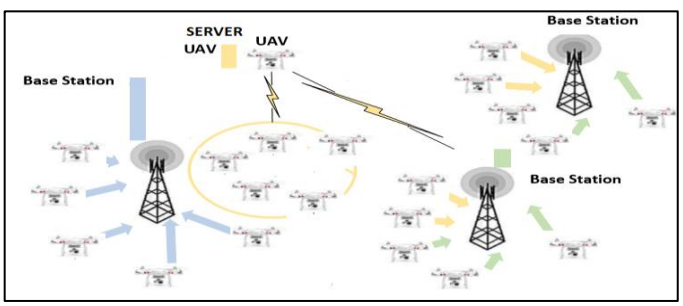

Fig. 2. A Scenario of an uncertain UAV Network.

The optimization assisted system refers to the client operating system and the security system running over on top of it. It is implemented for data security motive and maintains the simple systematic such that the system could be applied and analyzed. The client operating system process runs inside which ensures safety. The optimization controller rules the client operating system with simple modules which support the UAV network functionalities. The proposed system completely controls the uncertain environment in case of routing update failure for the path details due to a Denial-of-service attack which ensures a secure UAV network [13].

The main aim is to secure the data communication in the UAV swarm. The optimization system helps to regulate the security of the data in which it monitors the activity of the UAV nodes. So this will enable to track the position, UAV node energy capacity and distance from the base station for instant path planning.

A scenario of uncertain UAV networks is illustrated in Fig. 1. The optimization highlighted features in the uncertain environment, tracks the output from the client operating system. The identification of malicious activity, the tracking feature monitors the results from the client operating system and controls the major changes further [14].

B. Attacker Model

The real-time applications in the uncertain environment could maintain the data security in the initial stage, whereas the malicious embedded in an uncertain environment couldn't implement the optimization controller. The client operating system suffers adversary launch of Denial-of-service attack against the uncertain environment. The denial-of-service attack does not maintain the protection to overcome the optimization controller. The malicious movements do utilize the Denial-of-service attack to spoil the uncertain environment and UAV network performance [15].

C. CPU Denial of Service Attack Protection

In data security and CPU resource management, it will utilize the controlling system and maintain high performance. The CPU utilization priority improves against user requests. Every real-time application implements the first in first serve priority assignment; a high priority process could finish first and which is followed by the low priority [16]. This process helps the uncertain environment CPU utilization properly.

D. Memory Allocation and DoS Protection

The malicious movements in an uncertain environment could embed the Denial of Service (DoS) attack on the memory allocation by collecting a high amount of data from allocated memories which will affect the UAV network performance. The memory measurement feature encounters the CPU utilization in which the related system does not access the exceeding memory. The optimization controller uses the UAV network performance counter provided by the controller to monitor the memory access within the allocated period. The allocated period is maintained for accessing the memory without any restriction. It is highly suggested to resolve the memory constraint issues [17].

E. Data Communication DoS Protection

The optimization controller inside an uncertain environment maintains sensor data and utilizes client inputs to the UAV network to function properly [18]. The highlighted feature secures the system against DoS attacks. This will be required to control the uncertain environment and ensure system monitoring.

F. Simulation Mode

Times Sensible Sensors in uncertain environments are important components that should be protected from malicious activities in applications. The mandatory requirement in the simulation node is an optimization controller, where it doesn't control the memory access but will receive all necessary details from system activities. The thread activities showing in an uncertain environment will receive the data from sensor data and passes towards the optimization controller. This activity will arrest all Denial-of-service attack activities.

G. Data Security Monitoring

The scenario of an uncertain environment with a blockchain network is depicted in Fig. 3. The optimization controller maintains the network access to interface uncertain environment. To protect the uncertain environment from malicious activities, the UAV network controls have been separated in two ways.

