**Trust Computation in FANET**

**Joydeep Kundu, Suman Ghosh, Jeet Majumder, Tridibesh Debnath**

Department of Computer Science & Engineering, BRAINWARE UNIVERSITY,

Contact No. Email:

Contact No. – 9635346003 Email: [ghoshsuman1079@gmail.com](mailto:ghoshsuman1079@gmail.com)

Contact No. – 6297207270 Email: [jeet0912majumder@gmail.com](mailto:jeet0912majumder@gmail.com)

Contact No. – 7797282123 Email: [tridibeshdebnath@gmail.com](mailto:tridibeshdebnath@gmail.com)

**Abstract:**

Since unmanned aerial vehicles may function in dynamic environments including armed attacks, border monitoring, disaster management, rescue operations, and transportation, their application in building ad hoc networks has expanded dramatically. Flying ad hoc networks (FANETs) is a common name for these kinds of ad hoc networks. The two main characteristics of FANET nodes are cooperation and collaboration. The behaviour of these nodes can be predicted in large part by trust. To determine the trust value of a specific node in ad hoc networks—particularly in mobile and vehicular ad hoc networks—researchers have put forth several direct and indirect methods; consequently, there are frequent losses. In topology and connectivity changes. Consequently, the current trust management techniques collation are not productive and successful. This paper presents a new fuzzy-based trust model that has been put forth to address FANET's behavioural uncertainty nodes. Multicriteria fuzzy classification is used to classify nodes depending on how the node behaves and performs in a hazy and complicated environment. To separate the self-serving and malicious nodes, the social parameter (recommendation) and quality of service (QoS) are taken into account while assessing each node's trust value. FANET nodes are rewarded or punished based on their classification, which changes their behaviour into a trust value. The results of the simulation demonstrate that the suggested model performs better in FANETs in terms of accuracy, flexibility, and performance when compared to the current trust strategies.

