International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6960
***Article Received**: 31 March 2023 **Revised**: 20 May 2023 **Accepted**: 02 June 2023*

Decentralized Machine Learning based Energy Efficient Routing and Intrusion Detection in Unmanned Aerial Network (UAV)

C.Srinivas[1,*] ,S.Venkatramulu[2],V.Chandra Shekar Rao[3], ,B.Raghuram[4], K.VinayKumar[5] and Sreenivas Pratapagiri[6]
[1,2,3,4,5&6]Department of Computer Science and Engineering, Kakatiya Institute of Technology and Science, Warangal.
[*]Corresponding Author: cs.cse@kitsw.ac.in

Abstract

Decentralized machine learning (FL) is a system that uses federated learning (FL). Without disclosing locally stored sensitive information, FL enables multiple clients to work together to solve conventional distributed ML problems coordinated by a central server. In order to classify FLs, this research relies heavily on machine learning and deep learning techniques. The next generation of wireless networks is anticipated to incorporate unmanned aerial vehicles (UAVs) like drones into both civilian and military applications. The use of artificial intelligence (AI), and more specifically machine learning (ML) methods, to enhance the intelligence of UAV networks is desirable and necessary for the aforementioned uses. Unfortunately, most existing FL paradigms are still centralized, with a singular entity accountable for network-wide ML model aggregation and fusion. This is inappropriate for UAV networks, which frequently feature unreliable nodes and connections, and provides a possible single point of failure. There are many challenges by using high mobility of UAVs, of loss of packet frequent and difficulties in the UAV between the weak links, which affect the reliability while delivering data. An earlier UAV failure is happened by the unbalanced conception of energy and lifetime of the network is decreased; this will accelerate consequently in the overall network. In this paper, we focused mainly on the technique of security while maintaining UAV network in surveillance context, all information collected from different kinds of sources. The trust policies are based on peer-to-peer information which is confirmed by UAV network. A pre-shared UAV list or used by asymmetric encryption security in the proposal system. The wrong information can be identified when the UAV the network is hijacked physically by using this proposed technique. To provide secure routing path by using Secure Location with Intrusion Detection System (SLIDS) and conservation of energy-based prediction of link breakage done by location-based energy efficient routing (LEER) for discovering path of degree connectivity. Thus, the proposed novel architecture is named as Decentralized Federate Learning- Secure Location with Intrusion Detection System (DFL-SLIDS), which achieves 98% of routing overhead, 93% of end-to-end delay, 92% of energy efficiency, 86.4% of PDR and 97% of throughput.

Keywords- federated learning, machine learning, intrusion, energy efficiency, Unmanned aerial vehicles (UAVs).

I. Introduction

Major changes are occurring in the next iteration of wireless networks. By 2025, Cisco predicts, there will be more than 75 billion Internet of Things (IoT) devices [1], including sensors, wearables, smartphones, linked automobiles, and UAVs. This shift is fueling an explosion in the quantity of wireless data being transmitted between the many different kinds of linked devices. UAVs, also known as drones, are expanding rapidly in this setting due to their many useful uses in wireless networks [2] [3]. They range from military and telecommunications to hospital supply delivery and surveillance and monitoring. Due to their unique qualities, UAVs in particular can serve as providers of wireless network infrastructure, improving the capacity, coverage, and energy economy of these networks. Remote sensing, augmented reality, and package transportation are just some of the uses for UAVs, which can also function as aerial users of the current wireless infrastructure. In reality, the requirements and needs of these new applications are shifting [4].

UAVs-based wireless networks must provide low-latency and ultra-reliable services to keep up with the ever-changing needs of their end users [5], in addition to the high data rates that have been the primary prerequisite of traditional wireless networks over the past decade. For instance, in order to allow for real-time, low-latency management of autonomous drones, it is necessary to set up highly reliable communication links [6]. The amount of time that UAVs can stay in the air depends on many factors, including the UAVs' energy reserves, speed, altitude, trajectory, etc., and is therefore crucial to the successful implementation of such uses. However, Machine Learning

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6960
***Article Received**: 31 March 2023 **Revised**: 20 May 2023 **Accepted**: 02 June 2023*

(ML) methods are becoming increasingly popular in a wide variety of academic disciplines, including wireless networks [7]. The inefficiency of traditional model-based solutions, which cannot handle the dynamic complexity and heterogeneity of the next generation of wireless networks [8], is a major factor pushing the adoption of ML-based methods in wireless networks. This opens the door for the incorporation of additional intelligence into the network's operations in order to optimize them and to guarantee, in real time, the various requirements of emerging wireless apps. In other words, wireless devices will be able to intelligently control their environment and take proactive, more appropriate actions by learning and predicting the dynamic evolution of various network features like traffic pattern, communication channel dynamics, user context, content requests, etc. In addition, Deep Learning (DL) is maturing into the most cutting-edge ML component, outpacing classic ML techniques [9].

Deep learning (DL) is the most prominent form of machine learning. [10] Many fields and industries, including wireless networking, robotics, image, text, and speech recognition, language processing, etc., foresee DL as the dominant method. However, conventional ML methods are cloud-centric, meaning they necessitate data transmission to and processing by a centralized location like the cloud or a data center. UAV-based wireless networks are not a good fit for these ML algorithms because of the following. Due to the potentially delicate nature of the information contained in the generated data (such as the whereabouts and identities of UAVs), it must be protected. Second, in a world where bandwidth is limited and battery life is short, it is difficult for unmanned aerial vehicles (UAVs) to continuously upload raw data to the cloud. This is especially true for data kinds like images and videos. Finally, cloud-centric schemes entail unacceptable latency, which is a problem for applications that require real-time decisions, like those built on unmanned aerial vehicles (UAVs) and autonomous drones (ADS). To effectively manage the dispersed sub-datasets produced by UAVs, a shift toward decentralized learning methods is essential.

