JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.682-692
https://publishoa.com
ISSN: 1309-3452

Flying Ad-Hoc Networks rely on Trust-Aware Route Selection for Efficient Packet Transmission.

[1]*S.Sugantha Priya, [2]Dr.M.Mohanraj

[1]*Assistant Professor, Department of Computer Science

Dr SNS Rajalakshmi College of Arts and Science, Coimbatore, Tamil Nadu, India

Mail id: sugantha2612@gmail.com

[2]Associate Professor, Department of Computer Applications

Dr SNS Rajalakshmi College of Arts and Science, Coimbatore, Tamil Nadu, India

Mail id: mohanrajsns@gmail.com

ABSTRACT

Cost-effective unmanned aerial vehicles (UAVs) have just developed due to the accelerated spread of wireless communication and networking technologies, and they will soon occupy the majority of our airspace. UAVs can be used to efficiently complete complex missions when organized as an ad hoc network, resulting in the well-known Flying Ad Hoc Networks (FANETs). Furthermore, due to many flight limitations and the highly dynamic topology of FANETs, designing routing protocols is a problematic issue. Previously, we discussed energy-efficient clustering and fuzzy-based route selection for FANET. However, because of the open wireless boundary and the excellent mobility of the drones, FANETs are vulnerable to rogue nodes that might breach the network and pose significant security threats. Trust among the nodes is critical. In this paper, a unique trust method is presented in which the Adaptive Artificial Fish Swarm Strategy (AAFSA) strategy is employed to optimize cluster head (CH) selection. The suggested trust method measures direct trust using improved Bayesian theory and indirect trust using evaluation credibility and activity. ITOPSIS (Improved Technique for Order Performance by Similarity to Ideal Solution) is a new technique for improving the route-finding process. According to the experimental outcomes, the presented method is more adaptable in energy, throughput, delay, overhead, and packet delivery ratio.

Keywords: FANETs, Security, UAVs, Adaptive Artificial Fish Swarm Strategy, Trust

1. Introduction

In addition to military uses, UAVs have been utilized in an expanding variety of civil applications such as policing, firefighting, and so on in recent years. Instead of employing a single large UAV, numerous UAVs are now deployed for excellent coverage and precision. As a result, networking topologies that allow two or more UAV nodes to interact directly or thru a relay node are necessary. This is a relatively new technology in the network family, where the needs differ significantly from standard networking methods, such as mobile ad-hoc networks and vehicular ad-hoc networks [1].

Single UAV systems are made up of a single, huge UAV that interacts directly with the infrastructure of a ground control station. Because of technological and research improvements in embedded systems and wireless communication technologies and the trend toward integration and miniaturization, numerous tiny UAV systems may now be used at a low cost. A UAV must be outfitted with complicated hardware systems to maintain contact with the controller on the ground [2]. However, the mission must be aborted [3]. One of the most challenging issues is the interchange of information between UAVs that have experienced severe losses.

A dependable connection, or what is known as a routing protocol between UAVs, is a critical component of data delivery in any application [4]. As a result, a well-designed networking paradigm that allows UAVs to interact with one another and self-organize into a network known as FANET [5] must be established. To accommodate the expanding number of FANET applications and keep them running reliably and consistently, incremental design of routing protocols is required to address the difficulties mentioned above while also taking into account the specific characteristics of FANETs [6]. As a result, a wide variety of routing protocols employing various strategies is presented for FANETs to supply concurrent performance, reduce packet losses, and cope with different circumstances and situations.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.682-692
https://publishoa.com
ISSN: 1309-3452

Moreover, because FANETs are comparable to MANETs, researchers have investigated the feasibility of implementing the routing mechanisms employed in FANETs [7]. Even tho some changes have been made, other criteria, such as mobility patterns, energy limits, deployment area, node localization, and QoS requirements, have been disregarded. As a result, understanding the boundaries of the various routing protocols and existing techniques allows us to design new routing paradigms based on our needs constantly and to identify which near-optimal procedures to employ among UAVs in a specific circumstance.

In FANETs, UAVs typically face energy and computation constraints. So, intermediate nodes can refuse to forward packets to save resources, causing network traffic disturbance. Selfish nodes are known as selfish nodes [8]. The nodes' self-organized, anonymous, distributive, and independent activities make them more vulnerable to assaults. Trust management is one of the security solutions for FANETs since nodes need to trust each other to cooperate and coordinate. It allows a node to determine the reliability of other network nodes [9]. By isolating hostile and selfish node activities, trust management improves overall network performance. The development of trust management solutions requires measurement attributes and computing procedures for evaluating trust. Trust evaluation in FANETs includes node behaviour assessment regarding dependability and performance and a correct suggestion [10]. Motivated by the preceding, this work built TARS for efficient packet transmission in fly-ad-hoc networks. This work's primary goal is to build confidence among communicating UAVs and pick the most reliable UAV capable of storing data and having enough energy to complete the task.

For the remainder of this article, Section 2 outlines relevant work in the domain of ad hoc trust management. Section 3 presents the FANET trust method, and Section 4 discusses the test findings. Section 5 concludes with future scope.

2. Related work

Trust is essential in forecasting such node behaviour. Researchers have presented numerous techniques to measure a node's trust value in mobile and vehicular ad hoc networks (direct and indirect). In a FANET, node velocity is the main distinguishing feature; as a result, connection losses and topological changes occur often. So, conventional trust calculation procedures are inefficient and ineffective. [11] presented the findings of a study to improve FANET security. A new security architecture based on secret sharing and authorized encryption is created. The FANET hardware simulation method is used to test its efficiency. [12] proposes a Trust-Based Clustering Paradigm (TBCS) for FANETs.

TBCS employs a multicriteria fuzzy technique based on node activity in a fuzzy and complicated environment for categorization. The Takagi–Sugeno–Kang fuzzy inference procedure is used in the suggested strategy. The reward and punishment system was implemented in the FANET to turn node activity into trust and to separate malicious and disobedient nodes. A fuzzy categorization trust method (FCTM) for FANETs is presented in [13]. The node categorization is based on the network node's behaviour and performance. Furthermore, quality of service (QoS) and social factors are utilized to assess each node's trust value to distinguish between selfish and malevolent nodes.