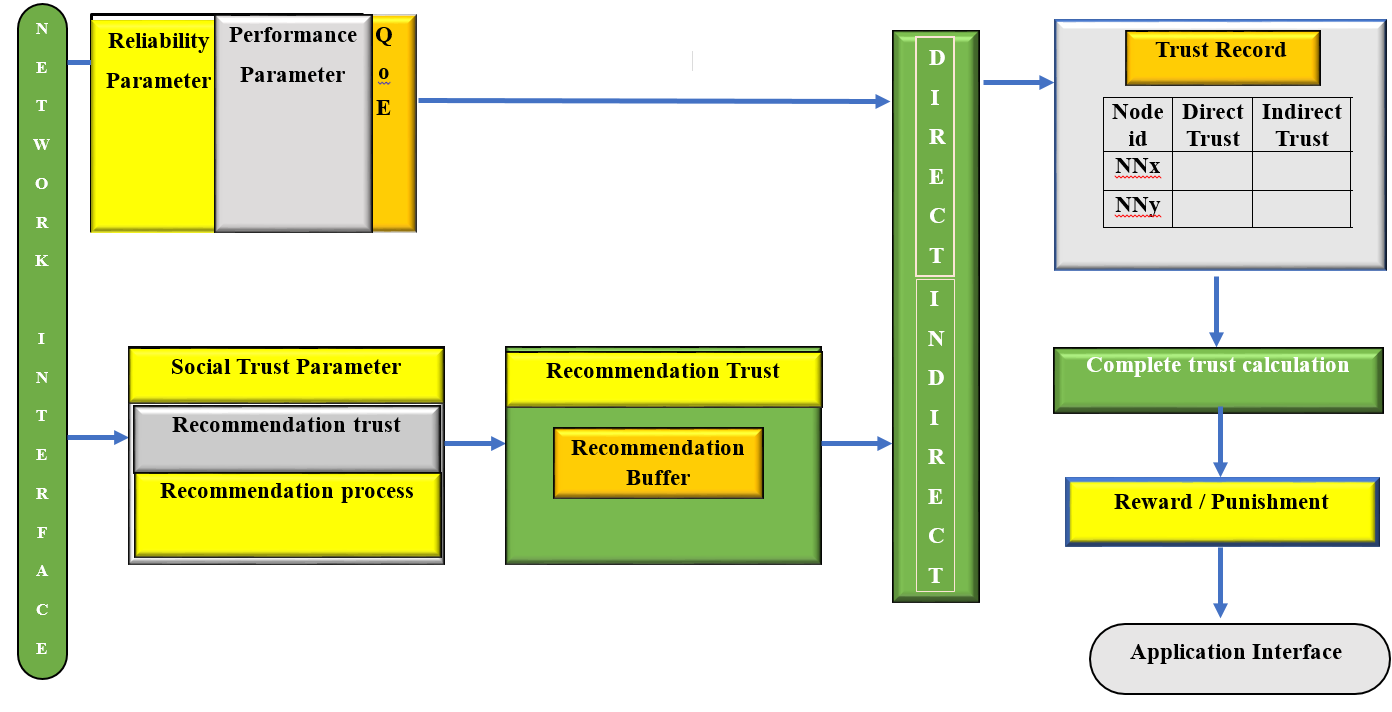
**1. Introduction:**

Drones are being employed for business and non-hobbyist reasons; they were mostly used as toys or military aircraft. Commercial operations become more time and financially effective as a result of the decreased need for infrastructure and human engagement. Drones find application in diverse fields such as agriculture, aerial photography, border surveillance, environmental disaster monitoring, search and rescue operations, emergency support, rebroadcast communications, and weather monitoring. The need for drones has grown, and by 2024, India is predicted to rank third in the world's commercial drone market. Drone technology advancements have created new prospects for a wide range of business uses. Created for automated flying systems, UAV-FANETs are clusters of unmanned aerial aircraft that communicate over ad hoc networks [1-5]. Smart antennas, ground controllers, and UAVs make up these networks. FANETs have two communication architectures. The dynamic nature of the surroundings and the different velocities of UAVs make the UAV network structure complex. Clustering techniques are essential for preserving network performance, including energy economy and end-to-end latency, as the number of UAVs rises. Cluster leaders oversee both intra- and inter-cluster communication. Successful operations depend on effective drone-to-drone communication, and a leader controls several drones to do this. Communication and range issues make it difficult to install numerous drones simultaneously. Failures in communication might result in crashes. Drones operate in clusters to carry out duties and maximise battery efficiency; leaders are selected to enhance communication.

**2. Related Work:**

There are several research [6-12] that have been done to compute trust scores in FANET. A compact mutual authentication system called ATS-LIA [11] was created for use in Flying Ad-hoc Networks (FANETs), which are made up of unmanned aerial aircraft (UAVs) that communicate wirelessly. By evaluating a UAV's trustworthiness based on past interactions and behaviour, adaptive trust techniques are used to enable secure and reliable communication between UAVs. This method ensures strong authentication while minimising communication and computing overhead. The three steps of ATS-LIA are mutual authentication, mutual trust assessment, and registration. By enabling contextual decision-making, its adaptive trust technique enhances network dependability and security. Based on trust levels, the technique can identify and isolate bad UAVs and is resistant to attacks. All things considered, in fast-moving and resource-constrained FANET contexts, ATS-LIA improves communication security and efficiency. Infrastructure-based and ad-hoc communication are combined in the Hybrid Communication Strategy for Efficient and Low-Cost Implementation of Upcoming Flying Ad-Hoc Networks (FANETs) [12] communication approach to maximise the deployment and operation of FANETs. Using a two-tier architecture made up of ground base stations (GBSs) and unmanned aerial vehicles (UAVs), the plan seeks to overcome issues like few resources, changeable network topology, and communication limitations. Whereas UAVs function as mobile nodes and GBSs as fixed backbone points, the FANET is an ad hoc, self-organizing network. Within the FANET, effective and low-latency data sharing is made possible by the ad-hoc communication mode. Path selection for the transfer of data is optimised by the hybrid communication system, which takes into account variables including network quality, resource availability, and distance from GBSs. This strategy maximises resource utilisation, leverages pre-existing infrastructure, and reduces the cost of setting up and operating FANETs. In TBCS, This work presents a novel trust model that is based on fuzzy logic and is intended to address the behavioural unpredictability of FANET nodes. A multicriteria fuzzy classification approach is used to classify nodes according to how they behave and function in a complex and fuzzy environment.