Recently, Google has introduced the idea of decentralized Federated Deep Learning (FDL) [11]. For FDL, mobile nodes pool their data and train DL models locally before transmitting the trained models (weights) to a centralized server. As a result, FDL allows for dispersed training of DL models and the retention of sensitive data in its original location. Furthermore, FDL greatly reduces network latency by not directing data to a centralized location. Because of this, FDL requires less information to function than centralized ML. Since FDL allows wireless devices to learn a shared prediction model in parallel while keeping all the training data on device, it is better suitable for ultra low latency applications. This indicates that, unlike centralized cloud-centric approaches, FDL could be an enabling tool for future wireless networks based on UAVs to train learning models. Given the power and computing constraints of UAVs, as well as the latter's restricted bandwidth, the FDL idea is better suited for UAVs-based wireless networks than centralized schemes of deep learning. FDL not only protects the private of the data collected by UAVs, but it also decreases network overhead and latency by eliminating the need to relay first-hand information to a centralized location. In this article, we explain how FDL can be used by wireless networks that also support UAVs to overcome these obstacles. In addition, we discuss which deep learning method is best suited to tackle each problem and why [14]. Safe and accurate communications will rely on legal encryption and lightweight information sharing in reconnaissance. For supporting observation, UAVs have been especially useful. UAVs usually collaborate in this particular situation to achieve a viable identification and related exercises, as established by the proposed game-based approach of composed movement for ideal inclusion, sensor awareness, and agreeable combination of data. For various observational purposes, UAVs have been used, such as proficient monitoring of a moving group and nonstop underlying inspection.

To overcome the distinctive previously mentioned issues and to be more motivated by the examined recommendations, a solid directing methodology must be characterized while thinking about the various difficulties of UAV. The vital thought behind this steering technique is to abuse UAVs in the organization to productively foresee way disappointments before their event and select option next jumps. In addition, the technique should be able to set up directions containing UAVs with higher residual energy levels while avoiding low-energy UAVs and also using a protection strategy relying on the secure location-based intrusion detection system (SLIDS) and the energy-efficient routing (LEER) mechanism based on location.

The remainder of the paper is organized as follows. In Section 2, we discuss a number of citations that have been made to our research. In the third part, we delve into the specifics of our work's technical descriptions. In Section 4, we explain the feasibility of our work based on simulation results. Section 5 concludes with some observations and conclusions based on this study.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6960
***Article Received**: 31 March 2023 **Revised**: 20 May 2023 **Accepted**: 02 June 2023*

II. Related works

In recent years, a promising distributed ML paradigm called federated learning (FL) has emerged to address the shortcomings of traditional cloud-centric ML. FL was first suggested by Google. Fundamentally, FL allows multiple devices to train a single ML model in parallel without transmitting the raw data to any other nodes, preserving device privacy, reducing experienced latency, and easing the bandwidth and energy burden. It was shown that FL, as opposed to ML, which is hosted in the cloud, is better suited to use in wireless peripheral networks.

In machine learning (ML), computer-generated programs automatically gain expertise through exposure to and analysis of accumulated data. Most ML can be categorized into one of four subcategories: supervised, uncontrolled, semi-supervised, or Reinforcement Learning (RL). Since the study's setting requires primarily sequential and consecutive decision-making, Wasswa Shafik et al., (2022) zeroed in on RL and Deep learning [15]. The environment's interactivity allows for a contrast to supervised and non-supervised learning. Utilizing the stimuli of automated systems and the upcoming accumulative compensation, intricate policy choices can be made. The research goes even further by analyzing and presenting ML viewpoints depicting state-of-the-art developments with progress, comparatively depicting the future trend of RL based on its applicability in technology. It's a problem for a hypothetical IoT and an example of a potential answer. In this research, we saw a synthesis of a number of different points of view on the various RL analytic domains. The research looked at how many methods were focused on switching policy values rather than altering other mechanisms to achieve a specific mental state. The study laid a solid groundwork for future studies to follow, allowing researchers from a variety of disciplines to build more accurate models and architectures.

The next generation of wireless networks may benefit from using unmanned aerial vehicles (UAVs) as airborne base stations to handle the astronomical growth in user demand. UAV features like portability, adaptability, better line-of-sight probabilities, and entry to previously inaccessible areas make this a reality. Extensive research is being conducted on many aspects of such networks, including their deployment, performance analysis, resource management, path optimization, and channel modeling. With a comprehensive review of all relevant study areas, Rolly RM (2022) concentrates on the various applications and related algorithms for realizing aerial base stations [16]. In summary, this article discusses the technology, important applications, and challenges involved in designing and analyzing UAVs for use as base stations.

In [17], an effective method, dubbed UAV for sustainable FL, is developed using the decomposition technique and a successive convex approximation strategy. (UAV-SFL). Finally, simulations show how our proposed UAV-SFL approach can reduce the UAV's transmit power by 32.95 percent, 63.18 percent, and 78.81 percent when compared to the benchmarks, making it a viable long-term option for FL-based wireless networks.

To support asynchronous distributed computing in networks that make use of multiple unmanned aerial vehicles (UAVs), it is necessary to develop an Asynchronous Federated Learning (AFL) framework [18]. For this reason, the AFL framework also includes a method for selecting appropriate instruments to use during training.

A swarm of UAVs equipped with sensors for measuring air quality is used to execute a distributed federated learning (FL) algorithm, as described in [19]. Using swarm intelligence, a method is suggested for identifying the location with the highest AQI value. A CNN-LSTM model is then used to forecast the AQI based on the collected data. Each UAV in the swarm sends its locally learned model to the server, which then compiles all of the models it has received.