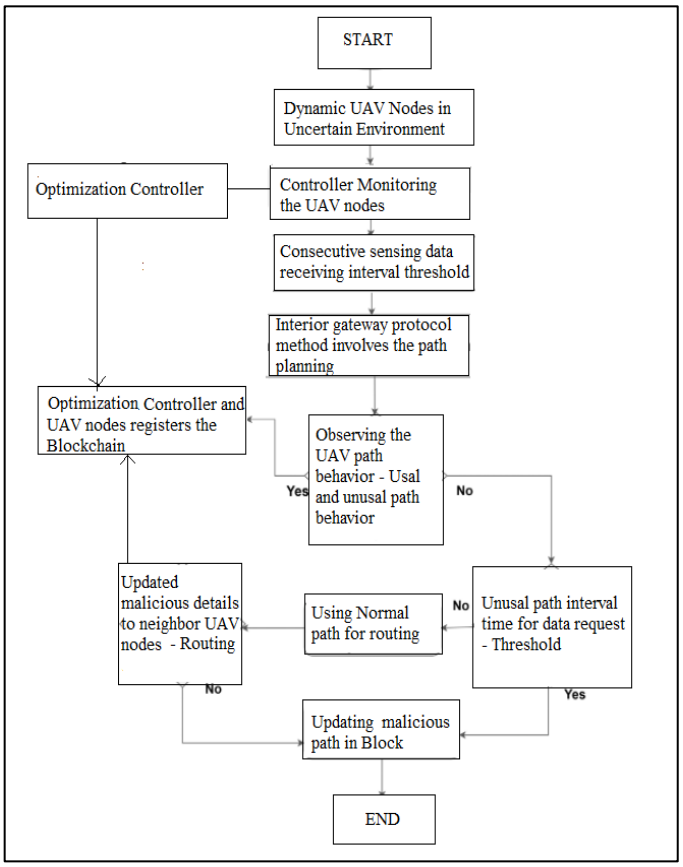

Fig. 3. A Scenario of Uncertain Environment with Blockchain Network.

The UAV network is deployed in an isolated application space where the UAV network does not have an internet connection to access data and through interface only it has to process the communication. An updated routing table is utilized to control the communication system which reduces the unwanted communication and damages caused by denial-of-service attacks. The modified swarm optimization method is developed with a dynamic UAV uncertain environment and identifying the positions in dynamic search space. The dynamic search space has identified the destination then the sender confirms the destination area which should not be smaller than pre-defined positions. The unrestricted area coverage is modelled with a sparse multi-link collaboration with unrestricted distance.

The optimization controller continuously monitors the results from the client operating system. The continuous monitoring system controls the uncertain environment and identifies the thread activity which diverts to the optimization controller. The consecutive sensing data receiving interval should not be set to a normal threshold and it should be set to average. The normal interval suggestions will fail the optimization controller.

VI. Experimental Results

The experimental level simulation settings and results are presented, further validating the blockchain performance in security and privacy in terms of data communication.

In this section, the Meta-Heuristic optimization algorithm is compared in experimental models and also various UAV environments. The ContikiCooja Experimental setup is introduced. In the cooja simulation, the area of interest is a 3Km radius. The main parameters utilized in our experiment are provided in Table II. The allocated bandwidth of each UAV node is assigned as 10 MHz. The other side of the UAV network servers also carries a 20 MHz band which means the high data traffic can be scheduled on the allocated bandwidth forwarded by the UAV nodes which could avoid congestion. The airframe spectrum range is assigned as 2.6, so the 20 MHz bandwidth can produce a 32 Mbps data rate. To this segment, here the UAV nodes are uniformly distributed on a geographical position. And the UAV nodes are operating in an uncertain environment with x = 22.45 and y=2.30 at 4 GHz carrier frequency. Considering the multipath flashing technology, the entire communication UAV network resources can be planned for a 180 Mbps data rate, which is the same as 25 Mbyte/s. The p is set as 10 x 103 which equates to the packet cost as 800 bits. In each UAV node, it has the packet cost in an uncertain field of each layer of the data transaction. The identification of the UAVs height and depth-dependent parameters α (h1) and δ(d1) are positioned according to the uncertain environment. The highest range of the position λnu is 24 ~36 dB while every UAV is at the height of 20m.In this experimental simulation, the value of λnu is assigned which is equivalent to the network locations of UAV node n and UAV servers. The special attention the subordinate UAV nodes in uncertain environment series location, share and update the values in λnu. The ideal value of the UAV network path loss is identified with the updated values and updates the location to the proposed path planning system.