To imitate the real-world behaviour of the UAVs, a decay function is also being examined. Experiments are used to identify the best trust aggregation weights across QoS and social characteristics to categorize network nodes. For reliable and secure communication, [14] proposes a secure energy-efficient dynamic routing protocol (SEEDRP). The SEEDRP is divided into two phases: (1) SEEDRP-Routing and (2) SEEDRP-Security. The first phase employs a unique dynamic routing strategy to determine the most cost-effective route between the source and destination nodes. The presented work's second phase centralizes on a different dynamic key generation system that transfers data securely. [15] describes a solution for mitigating a wide range of routing assaults in self-organizing ad-hoc networks (MANET, VANET, FANET, MARINET, IoT, WSN, mesh networks, M2M networks, and so on).

The new technique extends the Watchdog approach and determines the packet transfer coefficient (P-Secure) by implementing an ant swarm strategy for establishing a secure route in the network. All nodes act as agents to assess the security of surrounding nodes. [16] proposes a novel trust method in which the evolutionary strategy is utilized to optimize the weights of several attributes to estimate the direct trust values. An explicit trust is combined with commendation to compute a node's final trust value. Furthermore, nodes are grouped into clusters, and the trust levels of doubtful nodes are risk-assessed. Nodes are included in the recommendation or rejected list based on risk assessment.

As a result, malicious nodes are removed from the network via the discard list. [17] examines the conditions for effective UAV communication. We also compare and contrast MANETs and UAV-based networks and protocols. Finally, we address the various trust-based protocols and management paradigms that can be utilized in UAV networks and the UAV applications that can benefit from such protocols. In [18], a unique trust method based on fuzzy logic is presented to deal with the behavioural unpredictability of FANET nodes. A multicriteria fuzzy categorization procedure categorizes nodes based on their behaviour and performance in a fuzzy and complicated environment.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.682-692
https://publishoa.com
ISSN: 1309-3452

QoS and social attributes (recommendations) are used to evaluate each node's trust value. FANET nodes are rewarded or penalized based on their behaviour with node categorization. In [19], we present a Kalman Trust Estimator (KATE) to detect drone misbehaviour. Kate encourages the sharing of just the proper messages quickly. It combines direct and indirect trust values among drones in two scenarios. So, when estimating trust, the state transition variable and importance factor are attached. Weighted fused decision values based on predicted trust values

3. Presented Procedureology

paradigm is designed by The suggested paradigm designed TARS for efficient packet transfer in ad-hoc networks. This work's primary goal is to build confidence among communicating UAVs and pick the most reliable UAV that can keep data and has enough energy for the duration of the trip. The AAFSA strategy picks the CH (CH) for effective communication and data transmission. This research effort presents an ITOPSIS to improve route discovery. Fig. 1 depicts the methodology's basic outline.

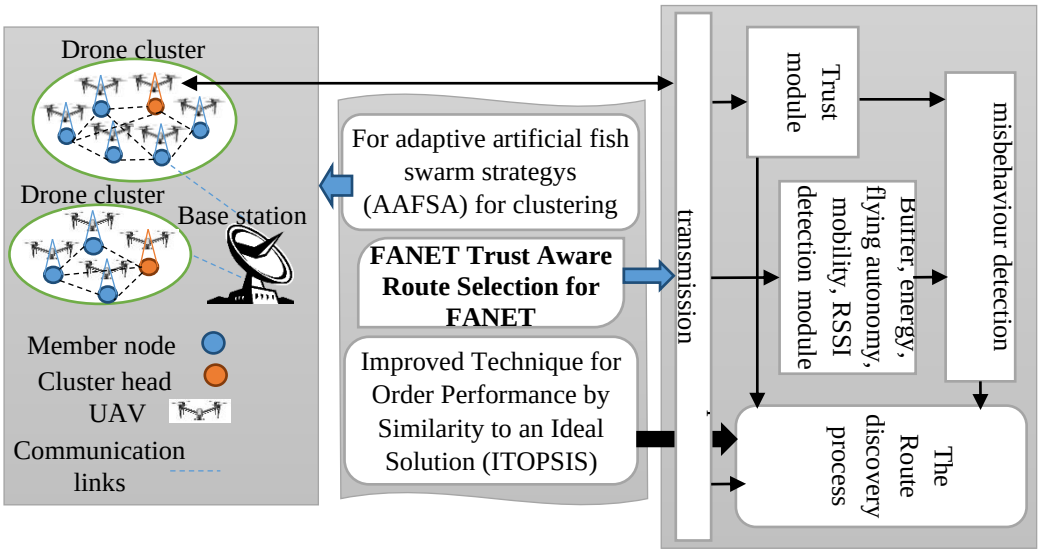

Fig. 1. The general framework of the presented procedure of Trust Aware Route Selection (TARS) in FANET

3.1. Network method

In this case, a collection of n UAVs is spread uniformly in 3D space. Each UAV's battery is initially considered fully charged, with the battery gradually depleting over time. UAVs collaborate to complete a task that demands the unicast exchange of important messages between them. Assume that each UAV utilizes GPS to measure its geographical position (x, y, z) and that it regularly updates both its routing and neighbour tables. Bidirectional links between two UAVs operate in the 5 GHz wireless band and are classified as such.

3.2. Cluster formation and CH selection using AAFSA

CH selection is a critical stage in the routing process. The AAFSA approach has been presented for extracting CH from network datasets to detect malicious assaults. AFSA [20] is a metaheuristic strategy that combines the random search concept with empirical rules. AFSA solves optimization issues by replicating the movement of schools of fish and the intelligence that drives these behaviours. AFSA is classified into three types: follow, swarm, and prey. AFSA performs these three functions for each fish (UAV node) to identify the best solution.