In [20], we suggest using a blockchain-based decentralized machine learning framework to improve UAV performance. The integrity and storage of data for smart decision making among numerous UAVs may be greatly improved by the suggested framework. We demonstrate the use of blockchain for distributed predictive analytics and provide a foundation for the distributed application and exchange of machine learning models.

In [21], the use of unmanned aerial vehicle (UAV) swarms is investigated, with each UAV carrying a machine learning classification task. A federated learning strategy is applied between a UAV leader and the swarm members to enhance the local learning model without resorting to extensive air-to-ground and ground-to-air communications.

From what we can tell, UAVs in FLs share a lot of data about their models' parameters with one another, which could be used against them by unscrupulous pilots. Blockchain, a distributed ledger for storing and verifying transactions, could be used to facilitate the safe trade of models in Florida (FL), even in the presence of adversarial unmanned aerial vehicles (UAVs). However, the blockchain-based approaches may have additional substantial overhead, such as additional block propagation, and should be thoroughly researched. Hence, to overcome the challenges the proposed Decentralized Federate

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6960
***Article Received**: 31 March 2023 **Revised**: 20 May 2023 **Accepted**: 02 June 2023*

Learning- Secure Location with Intrusion Detection System (DFL-SLIDS) helps to improve various parameters.

III. System model

In this proposed system, 3D is deployed fairly in UAV in team and it is considered by UAV battery which are energy trending of full level battery to the time of diminish as shown in figure 1. The crucial messages or exchange unique cast between each Other by the record mission achieved by the name of UAV as cooperatively. All UAV all is supposed to have itselfby geographical position (X,Y,Z) with the help of GPS and the routing table is updated periodically And its neighbours table also updated periodically. The bidirectional actions are considered for two UAV between the links for 5 GHS or band of wireless. IEEE 802.11a adopted as wireless interface in each UAV of Mac layer, the high dynamic topologies are considered for efficient support and wireless communications or provide coverage widely. To detect people using UAV proposed to adjust the surveillance of wide area particularly in the distributed management. A controlled area is crossing by a person normally assumed by this method which is based on architecture of overall system as given in below figure.

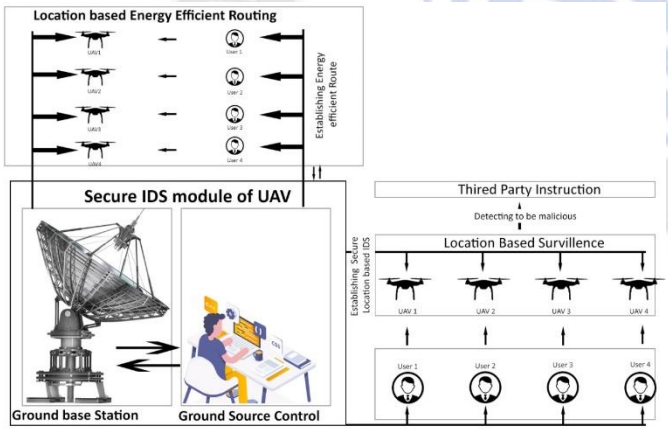

Figure-1 Overall system model

The proposed method of DFL-SLIDS of is mainly based on the system with intrusion detection. For all official UAV authenticated by ID for all network where UAV provides track record to follow. The proposed LEER method is used to optimise the system energy using its location. The peer to peer technique used in the proposed system for communication, the less fading is dominant for path loss which are expressed as follows:PLPP (x) = β10log10x + α,Whereβ is, a = √(ai − aj)2 + (bi − bj)2 + (ci − cj)2 which is the loss exponent and the communicating distance of UAVs ui and uj, The α reflects the failure of the direction at the reference point.Following the model of free-space propagation, β = 2 and α = 10log10 (4πw l) ; Where the carrier frequency is w and the light velocity is l = 3 X 108m/s

3.1 Federated Learning model

In this section, we will go over the basics of FL as they pertain to multi-UAV capable networks. The AI model under discussion here is the local FL model, which is trained with data unique to the device in question, while the global FL model is the one built by each UAV server with parameters from local models. The global model parameters for the nth UAV server will be denoted by w_n, the local model parameters for the kth device will be denoted by w_k, and the training datasets used by the kth device will be denoted by D_k. By introducing the loss function $f(w_n,s_{k,i},z_{k,i})$, we are able to quantify the FL performance error over the input data sample vector $s_{k,i}$ on the learning model w and the intended output scalar $z_{k,i}$ for each input sample i at the k^{th} device.

3.2 Energy model using Location based Energy Efficient Routing (LEER)

Wireless networking devices, such as integrated batteries, manages the energy resources of UAVs. The UAVs have a very low capacity, requirements with continuous wireless connectivity, portability, compact dimensions of energy. UAV ui (Rui) energy is below Ia $(Rui < Ia)$, in addition to specific circumstances where Ia can be altered by Ia according to the need to deliver the data packets. This includes adaptations for all kinds of uses. Two fields, containing the leftover energy and creation data of each UAV, are applied to the Hello packet format to know about the residual energy level of all neighbouring UAVs and to foresee any distinction between them, individually. The model of energy productivity for the proposed system is given below. Smart administration of residual UAVs is lifespan of the enterprise and the efficient provision of information. In view of the accompanying status, each UAV from time to time calculates its remaining energy power $(Rerc)$

$$R = Rerc\% = Battery\ residual\ energy\ Batteryfullenergy \times 100$$

Data packets of except for high-priority (i.e. priority = 0) or for cases when the UAV has a previously settled location. Another thing, the UAV needs to update the RP field with its R value only when it gets an RREQ packet $(RP > R)$.Three energy consumption dispersions are approved for each UAV for our work. To begin with, the use of energy is overshadowed by UAVs practise in the propulsion energy. First, we predict mobility of UAVs of 70%. Second, the consumption of wireless contact with 25 % on the grounds

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6960
Article Received: 31 March 2023 Revised: 20 May 2023 Accepted: 02 June 2023

that are recognised more often than not, especially during packet sending and acceptance. Finally, 5% of evaluated the usage during sitting is UAVs continue to do both Hello packet trading and listening activities (not having data) while drifting the region. We ignore the computation and capability of UAV energy for convenience.