TABLE II. SIMULATION PARAMETERS

Parameter	Description	Value
(X:Y)	Values in Uncertain Environment	(22.45;2.30)
p	Packet loss Cost (800 bit)	10x 10^3
λ_{nu}	Highest Range of the position	24~36 dB
α (h1)	UAV height	20m
δ(d1)	UAV depth	20m
R_{dr}	UAV Resource data rate (25Mbyte/s)	180 Mbps
UAV_c	UAV coverage radius	100~2000m
Eno	Total Episodes Number	10
N	Total UAV nodes	15
S	Total UAV server	1

A. Path Selection Scheme Evaluation

In this section, the access path selection scheme performance of the proposed Meta-Heuristic optimization algorithm is evaluated under an uncertain environment. The UAV node and UAV server scenario are executed. The sequence of the scenarios is considered for performance evaluations where all UAV nodes access the UAV server, one UAV server accessing all UAV nodes, and multipath flashing method. The multi-path flashing method always processes the UAV node with multipath channel access to the UAV server until the data traffic is cleared or all the UAV nodes are getting a response from the UAV server. The Meta-Heuristic optimization algorithm is hard to obtain the multipath flashing method due to the huge area and the comparisons with other schemes verify the performance of the proposed system. The ideal transformation straight line coordination system is produced to minimize the complexity and computational cost in the UAV path planning process. The existing methods produce high computational costs due to the complex optimization method.

Fig. 4 shows that the experimental radius of the region is occupied 900m, when the UAV coverage transmission radius is moving more than the assigned value of 900m, extended the excess UAV nodes wouldn't allow the transmission range and transmission cost.

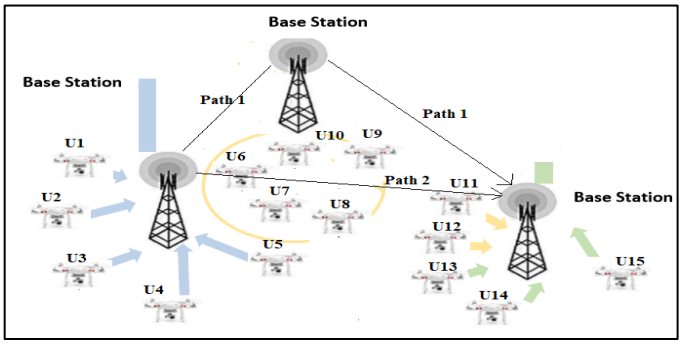

Fig. 4. Data Packet Transmission towards the UAV Network from Source to Destination.

The performance of the extended UAV nodes has a low packet transmission rate. Every uncertain environment UAV coverage is small about below 900m, the multipath flashing is done successfully in UAV node access in the UAV network. The assigned transmission range is fully occupied with resources and a scheduled pattern is achieved in the data traffic in the UAV network.

B. Multi-Path Flashing Model

This section proposes that countermeasures when multiple UAV nodes participate in the uncertain environment and investigate a scenario in which malicious activities and attacks are involved. The initial step of the environment that the attack could be using multipath signal receivers since every single attacker can spoil many numbers of receivers in its data transmission range. The attacker captures multiple signal receivers. The multiple numbers of signal receivers bounded the uncertain environment from which the attacker can be highly performed. The DoS locations depend on the UAV resource data range, called resource-based attack, constrained by the resource range between UAV nodes and UAV servers. The attacker activities purely depend on the locations, the possible position to reach the resources is suitable for them. The updated routing path keeps the updated routing details in a table. The update routing table keeps sending the details only to source and destination and the possible positions are set with two points. The fewer number of UAV nodes will entertain the attacks whereas a greater number of UAV nodes participated in uncertain environment UAV network doesn't allow to attack launch. The proposed system doesn't allow multiple UAV spoofing. The optimization method is based on defence cooperation localization. From these experimental results, the number of UAV node location is preserved and the distance maintained are safe [19]. The proposed distribution-based blockchain system spread out the defence model against spoofing attacks and the entire UAV network. The real experimental scenario offers multiple UAVs together, without any restrictions, offers opportunities for a DoS attack which encourages the malicious behaviour and captures the path. However, the defence model should also evaluate the attack behaviour and arrest the malicious activities [20].

C. Path Planning Algorithm Execution

Simulations were executed from this proposed enhanced interior gateway protocol method and tested through the following scenarios.