And a linkConverting the CH selection problem into an AFSA-friendly form is required. Researchers found flaws in AFSA's function, such as the likelihood of falling into a local optimum and lack of diversity. This study created a dynamic AAFSA procedure for UAV node swarm selection. The UAV nodes are indicated by x 1 to x n. In this case, 0 signifies that the UAV node is not selected, whereas 1 suggests that it is. The AAFSA randomly initializes the value of the drone clusters of each UAV node. Then use the fitness function Ff to measure the fitness value of each UAV node or drone cluster based on Link capacity, remaining energy, and distance between nodes. Execute the three search stages (follow, swarm, and prey) for each UAV node. If the strategy's terminal requirements are met, halt it and output the ideal drone cluster. If not, restart the procedure at finding fitness function $\mathfrak{F}\mathfrak{f}$ Assume $x_i = (x_i^1, \dots, x_i^d, \dots, x_i^D)$ is i[th] UAV's location, and the three optimal search stages of AAFSA (follow, swarm, and prey) are described below.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.682-692
https://publishoa.com
ISSN: 1309-3452

Follow Search. To execute a follow for x_i, its fitness value is compared to the best UAV node nearby (among its neighbours). Suppose the surrounding UAV node's best fitness value is better than the UAV node in question, and the neighbour's crowd degree is not greater than the maximum. In that case, the neighbour's cluster and attributes replace the drone cluster's. If the subset and attributes are successfully returned, the procedure proceeds to the next UAV node; otherwise, swarm for x_i.

Swarm Search. If the following function for x_i fails, the strategy swarms. The fitness value of $x_i$is now compared to the centre of the neighbouring UAV node. If the centre's fitness value is better than the UAV node's, and its crowd degree does not exceed the maximum, the centre's cluster and attributes replace the drone cluster's. If the subset and attributes are successfully returned, the strategy conducts follow for the next UAV node; otherwise, prey for x_i. Each cycle adds a specific x_i to the pool based on the crossover probability. The crossover is performed between each UAV node to create a child UAV node. The arithmetic crossover of the parent UAV node determines the position of the child UAV node:

$$x_i^{parent} = rand(\cdot) \times x_1^{parent} + \left(1 - rand(\cdot) \times x_2^{parent}\right) i \in (0, n)$$

Where $r\ and\ (\cdot)$ are randomly created numbers between zero and 1, and n is the number of variables.

AtPrey Search. If the swarm function fails for x_i, the strategy will prey. In this stage, the strategy randomly modifiesx_i's UAV nodes to build a new random UAV node. The UAV node's vision limits the most significant number of changes. If the random UAV node's fitness value exceeds x_i, the random UAV node's cluster and attributes are used instead. Otherwise, it will keep searching for a random UAV node until it reaches the specified maximum number of attempts. The AAFSA attributes are as below

:

$$dist(x_i, x_j) = \sum_{k=1}^{k} \left| x_i(k) - x_j(k) \right|$$

Dynamic vision-based CH detection: The vision parameter affects the number of surrounding UAV nodes with whom the target UAV node will interact, impacting the success of steps followed and swarm and assigning the vision parameter higher raises the possibility of identifying UAV nodes with better fitness levels, leading to swarming centralization. This reduces species variety and can lead to a local optimum. We used the endocrine-based formula from [21] to produce dynamic vision. Each UAV node gets its vision parameter values based on fitness. For example, if fitness is above average, vision is reduced, and vice versa. The endocrine ($\mathfrak{Ed}$)-based formula is described as below:

$$\mathfrak{Ed}(i) = \mathfrak{Ff}_1\left(\frac{\mathfrak{Ff}_{max} - \mathfrak{Ff}_i}{\mathfrak{Ff}_{max} - \mathfrak{Ff}_{avg}}\right) \cdot \left[\frac{\pi}{2} + \mathfrak{Ff}_2\left(\mathfrak{Ff}_i - \frac{\mathfrak{Ff}_{i-1} + \mathfrak{Ff}_{i+1}}{2}\right)\right]$$

$$Dynamic\ Vision\ (i)\ =\ Vision\ (x_i)\ \mathfrak{Ed}(i)\mathfrak{A}$$

$$Vision\ (Fe_i) = \frac{\sum_{k=1}^{k} \sum_{k=1}^{N} \left| Fe_i(k) - Fe_j(k) \right|}{Total\ number\ of\ fishes\ (UAV\ nodes)}$$

$\mathfrak{Ed}(i)$ represents the fitness value of the UAV node x_i, $\mathfrak{Ff}_{max}$. $\mathfrak{Ff}_{i+1}$represents the fitness values of the UAV node. $\mathfrak{Ed}(i)$represents the endocrine system of UAV node xi, $\mathfrak{Ff}_{max}$represents the maximum fitness value of the UAV node in the school, and $\mathfrak{Ff}_{avg}$represents the average fitness value in the school. $\mathfrak{Ff}_{i-1} = arc\ tangent\ (x); \mathfrak{Ff}_2 = arc\ tangent\ (-x)$. $\mathfrak{A}$ is the adjustment constant to raise the global search ability to acquire solutions more rapidly.

The formula found the neighbors $Neig$ of x_i. Any UAV node x_j with a distance surpassing 0 but not surpassing the vision of x_i is deemed a neighbour of x_i.

$$Neig(x_i) = \{Wx_k | 0 < dist(x_i, x_k) \leq dynamic\ vision\}$$

The Weight$W$ of each UAV can be evaluated by

$$\mathfrak{Ff} = W\ =\ w_1 C_l\ + w_2 R_e\ +\ w_3\ Neig(x_i), \qquad \forall w1\ +\ w2\ +\ w3\ =\ 1$$

C_l is the link capacity, R_e is residual energy, and $Neig(x_i)$ is the outcome of the neighbour search, $w_1, w_2, w_3$is described as a weighting factor.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.682-692
https://publishoa.com
ISSN: 1309-3452

Center detection: The centre *One cent* of Fe_i was evaluated using the formula. If among more than half of the UAV nodes in the neighbourhood of Fe_i, the first UAV node is 0, then the value of the centre is set to 0. If among more than half of these UAV nodes, the first UAV node is not 0, then the centre's value is set to 1.

$$Cent(x_i) = x_{center}(i) = \begin{cases} 0 & \sum_{k=1}^{k} x_k(i)\frac{k}{2} \\ 1 & \sum_{k=1}^{k} x_k(i)\frac{k}{2} \end{cases}$$

Crowd Degree calculation: The crowd degree $\mathfrak{CD}$ of x_i was evaluated using the formula. This parameter indicates the density of the UAV node in the vicinity of x_i.

$$\mathfrak{CD}(x_i) = \frac{Neighbors\ of\ x_i}{Total\ number\ of\ fishes}$$

In the execution of steps following and swarm, we intended to avoid the accumulation of all UAV nodes at the same spot by defining that if the crowd degree of x_i surpassed the maximum, then no other UAV node would be authorized to approach this location. In other words, no other UAV node would be able to replace its drone cluster using that of x_i.