Algorithm of Data packet processing

Input: Data Data: ui , Current UAV

Data: rtablei , Routing table of ui

Data: ui+1 , Next UAV

1 Temp ← rtablei .search(Data.Communication ID)

2 if Data.Destination = ui then // ui is uD.

3 Reception(Success)

4 else // CEuiui+1 is still valid.

5 if Temp and (rtablei .CEuiui+1 > 0 and rtablei .Rui+1 ≥ τ) then

6 Forward(Data,Next hop)

7 else // CEuiui+1 is not valid.

8 Greedy forwarding(Data,Destination)

The first order energy model predicts the following power usage for a sensing node transmitting K-bit bytes:

$$E_{Tx}(k,d) = E_{Tx-elec}(k) + E_{Tx-amp}(k,d)$$

$$E_{Tx}(k,d) = E_{elec} * k + \varepsilon_{amp} * k *$$

The following is the energy usage details for a sensing node receiving K-bit bytes:

$$E_{Rx}(k) = E_{Rx-elec}(k$$

$$E_{Rx}(k) = E_{elec} * k$$

$$\varepsilon_{amp} - Magnification\ of\ Signal\ Amplifier$$

E_{elec}
$-$ *The energy consumption of sending circuit and receiver circuit*

$$d - Distance\ of\ Signal\ Transmission$$

Each round, the network decides which nodes will become cluster heads based on the current number of cluster heads and the percentage of cluster heads that it has taken in earlier rounds. The node picks a random integer between 0 and 1 based on a threshold value T(n). In this iteration, the nodes become cluster leaders if the arbitrary number is less than T(n). What the T(n) was:

$$T(n) = \begin{cases} \dfrac{p}{1 - p.\left(\dfrac{rmod1}{p}\right)} & n \in G \\ 0 \end{cases}$$

p - Proportion of all nodes that become cluster leaders.

r - Round number currently in effect.

G - The group of servers that have never served as the cluster's leader.

The node will inform the cluster's leader that it has entered. The cluster leader receives transmissions from all of the nodes. The receiver at the cluster's head node has been kept in a constant receiving condition up to this point. The cluster head node will establish a schedule to inform all nodes in the cluster when to transmit data once it has received all data from cluster members.

Optimal cluster head count determination:

To simplify, we will refer to S as the assumed plane area and X(S) as the assumed number of sensor nodes within S. Then, X(S) is a free-standing model of energy,

$$p\{X(S) = n) = \frac{[\lambda A(S)^n e^{-\lambda A(S)}]}{n!} \quad n = 0,1,2 \ldots\ldots$$

The area of the province is denoted by A (S). A (S) should be 2M if and only if S is a square with sides of length M. If there are N sensor sites spread across S square kilometers. Each sensing node has a P% chance of becoming the cluster leader. Then, there are nodes here that serve as the heads of NP clusters. If the sensing node's distance from the base station, denoted by DB x y, is uncertain. PS is the uniformly distributed cluster head node probability density in set S. Theoretical maximum distance a cluster head node could be from the base station, assuming the base station is located in the center of the coverage region S, is

$$E(D_B(x,y)|X(S) = N) = \iint_S^n D_B(x,y).P_S dxdy = 0.3825M$$

In this area, you'll find NP clusters, each with their own unique set of heads. Cluster C has an unknown amount of sensors, so the average distance to the base station will be 0.3825NPM X(C) the distance from the cluster's leader node to the station. DC measures how far apart the cluster's main node is from all of the other nodes in the cluster.

$$E(D_C|X(S) = N) = \iint_C \sqrt{x^2 + y^2} k(x,y) dA(C) = \frac{2M}{3\sqrt{NP\pi}}$$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6960
***Article Received**: 31 March 2023 **Revised**: 20 May 2023 **Accepted**: 02 June 2023*

C -A circular area whose radius is$\frac{M}{NP\pi}$

K (x,y)- The number of sensor arrays follows a normal distribution.. EC - How much power does it take for a cluster of nodes to send a single piece of data to the cluster's master node . The mathematical expectation of EC is: $E(E_C|X(S)=N)=N^{1/2}.\frac{2M}{2r\sqrt{\pi}}.\frac{1-p}{\sqrt{p}}$

where, r -The wireless communication radius, EB- tthe power used by the cluster nodes to transmit fused data to the control center, the mathematical expectation of EB is:

$$E(E_B|X(S)=N)=\frac{0.3825NPM}{r}$$

Er- Total network energy usage . Then $E_T=E_B+E_C$ we can get the mathematical expectation of all energy: $E[E_T]=E[E(E_T|X(S)=N)]$

3.3 Distributed Federate Learning- Secure Location with Intrusion Detection System (DFL-SLIDS)

Before the UAV army starts the observation movement, all the UAVs should be officially enrolled. The UAVs asymmetric encryptions are therefore able to sign their messages with public key. The messages are transmitted via the UAV association, and a list of a particular individual's testing UAVs will be known to each UAV. A UAV authority could truly be caught and sold off. This UAV could submit false warnings properly endorsed for this circumstance to upset the UAV organization's proper functioning. Nevertheless, because of the necessary asymmetric encryption for verifying senders, the undermined UAV will not alter its character to mimic various specialists. From the messages of all UAVs, and tests if a few of the testing UAVs are obtained by each gatecrasher at any rate. Nevertheless, UAVs will have a dispersed confidence managers. This witnessing will consider the length of time of only one trust the occasion of an interloper, punishing the trust in it. It also takes into account the times when captured data is submitted. It would weigh the recent incidents as more relevant, but it would still consider the full past as well.