The testing is executed for observing the path planning of data packets from a UAV to another UAV when the attacker involves the usual routing paths. The process of sending data packets in transmission follows the usual links and avoids unusual paths where it occurs high computational costing. The experimental setup was tested using the EIGRP protocol and the computational cost and delay proves the proposed method and updates the instant path up-gradation at the time of execution. The proposed EIGRP protocol was tested through scenario 1 U1 to U11, Scenario 2 U2 to U12, Scenario 3 U3 to U13, Scenario 4 U4 to U14 and Scenario 5 U5 to U15.

TABLE III. COMPARISON VALUE OF DELAY IN PATH UP-GRADATION

Comparison value of delay in Path Up-gradation (seconds)					
Method	**Scenarios**				
	1	**2**	**3**	**4**	**5**
Proposed EIGRP	0.00634	0.00543	0.00435	0.00342	0.00234
Existing Routing	0.01245	0.01123	0.01103	0.01100	0.01023

The Table III results are obtained for the delay in path up-gradation resulting from the five different scenarios and the obtained delay in path up-gradation is as below:

1) Proposed EIGRP protocol

= (0.00634+0.00543+0.00435+0.00342+0.00234)/5

=0.004376 Seconds

2) Existing Path Up Planning Protocol

= (0.01245+0.01123+0.01103+0.01100+0.01023)/5

=0.011188 Seconds.

The Next scenario was tested before the path up-gradation attacker termination. The routing path considers for data packet transmission from U2 to U15 is U2 is switch UAV, Base Station 1, Base Station 2, Base Station 3 and U15 is Switch UAV. The path planning process is performed with different metric values which are utilized for sending data packets from source to destination.

Path Planning Metric = 256 * ((107/Minimum bandwidth) + (total path up gradation delay /10)).

The path planning up-gradation for sending data packets towards U2 to U15 with a minimum bandwidth of 200 kbps, delay 40000 ms, ethernet interface 200 ms delay, Path planning metric calculation is mentioned below,

Path Planning Metric= 256 *(107/200 kbps +(40000ms + 40000ms + 200 ms)/10) =53253120.

This value indicates that the data packet will send 53253120 metric values.

Metric values are derived for total path planning for data transmission from source to destination. Based on the Metric value calculation the updated routing details are distributed through a decentralized blockchain system with the existing network routing paths. The Distributed metric values based routing details support quickly and support multiple UAV's with normal computation delay and cost to reach the destination. The Proposed path planning algorithm overcomes the existing problems like restricted area path planning and specific autonomous area path planning. The low capability and minimized routing table with limited hop counts. These are the challenges that have been solved through the proposed path planning up-gradation model.

VII. SIMULATION RESULTS

Fig. 5, Fig. 6, and Fig. 7 are illustrated that the proposed algorithm in the case of uncertain environments performs better than the existing method since the UAV data transmission from one hop to another hop, neighbour count information, and received packets indicates the high impact created in the proposed algorithm. The proposed algorithm outperforms the novel approaches of path selection and moves directly to the uncertain UAV network environments all the time, and the improved performance gap between the proposed solution and the optimal access path selection solution is less than 3dB. The uncertain environment has the condition of attacker interception and when the average changing interval is suddenly increased, the proposed algorithm can perform the optimized path selection approach about crossing the malicious channel state path and outer performs a position with exact destination channel state, thus the overall performance is improved from the results provided by the proposed method.

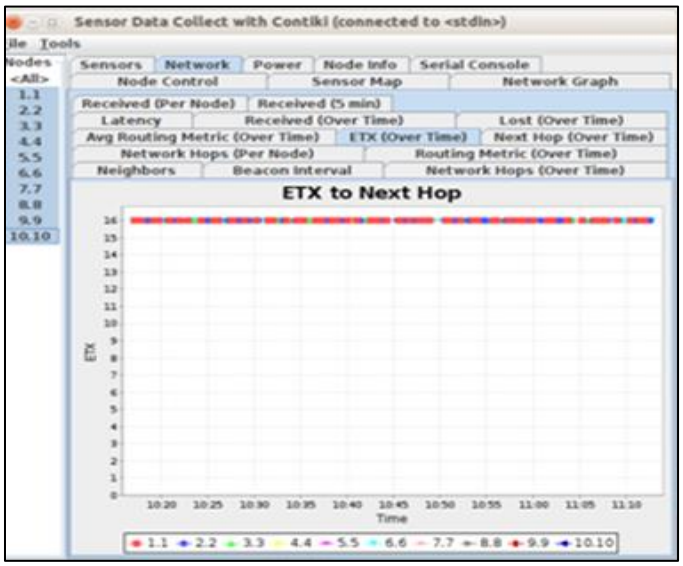

Fig. 5. Hop based Transmission Rate.