Maximum Number of Attempts: This is the maximum number of times that prey can be run. The flow diagram of CH selection based on AAFSA is shown in Fig. 2.

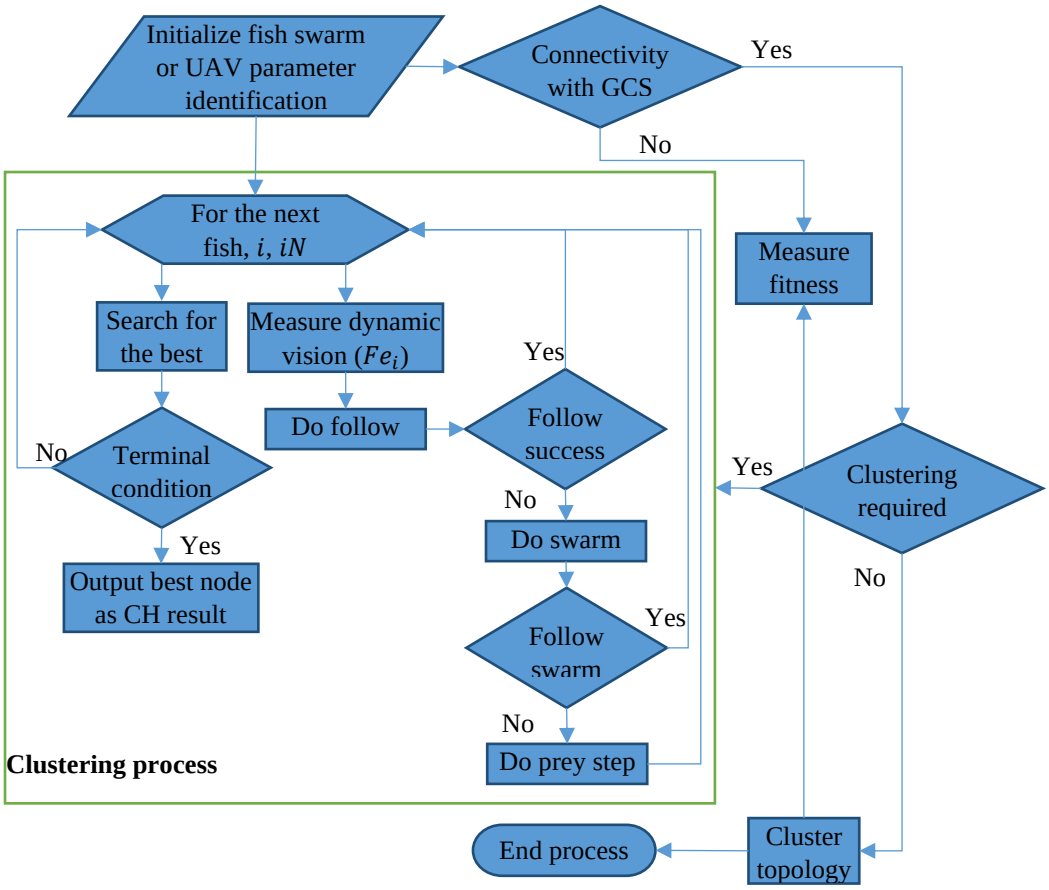

Fig.2.Flow Diagram of diagram of CH selection based on AAFSA

Every drone in a cluster determines its fitness. Each UAV delivers a message with its fitness. When UAV receives that, it compares it to its fitness. A UAV connected to GCS defines itself as CH. Suppose more than one UAV connects to the GCS, the fittest UAV broadcasts cluster formation and proclaims itself CH. If the UAV's fitness is lower than the others, it recognizes the CH and sends CJM. When a UAV needs to communicate data but is out of GCS range, an ad hoc coalition of UAVs is created. The UAV subsequently delivers data to the distant target via intermediate UAVs. The GCS-connected UAV will proclaim itself as CH and send the cluster formation message to other UAVs. The other UAVs

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.682-692
https://publishoa.com
ISSN: 1309-3452

will join it. If no UAV has direct contact with the GCS, communication can be done via a relay UAV from another cluster. As shown in Fig. 2, the UAV with the highest fitness is picked as CH, and the rest of the UAVs become cluster members.

3.3. Trust computation method

This work's trust method determines node trust by two factors: direct and indirect trust. The explicit trust is recognized using the modified Bayesian theorem.

Direct trust: To limit the fault in measuring a node's duplication, we combine the previous reputation level and likelihood function. Assuming the preceding chance is satisfiable by the Beta distribution and the likelihood function, then the final posterior probability is also satisfiable. The direct trust of UAV node B should be impacted by their interaction time and the total packets transmitted. So we can utilize two metrics: time attenuation and complete packets transmitted. The direct trust evaluating formula is as below:

$$Directrust_{AB} = \frac{\sum_{i=1}^{t} \rho^{t-i} PF_{AB}^{i}}{\sum_{i=1}^{t} \rho^{t-i}} * \frac{a_i}{a_i + b_i}$$

In which, $\rho^{t-i} (o < \rho < 1)$ indicates the time attenuation function, and PF_{AB}^{i} suggests the number of packets transferred by node *B* for node *A* during the period. When there is no direct communication between nodes *A* and *B*, the value of $Directrust_{AB}$ is set to 0.5.

Indirect Trust: The indirect trust factor is vital in node trust calculation. The indirect trust is measured using two trust recommendation indicators (recommendation credibility and activity factor). Although nodes A and B have never interacted, A can nevertheless determine B's trust value by aggregating other nodes' recommendations.