**3. Proposed Scheme:**

We suggest cluster-based trust computation in FANET, a fuzzy-based trust model, as a means of enabling reliable communication between network nodes. The fuzzy classification algorithm is to distinguish between network nodes. The below figure displays the several fuzzy model components that are utilised to determine a node's trust value within the network. The Quality of Service (QoS) model is utilised for characteristics (such as reliability and performance) and social parameters. The social parameter represents the network node's recommendation process and trust, whereas QoS is a measure of the node's performance. The trust computation model that has been suggested aims to classify nodes into three groups: good, bad, and neutral, depending on their performance and behaviour.

**Figure 1: Trust Computation Scheme**

**3.1. Trust Calculation:**

At the beginning, 0.5 is the same threshold value granted to each node. Adjacent nodes use direct observation to determine the direct trust, and they share a recommended value to determine the indirect trust. Every node is categorised into three clusters (bad and good) and Table illustrates how each cluster is rewarded or penalised.

|  |  |  |
| --- | --- | --- |
| **Cluster** | **Reward** | **Punishment** |
| Bad | 0 | 0.5 |
| Good | 2 | 0 |

Using fuzzy clustering, Algorithm 1 proposes a step-by-step method for classifying different nodes in clusters by minimising the objective function. This Algorithm 1 finds the direct trust observation for each node by optimising the weights of each parameter.  Algorithm 2 determines the indirect trust of each node's trust values by using direct trust.

**Input:** Node energy, Packet delivery ratio, Transmission delay, Signal strength

**Output:** Direct Trust ( )

1. No. of Drones = { | x = 1, 2, 3, ……….., n} // Total no. of drones
2. No. of input Parameters= = { | x = 1, 2, 3, ……….., n| y = 1, 2, 3, ………., m} // Total input Parameters set
3. Weight factors of the Drones (W)= {| f = 1, 2, 3, ……., m} // Weight assigned to individual drones which satisfy
4. Normalization of the input parameter matrix P in terms of 1
5. Calculate Weight matrix
6. Calculate Direct Trust through weight matrix

for i = 1 :

if ( weight < = 0.29 )

trust = 0.5\*

else if ( 0.3 < weight < 0.69 )

trust = 0.5\*

else (weight > 0.7 )

trust = 0.5\*

end

end

1. **return** Direct Trust

**Figure: Algorithm 1 (Direct Trust)**

**Algorithm 1: Direct Trust Score Computation**

**Input:** Direct Trust of nodes

**Output:** Indirect Trust ( )

1. Direct Trust of nodes
2. // Recommendation of nodes from other network

//The received recommendation ( Rec ) sourced by UAV A concerning the behavior of UAV B ( ) is represented by

1. **Return** Indirect Trust

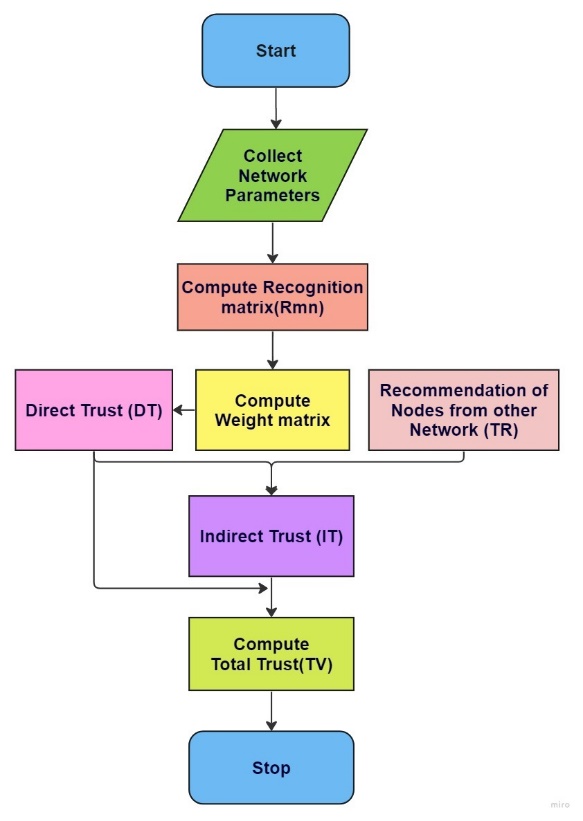
**Algorithm 2: Indirect Trust Score Computation**