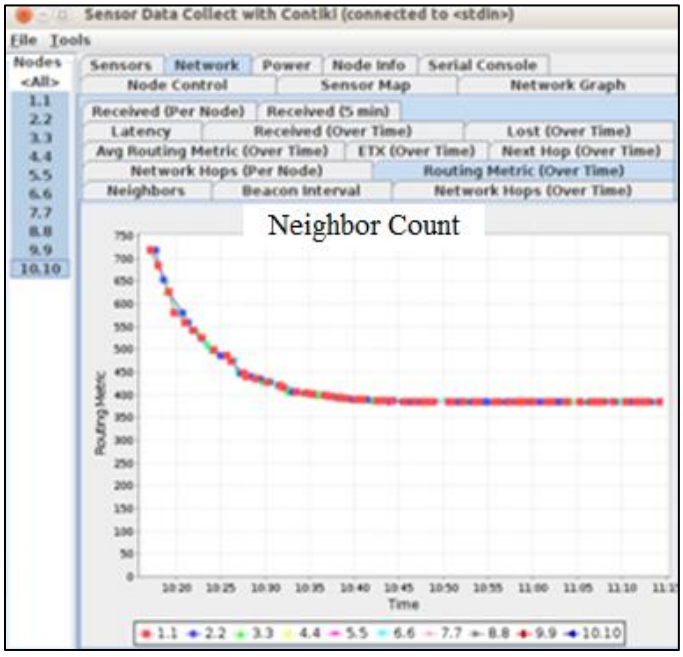

Fig. 6. Engaged Neighbour Count.

Fig. 5 shows that a high data transmission rate can reach a satisfactory result in the end, while the usage needed data transmission rate can reach a better result. Fig. 6 shows that high time engaged neighbour count can accelerate data transmission at the beginning stage; it will achieve the exact path selection methodology and does improve the data transmission in an uncertain UAV environment. Fig. 7 shows that the estimated received packets and estimated loss packets after implementing the proposed model.

The proposed algorithm is compared with GNSS based optimal access path selection approach of UAV flying object towards the same UAV network with different heights in Fig. 8. The existing Deterministic probabilistic algorithm and GNSS algorithm applied the fixed methodology to obtain the path where the fault tolerance was medium. Table IV shows the comparison of performance metrics between the existing Deterministic probabilistic algorithm and GNSS algorithm and the proposed optimization path selection and Meta-Heuristic path planning algorithm. The proposed Optimization path selection and Meta-Heuristic Path Planning algorithm apply a hybrid fuzzy possibility algorithm which creates the accurate destination path with dynamic location and overcomes the obstacle detection and radio path detection issues. Also, the Existing method does not provide proper ideology for data security against attacks whereas the proposed blockchain methodology, distributed the path location to the source point which creates smooth data delivery, no path deviation, and redirects path.

The proposed methodology reduces the time delay and improves the throughput. The uncertain UAV network environment is considered and the average channel path loss interval is set as 200s. The common value of the additional path loss λnu is very small when the UAV height is too high.

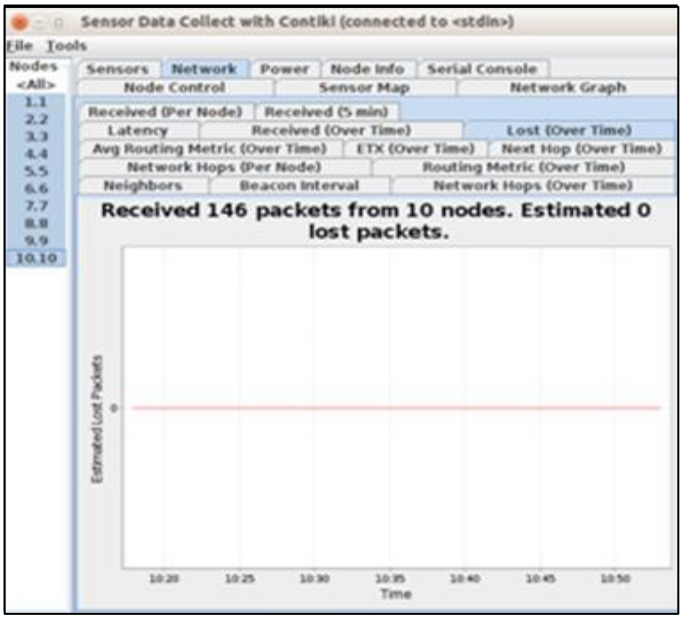

Fig. 7. Estimated Received Packets and Estimated Loss Packets.