Credibility. Others defame other trustworthy nodes while not discarding or modifying the traffic. This form of attack is also known as slander. To counteract these assaults, we can measure the recommendation node's credibility. Node credibility recommendation:

$$Indirectrust_{credit\,j} = \frac{e^{\frac{-1}{R}} \sum_{i=1}^{R} \sum_{k=1}^{N} \rho^{N-k} \left(1 - \left| directrust_{jj_l}^{k} - directrust_{ij_l}^{k} \right|\right)}{R}$$

It is assumed that $\{j_1, j_2, \ldots, j_r\}$ are the neighbours of a node that have interactions with node i, j_l is termed as the trust evaluation of node, $0 < e^{-\frac{1}{R}} < 1$, and this metric is used to modify the number of nodes in the assessment of trust. The greater the value of R is, the closer it is to 1.

Activity. The metric $Activity$ can be defined as the activity factor. If the number of neighbours of a specific node is G, and the number of neighbours that have recently interacted with this node is F, then we can measure roughly the activity of this node using an indirect trust following equation,

$$Indirectrust_{B} = \frac{\sum_{j=1}^{F} Indirectrust_{credit\,j} Directrust_{jB} PF_{AB}^{i}}{\sum_{j=1}^{F} Directrust_{jB} PF_{AB}^{i}} * \frac{F}{G}$$

3.4. Trust Aware Route Discovery (TARD)

Communication routes in a FANET are chosen depending on hop count, battery, delay, and mobility. The method transmits data by picking the most reliable way. The link-state information is monitored during transmission, and broken links are fixed quickly to increase data transmission efficiency and link stability. Node mobility was anticipated to be 3-20 m/s. Following is the ITOPSIS route selection process.

Step 1: The first step is to define your goals. In our scenario, the goal is to pick a dependable route from among the choices. The goal is to find routes with high flight autonomy, high trust value, low mobility, short neighbour range, higher link quality, and higher RSSI. It reduces network energy consumption and, as a result, raises cluster longevity.

Step 2: Create the matrix based on the attributes' values and information for all choices.

Step 3: The normalized decision matrix was derived using the given equation.

$$NR_{i,j} = \frac{m_{i,j}}{\left[\sum_{j=1}^{OM} m_{i,j}^{2}\right]^{1/2}}$$

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.682-692
https://publishoa.com
ISSN: 1309-3452

In which $m_{i,j}$ is the element that gives the jth attribute of ith alternative. OM is the order of the matrix.

Step 4: Create a relative priority matrix for various attributes using the Analytical Hierarchy Process (AHP).

Step 5: Acquire the weighted normalized matrix $WN_{i,j}$ as shown in equation

$$WN_{i,j} = w_j NR_{i,j}$$

In which w_j is the weight given by the AHP.

Step 6: To retrieve the ideal best (WN^+) and ideal worst (WN^-).

$$WN^+ = \left\{\left(\sum_i^{max} WN_{i,j\,/j\in J}\right), \left(\sum_i^{min} WN_{i,j\,/j\in J}\right)\right\}, i = 1,2,\dots,N$$

$$WN^- = \left\{\left(\sum_i^{max} WN_{i,j\,/j\in J}\right), \left(\sum_i^{min} WN_{i,j\,/j\in J}\right)\right\}, i = 1,2,\dots,N$$

Where J is related to beneficial attributes like battery whereas J' is related to attributes that are non-beneficial, WN^+ reflects the best value of the particular attribute of all the alternatives, WN^- reflects the worst deal of the specific attribute among options.

Step 7: The Euclidian distance's separation measurements from the ideal solution are given, as illustrated below equations.

$$sol^+ = \left\{\sum_{J=1}^{M}\left(WN_{i,j} - WN_j^+\right)^2\right\}^{0.5}$$

$$sol^- = \left\{\sum_{J=1}^{M}\left(WN_{i,j} - WN_j^-\right)^2\right\}^{0.5}$$

Step 8: The relative closeness of alternative to the ideal solution P_i can be described by$P_i = \frac{sol^-}{sol^+ + sol^-}$

Step 9: From the ratioPi, a list of options is constructed in descending order, delivering the most desirable and least desirable routing route solution. After the procedure, it is checked once more to see if the produced result is an absolute route and a route between the two points. After locating the routes, the two shorter than the others are chosen; the first route is utilized to transfer data packages, while the second is saved as a substitute route to be used if the first route fails.

4. Experimental outcomes and discussion

The presented AAFSA strategy's performance regarding energy consumption, throughput, delay, overhead, and packet delivery ratio is evaluated and compared to previous Adaptive Mutation with Teaching-Learning-Based Optimization (AMTLBO), Ant Colony Optimization (ACO) [22], and Self Organization based Clustering Paradigm (SOCS) [23] approaches. The performance study was carried out using the NS2 simulation environment, and it assessed different area sizes for deploying UAVs with varying numbers of UAVs. The remaining simulation assigning's are listed in Table 1.

Table 1: Simulation attributes

Attributes	**Values**
Grid size	1000×1000 m^2, 2000×2000 m^2
Number of UAVs	50
The minimum distance between UAVs	5m
Mobility method	Reference point mobility method
Simulation time	120s

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.682-692
https://publishoa.com
ISSN: 1309-3452

Transmission range	Dynamic
Position exchange interval	2s
Receiver sensitivity	-90dBm
Transmission frequency	2.45GHz
Constant bit rate	100kbps