In three modules, the model of this DFL-SLIDS was coordinated: the "Setup" techniques (first performed the recreation); the techniques (occasionally summoned in simulation); and the "Measure" techniques (utilized for refreshing the diagrams). With regards to techniques. On the left hand, the key strategy emerges. Both UAVs and individuals travel initially. A variable non-deterministic strategy is used by the former, whereas individuals primarily seek to cross a controlled field in a certain direction with only minor variations. At that point, UAVs decide if any entity is nearby. V2V interchanges are simulated after this. The block diagram also decides the V2V correspondences that care from the points of view of senders and receivers separately. UAVs exchange separate signals as to whether they have observed the gatecrasher specifically. Provided the energy constraints, they only associate with nearby UAVs. In order to update their nearby viewers confidence, they unscramble the content. UAVs have a secret key such that, with asymmetric encryption, they can prove their identity. Architecture for location based secure IDS is given in figure 2.

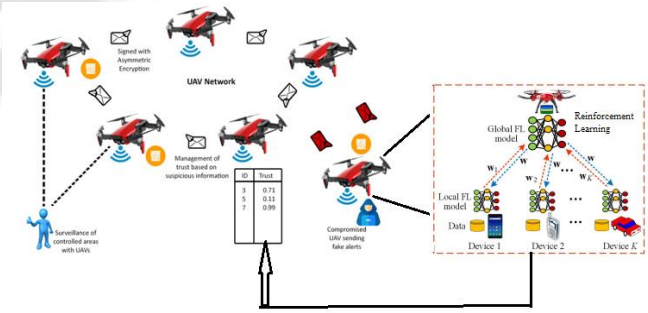

Figure 2- Architecture for DFL-SLIDS

In the off case that there is a situation where the gatecrasher region was not protected by UAV, a possibility was relegated to the option of shifting the path, and then this choice was simulated by comparing an odd number and this probability resulted in the threshold. Furthermore, with unique cutoff points, the rotation angle was calculated non-deterministically, as Equation 2 shows:

$$\alpha = (rf(\beta) - (\beta/2),$$
$$if\ r \leq pr\ 0, otherwise$$
$$ap = a/n$$
$$t = at/a$$
$$dp = d/n$$
$$ids = P\ x \in A\ |lx|\ a$$

Where an is the number of UAVs that received an alert from another UAV, n is the total number of UAVs, t is the number of UAVs that trusted the information they received about an intruder, d is the number of UAVs that directly noticed and announced an intruder, A is the arrangement of all UAVs that received an alert, and lx is the list of direct UAV observer IDs stored locally in the UAV x. The seized UAVs fly around like other unmanned aerial vehicles. The single difference is that false warnings from intruders are persistently recorded. They aim to report false warnings to the fleet of UAVs, so that the framework lacks relevance and it can continue to be overlooked by customers. Along

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6960
***Article Received**: 31 March 2023 **Revised**: 20 May 2023 **Accepted**: 02 June 2023*

these lines, when UAV warnings are ignored, a real attacker may experience the controlled area.

Assume that the imbalanced training data set is $D = \{(x1, l1), (x2, l2), \ldots, (xn, ln)\}$ where xi is the ith sample and li is the label of the ith sample. We suggest training a classifier in RL-MDP where the classifier itself is an evolving agent.

- State S: The sample used for training controls the environment's current condition. The first sample, x1, is given to the agent as its starting state s1 at the start of training. Sample xt represents the environment's condition st at that instant in time. The training data set's sample order is randomly reshuffled by the environment at the start of each new show.
- Action A: Each training data collection has a label that corresponds to the agent's behaviour. The agent's current move is a label prediction. Where 0 stands for the underrepresented class and 1 stands for the overrepresented class, A = 0 and 1 for a binary classification issue.
- Reward R: A reward rt is the environmental data that indicates whether or not an agent's activities were successful. Samples from the minority class are rewarded at a greater absolute value than those from the majority class so as to steer the agent toward learning the optimal classification policy in skewed data. That is, the agent receives a harsher reward or punishment from the environment depending on whether or not it accurately identifies a minority class sample.
- Transition probability P: The chance of a transition p(st+1|st, at) is fixed. Following the sequence of samples in the training data collection, the agent transitions from state st to state st+1.

In an unbalanced data collection, identifying minority group samples accurately is a significant challenge. In order for the algorithm to accurately recognize minority group samples, it needs to be more sensitive to that group. When an agent obtains a sub-par sample, it receives a disproportionately big reward or punishment. The agent's forecast cost equals the reward function's value. Prediction cost values for the minority class are larger than those for the majority class when the data collection is imbalanced ($\lambda < 1$). The forecast cost values are the same for all classes if and only if the class distribution in the training data set is uniform ($\lambda = 1$). In reality, λ is a trade-off measure used to modify the weight given to the dominant social group.