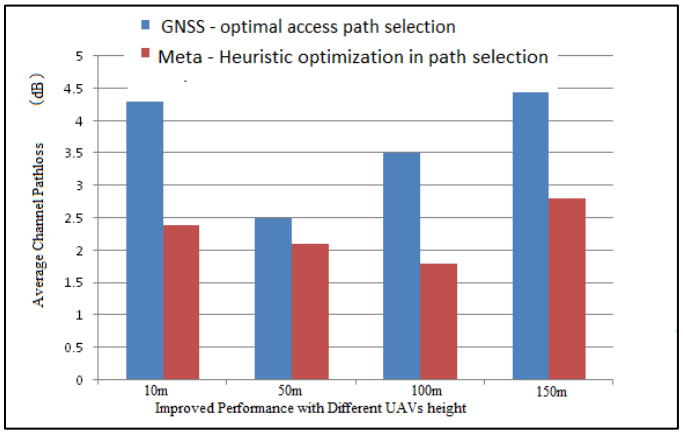

Fig. 8. Average Cost with different Values of UAV Coverage Radius.

TABLE IV. PERFORMANCE COMPARISONS OF META-HEURISTIC PATH PLANNING

Comparison Parameters	**Deterministic & Probabilistic Algorithm**	**GNSS(Global Navigation Satellite System-based Path selection Algorithm)**	**Proposed - optimization path selection and Meta-Heuristic path planning**
Technique Applied	Explore Obstacles	Radio Path detection	HFPCM-Hybrid Fuzzy Possibility
Throughput	Low	Low	High
Fault Tolerance	Low	Medium	High
Bandwidth	20%	25%	35%
Process Efficiency	35%	40%	50%
Node to Node Delay	30%	25%	10%
Security Improvement	Low Security	Normal Security	High Security
Overhead Latency	Low Priority & High Latency	Average Priority & Medium Latency	High Priority & Low Latency
Scalability	Low Adaptability	Medium Adaptability	High Adaptability
Packet Delivery Ratio	Low	Medium	High
Packet Loss	High	Medium	Low
Mean Time Delay	High	Medium	Low

VIII. CONCLUSION AND FUTURE WORK

In this paper, the issues in UAV assisted flying object optimal path selection schemes and the path deviation attacks against UAVs are investigated. The proposed model clearly defined the optimization path selection method and Meta-Heuristic optimization in path planning to effectively increase the secure data transmission in an uncertain environment UAV network, where extended coverage in real time scenarios of uncertain environment is successfully performed by the

proposed algorithm which is not addressed in the existing algorithms. The proposed blockchain aided UAV swarm will secure the UAV network from the security attacks. Blockchain provides promising results in the terms of preserving the security of the network. And tit can be implemented in the UAV domains for rescue operations, surveillance operations and inspection of critical resources. The secure communication process is proposed using blockchain and controlled the attack activities through a blockchain based defense distribution system. The distribution-based defense blockchain system supports, updated routing table which has been scheduled and the data is transmitted perfectly. In this paper, the results have been validated and swarm optimization controls the network security. In the future, experiments with multi-agent machine learning-based path selection in UAV networks with different environments will be considered and the energy consumption of a UAV which depends on its speed and transmits power will be discussed.

REFERENCES

[1] T. Zhao, X. Pan and Q. He, "Application of dynamic ant colony algorithm in route planning for UAV," 2017 Seventh International Conference on Information Science and Technology (ICIST), 2017, pp. 433-437, doi: 10.1109/ICIST.2017.7926799.

[2] Li, Z., & Han, R. (2018, July). Unmanned aerial vehicle three-dimensional trajectory planning based on ant colony algorithm. In *2018 37th Chinese Control Conference (CCC)* (pp. 9992-9995). IEEE.

[3] Bai, X., Wang, P., Wang, Z., & Zhang, L. (2019, July). 3D Multi-UAV Collaboration Based on the Hybrid Algorithm of Artificial Bee Colony and A. In *2019 Chinese Control Conference (CCC)* (pp. 3982-3987). IEEE.