**Input:** Weights for direct and indirect trust and

**Output:** Total trust value

1. Direct Trust
2. Indirect Trust
3. \* + \*
4. **return**

**Algorithm 3: Total Trust Score Computation**

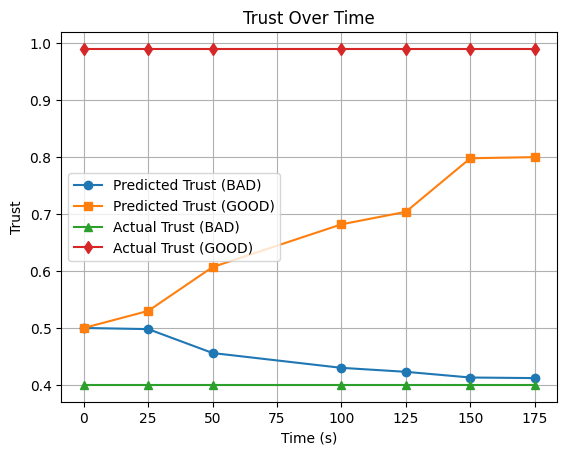
**3.3. Flowchart:**

**Figure 2: Proposed Working Mechanism of Trust Score Computation**

**4. Implementation of result:**

The simulation results of the suggested trust model are reviewed in this section. An evaluation environment has been set up to assess the effectiveness of the suggested trust structure. There are three categories of nodes in the network: good and bad nodes. Good nodes are those that correspond to network protocols and behave appropriately, and bad nodes are those that consistently misbehave.

**4.1. Trust Levels:**

The figure makes it clear that the network's trust levels for the good nodes approach 0.9 and the bad nodes' trust levels near 0.4. The nodes are classified as good and bad based on threshold values that are defined by trust levels.

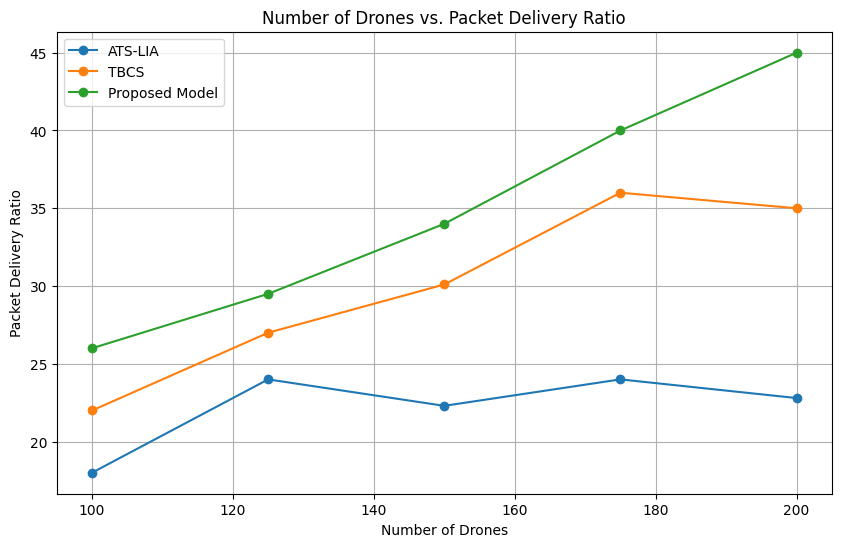
**Figure:** Trust levels of good and bad node

**4.2. Membership functions:**

The membership function of the three main characteristics— packet delivery ratio, node energy, and transmission delay—that are suggested to be utilised in determining the trust value in FANETs are covered.