DFL-SLIDS's classification strategy π is a function that, when given a sample, can calculate the probabilities of all possible labels.

$$\pi(a|s) = P(at = a|st = s)$$

The goal of the classifier agent is to correctly label as many instances as possible from the training data collection. By optimizing for accumulated rewards, the classifier agent achieves its goal. it receives for accurately identifying samples.

$$gt = \sum_{k=0}^{\infty} \Omega k \, (t = k)$$

The Q function is a reinforcement learning concept that measures the strength of a state-action pair.

$$Q\,\pi\,(s, a) = E\pi[gt|st = s, at = a]$$

The Bellman equation provides an expression for the Q function, which looks like this:

$$Q\,\pi\,(s, a) = E\pi[rt + \gamma Q\pi\,(st + 1, at + 1)|st = s, at = a]$$

In order for the classifier agent to maximize the sum of its rewards, it must solve the optimal Q function, and the greedy strategy under this function yields the best possible classification. The Q network's structure is determined by the nature and size of the data used for training. The structure of the training sample is reflected in the input of the Q network, and the number of outputs is proportional to the number of groups in the training set. The Q network is a classification built on a neural network, but it lacks the conventional softmax output layer.

IV. Performance analysis

The experimental result is carried out using and the parameters such as Routing Overhead (RO),the end-to-end delay (EED), the packet delivery ratio (PDR), energy efficiency, and throughput for different rates and densities are calculated by a few evaluation measurement . These parameters are compared with three state of art methods such as UAV for Sustainable FL (UAV-SFL), Asynchronous Federated Learning (AFL), with the proposed Decentralized Federate Learning- Secure Location with Intrusion Detection System (DFL-SLIDS). We settled on a network size of 500 UAVs because, according to the literature on UAV communication systems, this is the norm for such networks. We decided on a break term of 1000 s for all V2V exchanges and for transmitting direct impressions, as this is the usual time period used in writing about helpful UAVs. The modeling setup is depicted in Figure 3.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6960
***Article Received**: 31 March 2023 **Revised**: 20 May 2023 **Accepted**: 02 June 2023*

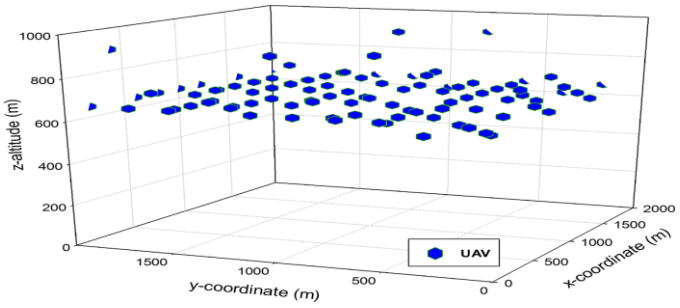

Figure 3 Simulation scenario

- As shown in Equation 20, the amount of routing packets transmitted for route maintenance and route finding can be thought of as the routing overhead (RO).

$$RO = \frac{H}{P}$$

Where, H is counted once per hop and P is total number of routing packets

Table-1 Comparison for routing overhead

Number of UAV's	UAV-SFL	AFL	DFL-SLIDS
100	45	78	81
200	59	80	83
300	61	84	85
400	72	86	89
500	85	89	94

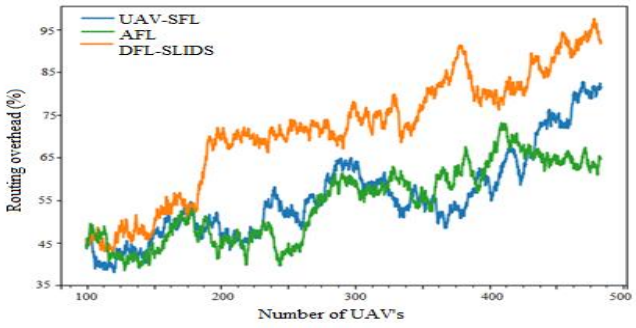

Figure-4 analysis of routing overhead

In Figure 4, the X-axis depicts the total number of UAVs used in the study, while the Y-axis displays the percentage of routing overhead for each of the current UAV-SFL, AFL, and proposed DFL-SLIDS methods. The suggested DFL-SLIDS method outperforms the state-of-the-art UAV-SFL and AFL methods by 3% and 2%, respectively, in terms of routing overhead, while the existing QSIA and RNN-OCSA methods only manage 90% and 91%, respectively.

- The "end-to-end delay" of a packet is the total amount of time it takes to move from its point of origin across a network to its destination.

Table-2 Comparison for End-to end delay

Number of UAV's	UAV-SFL	AFL	DFL-SLIDS
100	65	68	71
200	69	70	73
300	71	74	75
400	72	76	79
500	75	79	84

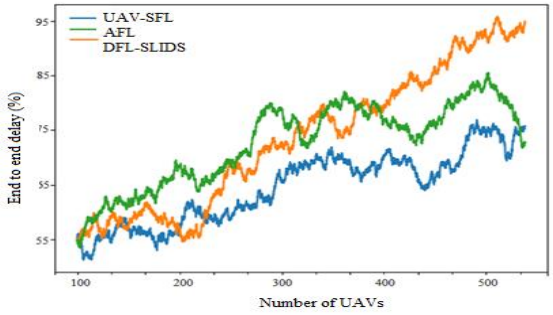

Figure-5 analysis of end to end delay

In Figure 5, the X axis represents the total number of UAVs used in the study, while the Y axis displays the percentage of end-to-end delay for each of the three methods (UAV-SFL, AFL, and the proposed DFL-SLIDS). The proposed DFL-SLIDS method gets 93% of routing overhead, which is 3% better than UAV-SFL and 2% better than AFL compared to the existing QSIA and RNN-OCSA methods.