4.1. Packet Delivery Ratio (PDR)

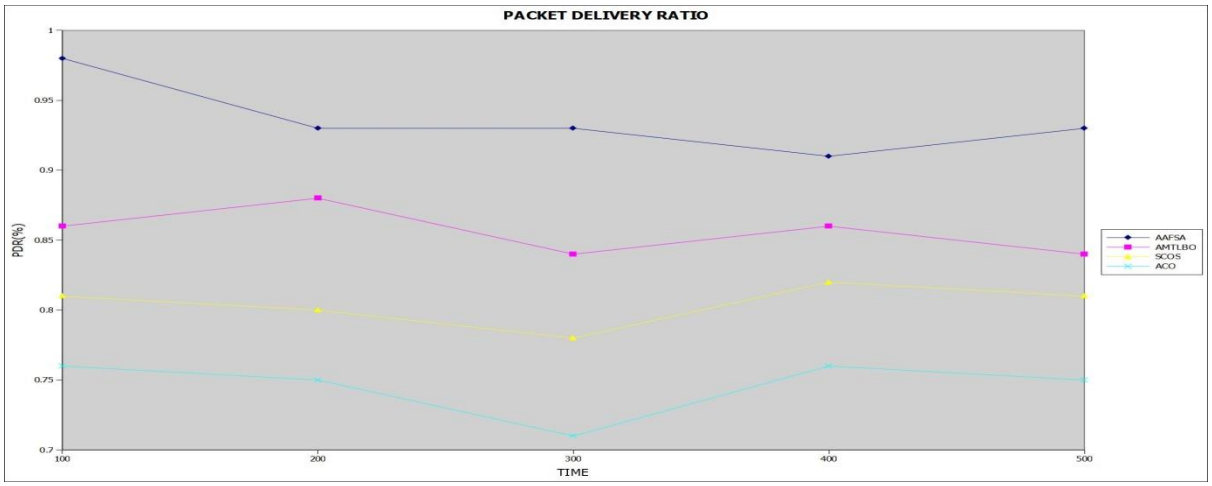

Fig.3. Packet Delivery Ratio vs Time

Figure 3 shows the packet delivery ratio, simply the number of delivered and transmitted messages to the user. It usually depicts the message's status at the destination node. Compared to the existing ACO, SCOS, and AMTLBO techniques, the presented AAFSA has a more excellent packet transmission ratio. As shown in the figure, the proper delivery ratio grows with time. When the time value is 50, and the AAFSA PDR is 94%, the presented work is more effective for FANET. Indirect and direct trust calculations find trustworthy nodes in their neighbour.

4.2. Throughput (TP)

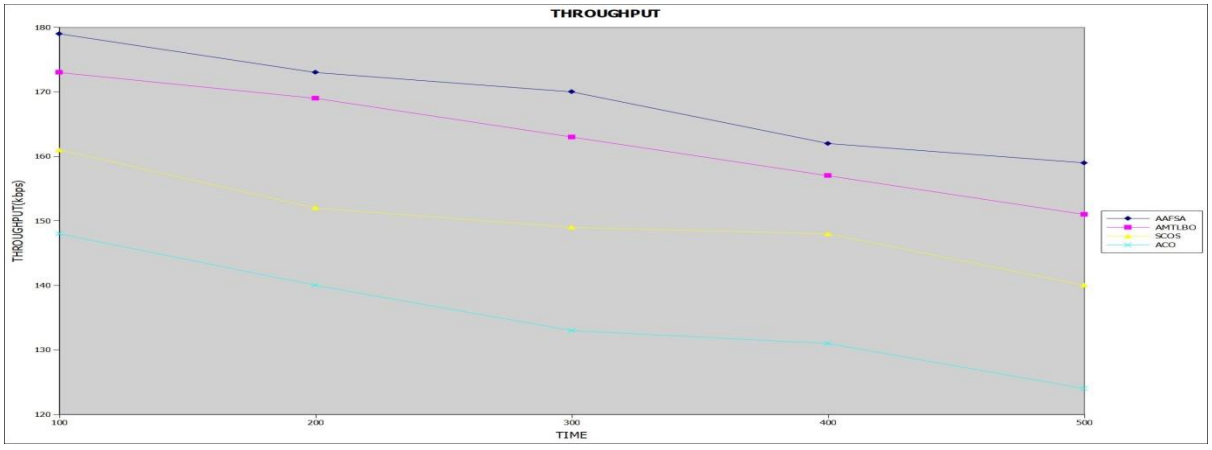

Fig.4. Throughput vs Time

Fig.4 compares the anticipated AAFSA with the existing ACO, SCOS, and AMTLBO techniques. The recommended AAFSA achieves greater throughput than conventional techniques. The performance of node throughput is observed to be higher with increasing nodes. Compared to existing procedures, the suggested process has a throughput rate of 178kbps at 100. Because the presented method can recognize rogue nodes in an AAFSA-based system, the throughput would be higher.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.682-692
https://publishoa.com
ISSN: 1309-3452