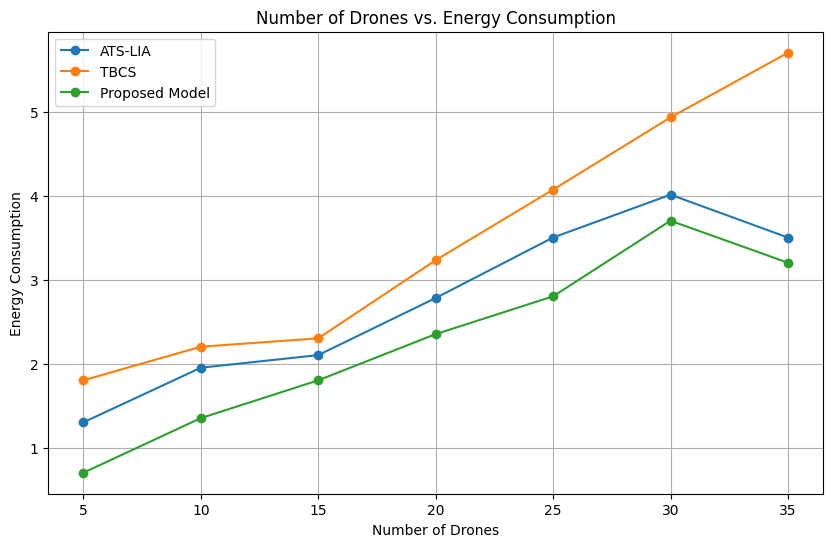
**4.2.1. Packet Delivery Ratio:**

A network of nodes was simulated using the network performance evaluation as a basis, and the average, lowest, and maximum packet delivery ratio values were recorded. A node with a packet delivery ratio of more than 40% is regarded as trustworthy and has a good reputation. A network node with a reputation for neutrality is defined as having a delivery drop ratio of greater than 35%. Conversely, a node with a reputation for unreliability is defined as having a packet delivery ratio of less than 25%.



**Figure: Number of Drones VS Packet Delivery Ratio**

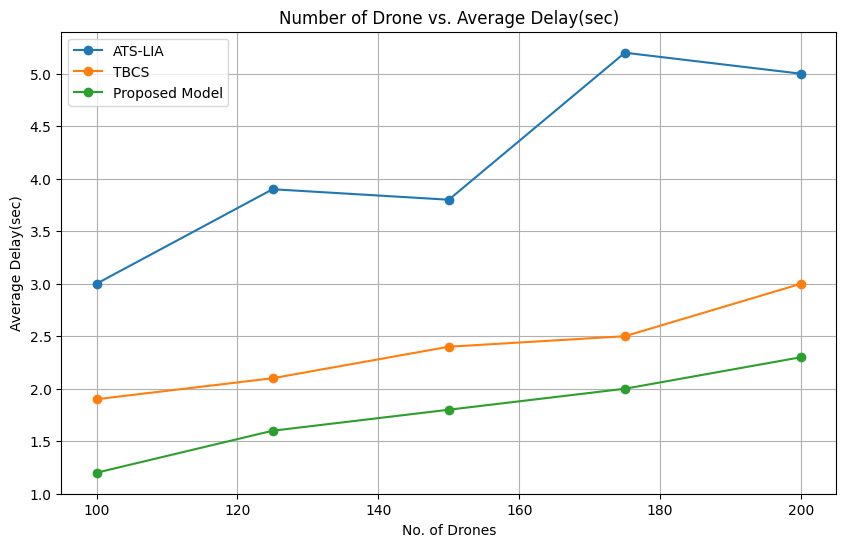
**4.2.2. Node’s Energy:**

**** Node energy, as used in Flying Ad-Hoc Networks (FANET), describes the energy resources that are accessible to particular nodes, which are usually drones or unmanned aerial vehicles (UAVs). FANET development and execution are highly dependent on managing node energy because these UAVs' ongoing batteries have a limited capacity.