[4] Muntasha, G., Karna, N., & Shin, S. Y. (2021, April). Performance Analysis on Artificial Bee Colony Algorithm for Path Planning and Collision Avoidance in Swarm Unmanned Aerial Vehicle. In *2021 International Conference on Artificial Intelligence and Mechatronics Systems (AIMS)* (pp. 1-6). IEEE.

[5] Priyadarsini, P. L. K. (2021, January). Area Partitioning by Intelligent UAVs for effective path planning using Evolutionary algorithms. In *2021 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-6). IEEE.

[6] Wei, Y., Wang, B., Liu, W., & Zhang, L. (2021, July). Hierarchical Task Assignment of Multiple UAVs with Improved Firefly Algorithm Based on Simulated Annealing Mechanism. In *2021 40th Chinese Control Conference (CCC)* (pp. 1943-1948). IEEE.

[7] Aliwi, M., Aslan, S., & Demirci, S. (2020, October). Solving UAV Localization Problem with Firefly Algorithm. In *2020 28th Signal Processing and Communications Applications Conference (SIU)* (pp. 1-4). IEEE.

[8] Wang, S., Bai, Y., & Zhou, C. (2019, July). Coverage Path Planning Design of Mapping UAVs Based on Particle Swarm optimization Algorithm. In *2019 Chinese Control Conference (CCC)* (pp. 8236-8241). IEEE.

[9] Aggarwal, K., & Goyal, A. (2021, March). Particle Swarm Optimization based UAV for Disaster management. In *2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)* (Vol. 5, pp. 1235-1238). IEEE.

[10] E. Yanmaz, R. Kuschnig, M. Quaritsch, C. Bettstetter, and B. Rinner, ''On path planning strategies for networked unmanned aerial vehicles,'' in Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS), Apr. 2011, pp. 212–216.

[11] Tarun Rana ., Achyut Shankar , Mohd Kamran Sultan , Rizwan Patan ., "An Intelligent approach for UAV and Drone Privacy Security Using Blockchain Methodology"Vol .4 no -13 978-1-5386-5933-5/19 -IEEE 2019.

[12] Jiyang Chen1, Zhiwei Feng2,1, Jen-Yang Wen1, Bo Liu*3, and Lui Sha.," A Container-based DoS Attack-Resilient Control Framework for Real-Time UAV Systems"Vol .1 no -18 978-3-9819263-2-3/DATE19/ DAA 2019.

[13] Hongzhi Guo and Jiajia Liu. Uav-enhanced intelligent offloading for internet of things at the edge. IEEE Transactions on Industrial Informatics, 2019.

[14] Safae Lhazmir, Abdellatif Kobbane, Khalid Chougdali, and Jalel BenOthman. Energy-efficient associations for iot networks with uav: A regret matching based approach. In Proceedings of the 9th International Conference on Information Communication and Management, pages 132–136. ACM, 2019.

[15] Safae Lhazmir, Mohammed-Amine Koulali, Abdellatif Kobbane, and Halima Elbiaze. Performance analysis of uav-assisted ferrying for the internet of things. In 2019 IEEE Symposium on Computers and Communications (ISCC), pages 1–6. IEEE, 2019.

[16] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, "Towards secure industrial iot: Blockchain system with credit-based consensus mechanism,"IEEE Transactionson IndustrialInformatics,vol.15,no.6, pp. 3680–3689, 2019.

[17] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted iot data in smart cities," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 7702–7712, 2019.

[18] L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-based secure and trustworthy internet of things in sdn-enabled 5g-vanets," IEEE Access, vol. 7, pp. 56656–56666, 2019.

[19] F. Li, H. Yao, J. Du, C. Jiang, and Y. Qian, "Stackelberg game-based computation offloading in social and cognitive industrial internet of things," IEEE Transactions on Industrial Informatics, vol. 16, no. 8, pp. 5444–5455, 2020.

[20] C. Qiu, H. Yao, F. R. Yu, F. Xu, and C. Zhao, "Deep q-learning aided networking, caching, and computing resources allocation in softwaredefined satellite-terrestrial networks," IEEE Transactions on Vehicular Technology, vol. 68, no. 6, pp. 5871–5883, 2019.