4.3. End-To-End Delay (EED)

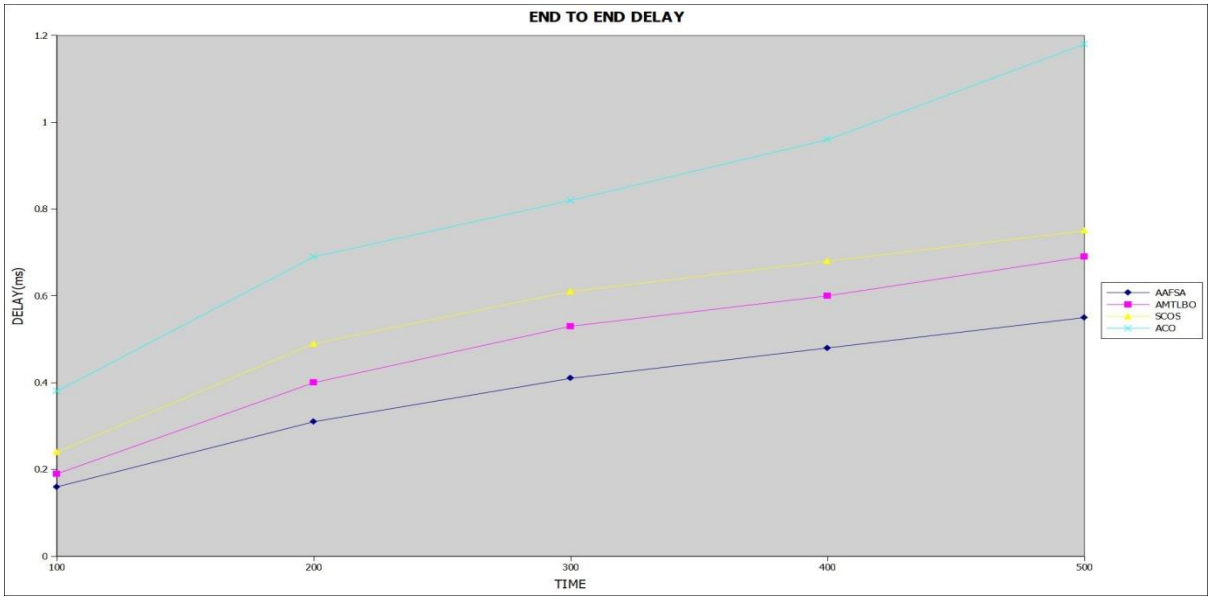

Fig.5. Delay vs Time

Fig.5 compares the planned aafsa to the present UAKMP. Delay was reduced compared to conventional procedures as time rose. The suggested AAFSA has a 98ms delay rate than the present UAKMP, which is 7.94ms higher than the presented technique. The recommended approach measures a sensor node's secret key value using the ROR method at each layer. As a result, the suggested job is faster than the previous study.

4.4. Communication overhead

End to end delay is defined as the total time to complete the successful data transmission.

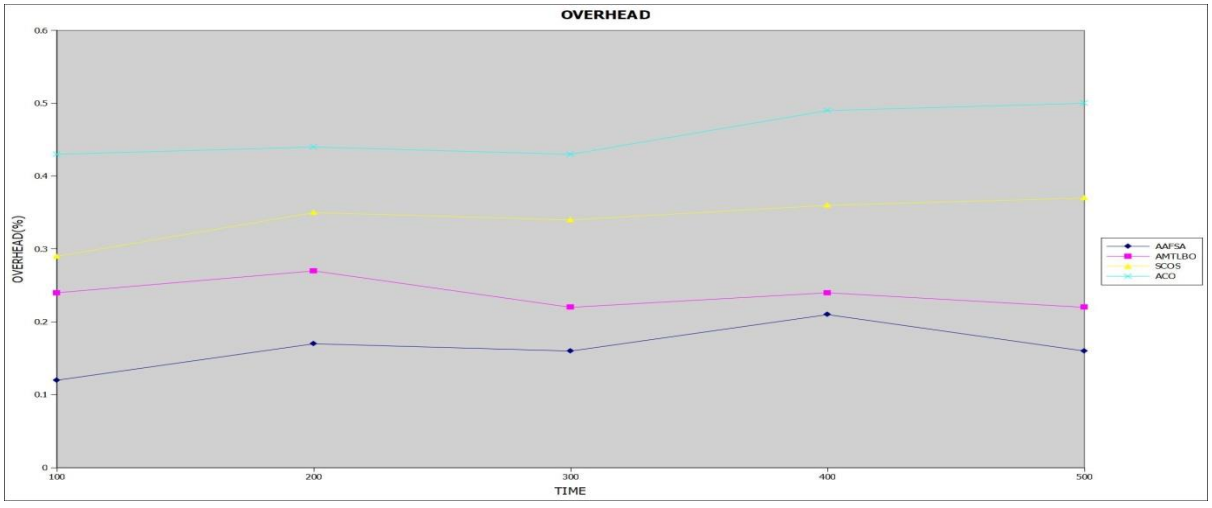

Fig.6. Communication overhead vs Time

Figure 6 compares the suggested AAFSA to ACO, SCOS, and AMTLBO paradigms. This approach uses a low communication overhead of 77105bits per second. When compared to conventional procedures, the communication overhead rate is low. As a result, AAFSA is more efficient due to its reduced communication bandwidth.

4.5. Energy consumption

The overall time expected to accomplish a successful data transfer is an end-to-end delay.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p.682-692
https://publishoa.com
ISSN: 1309-3452

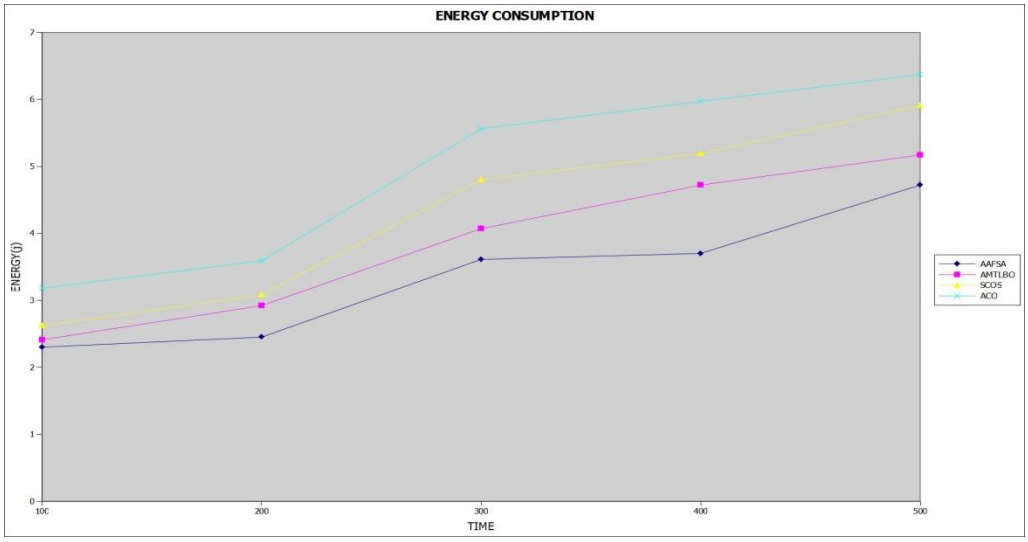

Fig.7. Energy consumption vs Time

Figure 7 depicts the energy consumption comparison outcomes between the suggested AAFSA and the existing ACO, SCOS, and AMTLBO paradigms. At a time rate of 100, the presented approach has a low energy consumption rate of 9.8J. The findings are impressive when comparing the energy consumption rate of previous procedures. The AAFSA is more efficient due to the efficiency of picking the most trustworthy nodes as possible group leaders and detecting harmful actions using TARD. These trust ratings were based on various measures used to analyze UAV's behaviour within the group while protecting the members' privacy and minimizing network overhead.