**Figure: Number of Drones VS Energy Consumption**

**4.2.3. Transmission Delay:**

One measure of network performance that can be used to assess a node's trustworthiness is transmission delay. A node that lacks self-interest or wicked intentions will transfer data packets slowly. The time it takes for a signal or data packet to go from the initial node to the destination node inside the network is referred to as the transmission delay in a Flying Ad-Hoc Network (FANET). Numerous factors affect this latency, which is an important element to take into account while designing and assessing the performance of FANETs.



**Figure: Average Transmission delay over the number of drones**

**5. Conclusion:**

This study proposes a fuzzy-based trust model that combines direct and indirect trust to detect and separate hostile and non-cooperative nodes in FANETs. The outcomes confirm that the suggested trust model can be used to distinguish between wicked and no cooperative nodes. Additionally, when network size increases, detection accuracy rises as well, suggesting that the suggested approach is very scalable. The model's trust levels and node behaviour are in agreement. Moreover, it has been shown that a strong dependence on recommendations, or social trust, results in erroneous trust values. The suggested paradigm reduces links with malicious nodes, saving node energy.

**6. References:**

[1] Hosseinzadeh, M., Mohammed, A. H., Alenizi, F. A., Malik, M. H., Yousefpoor, E., Yousefpoor, M. S.,& Tightiz, L., A Novel Fuzzy Trust based Secure Routing Scheme in Flying Ad Hoc Networks, Vehicular Communications, 100665, 2023.

[2] Wang, Z., Tian, L., Lin, L., Xie, J., Wu, W., & Tong, Y., Data Collection System of IoT Based on the Coordination of Drones and Unmanned Surface Vehicle. Journal of Advanced Transportation, 2023.

[3] Liu, Y., Xie, J., Xing, C., & Xie, S., Topology construction and topology adjustment in flying Ad hoc networks for relay transmission. Computer Networks, 228, 109753, 2023.

[4] Ye, Z., Wang, K., Chen, Y., Jiang, X., & Song, G., Multi-UAV navigation for partially observable communication coverage by graph reinforcement learning. IEEE Transactions on Mobile Computing, 2022.

[5] Tsao, K. Y., Girdler, T., & Vassilakis, V. G., A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. Ad Hoc Networks, 133, 102894, 2022.

[6] Messaoudi, K., Oubbati, O. S., Rachedi, A., Lakas, A., Bendouma, T., & Chaib, N., A survey of UAV-based data collection: Challenges, solutions and future perspectives. Journal of Network and Computer Applications, 103670, 2023.

[7] Tlili, F., Fourati, L. C., Ayed, S., & Ouni, B., Investigation on vulnerabilities, threats and attacks prohibiting UAVs charging and depleting UAVs batteries: Assessments & countermeasures, Ad Hoc Networks, 129, 102805, 2022.

[8] Singh, K., & Verma, A. K., TBCS: A trust based clustering scheme for secure communication in flying ad-hoc networks. Wireless Personal Communications, 114, 3173-3196, 2020.

[9] Barka, E., Kerrache, C. A., Lagraa, N., Lakas, A., Calafate, C. T., & Cano, J. C., UNION: A trust model distinguishing intentional and UNIntentional misbehaviour in inter-UAV communicatiON. Journal of Advanced Transportation, 2018.

[10] Ganesan, R., Raajini, X. M., Nayyar, A., Sanjeevikumar, P., Hossain, E., & Ertas, A. H., Bold: Bio-inspired optimized leader election for multiple drones. Sensors, 20(11), 3134, 2020.

[11] Du, X., Li, Y., Zhou, S., & Zhou, Y., ATS-LIA: A lightweight mutual authentication based on adaptive trust strategy in flying ad-hoc networks, Peer-to-peer Networking and Applications, 15(4), 1979-1993, 2022.

[12] Bhardwaj, V., Kaur, N., Vashisht, S., & Jain, S., SecRIP: Secure and reliable intercluster routing protocol for efficient data transmission in flying ad hoc networks. Transactions on Emerging Telecommunications Technologies, 32(6), e4068, 2021.