- Energy efficiency is determined by dividing the amount of energy used to produce a usable amount of energy (the energy output) by the amount of energy used to start the process (the energy input).

$$E = \frac{Wout}{Win} \times 100$$

Table 3. Comparison for energy efficiency

Number of UAV's	UAV-SFL	AFL	DFL-SLIDS
100	86	88	89
200	88	89	90
300	89	90	91
400	90	91	92
500	91	92.5	93

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6960
***Article Received**: 31 March 2023 **Revised**: 20 May 2023 **Accepted**: 02 June 2023*

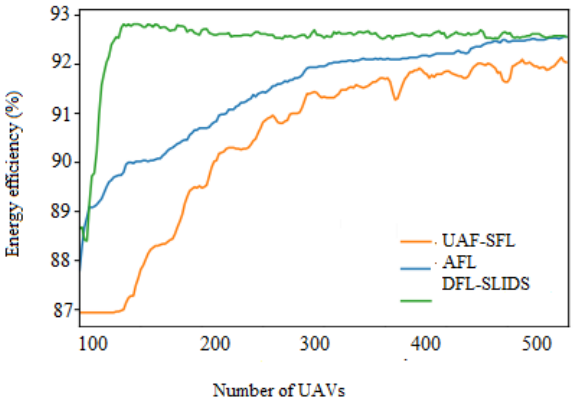

Figure 6. Comparison of energy efficiency

Figure 6 shows the percentage of UAVs with high energy efficiency values plotted against the total number of UAVs used in the study (X-axis). This allows for a direct comparison of the sensitivity of UAV-SFL, AFL, and the proposed DFL-SLIDS method. Energy efficiency is improved by 3% when using the proposed DFL-SLIDS method compared to the current UAV-SFL method and by 2% when using the existing AFL method.

- **Packet Delivery Ratio (PDR)-** It is the average ratio of the total packets received (R)successfully to the total packets originally sent (S)as shown:

PDR= $\sum_0^N \frac{R}{S}$

Table 4. Comparison for PDR

Number of UAV's	UAV-SFL	AFL	DFL-SLIDS
100	84	85	87
200	85	87	89
300	85	88	90
400	86	89	91
500	87	90	92

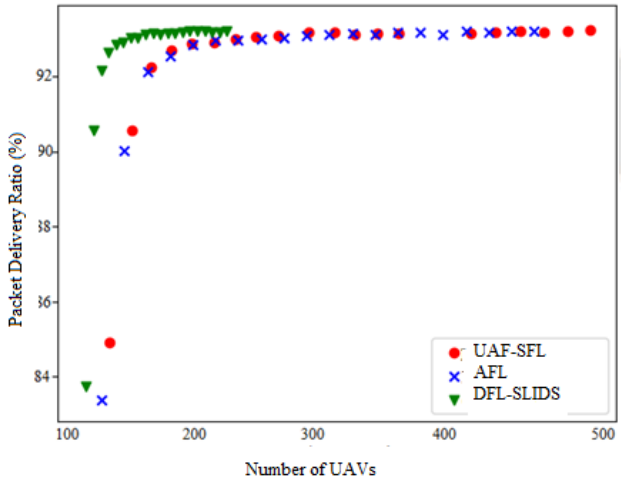

Figure 7. Comparison of packet delivery ratio

In Figure 7, the X axis represents the total number of UAVs used in the analysis, while the Y axis displays the percentage values found for the packet delivery ratio when comparing the existing UAV-SFL, AFL, and proposed DFL-SLIDS methods. Existing UAV-SFL and AFL methods accomplish 87% and 90% of packet delivery ratio, respectively, while the proposed method achieves 92% of packet delivery ratio, improving on both by 5%.

- Throughput is the amount of data that can be sent or received per second over a given transmission channel. The significance of throughput in MANET apps is demonstrated by the following.

Throughput (bits/sec) = $\sum \frac{(n)*(avg)}{T}$

Tab 5. Comparison for throughput

Number of UAV's	UAV-SFL	AFL	DFL-SLIDS
100	78	79	80
200	80	81	82
300	82	83	84
400	84	85	86
500	86	87	88

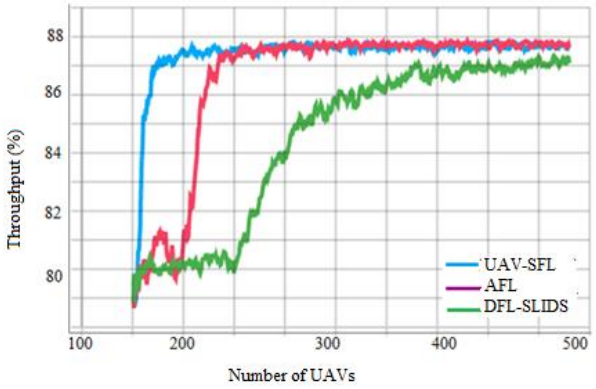

Figure 8. Comparison of throughput

Figure 8 depicts a throughput comparison of existing UAV-SFL, AFL, and the proposed DFL-SLIDS method, where the X axis depicts the number of UAVs used for analysis and the Y axis depicts the percentage of throughput achieved. Existing UAV-SFL and AFL methods achieve 86% and 87% throughput, respectively, while the proposed DFL-SLIDS method gets 88%, improving on both by 2%.

parameters	UAV-SFL	AFL	DFL-SLIDS
Routing overhead	94	95	98
End to end delay	90	91	93
energy efficiency	87	90	92
PDR	84	85	86.4
throughput	86	87	97

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6960
***Article Received**: 31 March 2023 **Revised**: 20 May 2023 **Accepted**: 02 June 2023*

V. Conclusion

To manage UAV communications between the network by location based routing which are promising solution. There are a lot of difficulties happened in such network like, UAVs high mobility, energy restriction on the disconnections occur frequently. The traditional mechanism is the process of route Discovery which are used to identify the position of destination and lead with routing for appropriately. This process is not to explore fully in several times to connected with durable paths and named as frequent disconnection and the data transmission is seriously affecting by the important overhead this issues by DFL-SLIDS, by which is useful to predict the failure lings really in the discovery phase to their occurrence and energy consumption is achieved among all UAVs. There is alternative solutions provided when the path failure occurred in maintenance process and received your energy with the links ok of lifetime process of UAVs. The given simulations are based on DFL-SLIDS clearly. In this paper, the supporting surveillance given for the UAV network in UAVs was proposed in the protection framework for detection based on the trust model. It is based on the premise that more than one UAV would typically observe individuals at the boundary. Therefore, if a UAV identifies persons who are also reported by other UAVs repeatedly, this fact would be identified by each UAV.