5. Conclusion and future work

We presented an AAFSA-based FANET clustering technique. An efficient CH election based on ground control station connectivity, luciferin value and UAV residual energy was optimized by AAFSA for communication in FANETs. Propose a trust-based route selection system based on neighbour range, residual power, and UAV position for effective communication. The suggested AAFSA outperforms TARD paradigms regarding energy consumption, PDR, delay, throughput, and delay success. AAFSA exceeds ACO, SCOS, and AMTLBO because it can optimize CH selection and optimal trust-based neighbour selection from a neighbourhood range, making it suited for cluster-based FANET. In other words, by picking more stable channels with higher energy rates, the technique improved overall network efficiency and data package delivery reliability. In the future, a Collison-free Hybrid Trust Method (HTM) can be utilized to assess UAV reliability in FANETs. Intend to implement a lightweight access control procedure to respond to external attackers.

References

1. Tareque, M. H., Hossain, M. S., &Atiquzzaman, M. (2015, September). On the routing in flying ad hoc networks. In *2015 federated conference on computer science and information systems (FedCSIS)* (pp. 1-9). IEEE.
2. Zafar, W., & Khan, B. M. (2016). Flying ad-hoc networks: Technological and social implications. *IEEE Technology and Society Magazine*, *35*(2), 67-74.
3. Bekmezci, I., Sahingoz, O. K., &Temel, Ş. (2013). Flying ad-hoc networks (FANETs): A survey. *Ad Hoc Networks*, *11*(3), 1254-1270.
4. Zheng, Z., Sangaiah, A. K., & Wang, T. (2018). Adaptive communication protocols in flying ad hoc network. *IEEE Communications Magazine*, *56*(1), 136-142.
5. Zhou, Y., Cheng, N., Lu, N., & Shen, X. S. (2015). Multi-UAV-aided networks: Aerial-ground cooperative vehicular networking architecture. *ieee vehicular technology magazine*, *10*(4), 36-44.
6. Cumino, P., Lobato Junior, W., Tavares, T., Santos, H., Rosário, D., Cerqueira, E., ... &Gerla, M. (2018). Cooperative UAV paradigm for enhancing video transmission and global network energy efficiency. *Sensors*, *18*(12), 4155.
7. Rosati, S., Krużelecki, K., Heitz, G., Floreano, D., &Rimoldi, B. (2015). Dynamic routing for flying ad hoc networks. *IEEE Transactions on Vehicular Technology*, *65*(3), 1690-1700.
8. Naseer, A. R. (2012). Reputation system based trust-enabled routing for wireless sensor networks. *Wireless Sensor Networks: Technology and Protocols*, 233.

9. Kerrache, C. A., Barka, E., Lagraa, N., &Lakas, A. (2017, September). Reputation-aware energy-efficient solution for FANET monitoring. In *2017 10th IFIP Wireless and Mobile Networking Conference (WMNC)* (pp. 1-6). IEEE.
10. Singh, K., Verma, A. K., & Aggarwal, P. (2018). Analysis of various trust computation procedures: a step toward secure FANETs. In *Computer and Cyber Security* (pp. 171-193). Auerbach Publications.
11. Shenets, N. N. (2019). Security infrastructure of FANET based on secret sharing and authenticated encryption. *Automatic Control and Computer Sciences*, *53*(8), 857-864.
12. Singh, K., &Verma, A. K. (2020). TBCS: A trust based clustering paradigm for secure communication in flying ad-hoc networks. *Wireless Personal Communications*, *114*, 3173-3196.
13. Singh, K., &Verma, A. K. (2018). FCTM: A Novel Fuzzy Categorization Trust Method for Enhancing Reliability in Flying Ad Hoc Networks (FANETs). *Ad Hoc Sens. Wirel. Networks*, *40*(1-2), 23-47.
14. Bhardwaj, V., & Kaur, N. (2021). SEEDRP: a Secure Energy Efficient Dynamic Routing Protocol in Fanets. *Wireless Personal Communications*, 1-27.
15. Kalinin, M. O., Zubkov, E. A., Suprun, A. F., &Pechenkin, A. I. (2018). Prevention of attacks on dynamic routing in self-organizing adhoc networks using swarm intelligence. *Automatic Control and Computer Sciences*, *52*(8), 977-983.
16. Singh, K., &Verma, A. K. (2018, April). A trust method for effective cooperation in flying ad hoc networks using genetic algorithm. In *2018 International Conference on Communication and Signal Processing (ICCSP)* (pp. 0491-0495). IEEE.
17. Mohammed, F., Jawhar, I., Mohamed, N., &Idries, A. (2016, April). Towards trusted and efficient UAV-based communication. In *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)* (pp. 388-393). IEEE.
18. Singh, K., &Verma, A. K. (2018). A fuzzy-based trust method for flying ad hoc networks (FANETs). *International Journal of Communication Systems*, *31*(6), e3517.
19. Bhargava, A., &Verma, S. (2020). KATE: Kalman trust estimator for internet of drones. *Computer Communications*, *160*, 388-401.
20. Neshat, M., Sepidnam, G., Sargolzaei, M., &Toosi, A. N. (2014). Artificial fish swarm algorithm: a survey of the state-of-the-art, hybridization, combinatorial and indicative applications. *Artificial intelligence review*, *42*(4), 965-997.
21. Lin, K. C., & Hsieh, Y. H. (2015). Categorization of medical datasets using SVMs with hybrid evolutionary algorithms based on endocrine-based particle swarm optimization and artificial bee colony algorithms. *Journal of medical systems*, *39*(10), 1-9.
22. Zhao, L., Saif, M. B., Hawbani, A., Min, G., Peng, S., & Lin, N. (2021). A novel improved artificial bee colony and blockchain-based secure clustering routing paradigm for FANET. *China Communications*, *18*(7), 103-116.
23. Khan, A., Aftab, F., & Zhang, Z. (2019). Self-organization based clustering paradigm for FANETs using Glowworm Swarm Optimization. *Physical Communication*, *36*, 100769.