Reference

[1] B. Brik, A. Ksentini, and M. Bouaziz, "Federated learning for UAVsenabled wireless networks: Use cases, challenges, and open problems," IEEE ACCESS, vol. 8, pp. 53841-53849, 2020.

[2] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Arcas, "Communication-efficient learning of deep networks from decentralized data," in Proc. AISTATS, pp. 1273-1282, 2017.

[3] S. Samarakoon, M. Bennis, W. Saad, and M. Debbah, "Federated learning for ultra-reliable low-latency V2V communications," in Proc. IEEE GLOBECOM, pp. 1-7, 2018.

[4] M. Chen, H. V. Poor, W. Saad, and S. Cui, "Wireless communications for collaborative federated learning," IEEE Communications Magazine, vol. 58, no. 12, pp. 48-54, 2020.

[5] P. Pinyoanuntapong, P. Janakaraj, P. Wang, M. Lee, and C. Chen, "FedAir: Towards multi-hop federated learning over-the-air," in Proc. IEEE SPAWC, pp. 1-5, 2020.

[6] S. Hosseinalipour, C. G. Brinton, V. Aggarwal, H. Dai, and M. Chiang, "From federated to fog learning: Distributed machine learning over heterogeneous wireless networks," IEEE Communications Magazine, vol. 58, no. 12, pp. 41-47, 2020.

[7] T. Zeng, O. Semiari, M. Mozaffari, M. Chen, W. Saad, and M. Bennis, "Federated learning in the sky: Joint power allocation and scheduling with UAV swarms," in Proc. IEEE ICC, pp. 1-6, 2020.

[8] S. S. Ram, A. Nedic, and V. V. Veeravalli, "Asynchronous gossip algorithms for stochastic optimization," in Proc. IEEE CDC, pp. 3581- 3586, 2009.

[9] A. Nedic and A. E. Ozdaglar, "Distributed subgradient methods for multi-agent optimization," IEEE Transactions on Automatic Control, vol. 54, no. 1, pp. 48-61, 2009.

[10] X. Lian, C. Zhang, H. Zhang, C.-J. Hsieh, W. Zhang, and J. Liu, "Can decentralized algorithms outperform centralized algorithms? A case study for decentralized parallel stochastic gradient descent," in Proc. NIPS, pp. 5330-5340, 2017.

[11] Z. Tang, S. Shi, and X. Chu, "Communication-efficient decentralized learning with sparsification and adaptive peer selection," in Proc. IEEE ICDCS, pp. 1207-1208, 2020.

[12] M. Chen, Z. Yang, W. Saad, C. Yin, H. V. Poor, and S. Cui, "A joint learning and communications framework for federated learning over wireless networks," IEEE Transactions on Wireless Communications, vol. 20, no. 1, pp. 269-283, 2021.

[13] N. H. Tran, W. Bao, A. Y. Zomaya, M. N. H. Nguren, and C. S. Hong, "Federated learning over wireless networks: Optimization model design and analysis," in Proc. IEEE INFOCOM, pp. 1387-1395, 2019.

[14] J. Ren, G. Yu, and G. Ding, "Accelerating DNN training in wireless federated edge learning systems," IEEE Journal on Selected Areas in Communications, vol. 39, no. 1, pp. 219-232, 2021

[15] Wasswa Shafik et al., "A reawakening of Machine Learning Application in Unmanned Aerial Vehicle: Future Research Motivation," EAI Endorsed Transactions on Internet of Things, Volume 8 Issue 29, 2022

[16] Rolly RM, Malarvezhi P, Lagkas TD. Unmanned aerial vehicles: Applications, techniques, and challenges as aerial base stations. International Journal of Distributed Sensor Networks. 2022;18(9). doi:10.1177/15501329221123933

[17] Pham, Q. V., Zeng, M., Ruby, R., Huynh-The, T., & Hwang, W. J. (2021). UAV communications for sustainable federated learning. IEEE Transactions on Vehicular Technology, 70(4), 3944-3948.

[18] Yang, H., Zhao, J., Xiong, Z., Lam, K. Y., Sun, S., & Xiao, L. (2021). Privacy-preserving federated learning for UAV-enabled networks: learning-based joint scheduling and resource management. IEEE Journal on Selected Areas in Communications, 39(10), 3144-3159.

[19] Chhikara, P., Tekchandani, R., Kumar, N., Guizani, M., & Hassan, M. M. (2021). Federated learning and autonomous UAVs for hazardous zone detection and

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6s
DOI: https://doi.org/10.17762/ijritcc.v11i6s.6960
Article Received: 31 March 2023 Revised: 20 May 2023 Accepted: 02 June 2023

AQI prediction in IoT environment. IEEE Internet of Things Journal, 8(20), 15456-15467.

[20] 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, 196, 108217.

[21] Mrad, I., Samara, L., Abdellatif, A. A., Al-Abbasi, A., Hamila, R., & Erbad, A. (2021). Federated Learning for UAV Swarms Under Class Imbalance and Power Consumption Constraints. arXiv preprint arXiv:2108.10748.