IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 21 May 2024, accepted 12 June 2024, date of publication 27 June 2024, date of current version 26 July 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3419904

SURVEY

Trust-Based Flying Ad Hoc Network: A Survey

JOYDEEP KUNDU[1,2], SAHABUL ALAM[1], JADAV CHANDRA DAS[3], ARINDAM DEY[4], AND DEBASHIS DE[2], (Senior Member, IEEE)

[1]Department of Computer Science and Engineering, Brainware University, Barasat, Kolkata, West Bengal 700125, India
[2]Department of Computer Science and Engineering, Maulana Abul Kalam Azad University of Technology, West Bengal, Simhat, Nadia 741249, India
[3]Department of Information Technology, Maulana Abul Kalam Azad University of Technology, West Bengal, Simhat, Nadia 741249, India
[4]School of Computer Science and Engineering, VIT-AP University, Amaravati, Andhra Pradesh 522237, India

Corresponding author: Arindam Dey (arindam84nit@gmail.com)

This work was supported by Vellore Institute of Technology-Andhra Pradesh (AP) University, Amaravati, Andhra Pradesh, India.

ABSTRACT An efficient data transmission can be established by flying ad hoc networks (FANETs) that emphasized the cooperation and coordination among various unmanned aerial vehicles (UAVs) as a crucial aspect. The FANET's security becomes a crucial area for exploration due to its limited resources. Earlier research on trust-based computation in ad-hoc environments has demonstrated that previous strategies are efficient at safeguarding ad-hoc environments against a wide range of attacks. So, to curb such circumstances, trust-based management systems can be considered the major need of the hour for calculating the reputation score within the network. Trust management systems are aimed at detecting untrustworthy network nodes and keeping track of all the activities being performed by the nodes, for trust score computation. This will aid in segregating the malicious node from the network. In this article, several types of trust mechanisms of FANET have been addressed thoroughly, and several types of trust mechanism calculations are clarified primarily with the major challenges that FANET is encountering in the context of its trust management design, open research problems and solutions are being incorporated with the existing FANET-based protocols.

INDEX TERMS FANET, UAV, trust, protocol, energy.

I. INTRODUCTION

A FANET network can be visualized as intercommunicating clusters, consisting of a large number of UAVs that are assigned to execute a particular job. This intercommunication is being implemented wirelessly without any infrastructural support [1], [2], [3], [4], [5]. In a FANET-based network, all the UAVs are pre-programmed per the flight plan to make them autonomous at the time of flying. These UAVs can also be subjected to complex dynamic infrastructure in the context of automation [6], [7], [8], [9], [10]. This complex infrastructure can be termed flexible and versatile at the time of implementation [11], [12]. Eventually, if an ordinary communicating channel (infrastructure-based) becomes out of order or unavailable, then at that instance of time, these cluster-based flying robots (UAVs) can furnish a speedy wireless network to communicate and coordinate with the rescue team.

FANETs can be implemented in various applications like location-aware services, disaster management, security services, and rescue operations [13], [14], [15]. The nodes of a FANET are also freed to make movement irrespective of direction. These aid FANET to complete their assigned job. At the time of completion in accordance to their mobile nature, the topology of the network can change several times. The participating node can get linked or delinked from the network as per the requirement. FANET is also responsible for offering a self-structured and autonomous trend of the node which may result in biases and harmful characteristics in the network to the node [16], [17], [18], [19], [20].

A single node must abide by the norms of coordination from the perspective of the large usage of FANETs. These biases and harmful traits brought attention to the urge to enhance the security of the networks. In this case, the classical methods, from the context of security that includes the technique related to cryptographic methodologies, are responsible for the huge consumption of resources [21], [22], [23], [24], [25]. Hence, securing a FANETs-based network with an optimal resource consumption is becoming a burning agenda for research. Past research is being carried out in the context of trust schemes from the perspective of ad-hoc environments

The associate editor coordinating the review of this manuscript and approving it for publication was Xijun Wang.

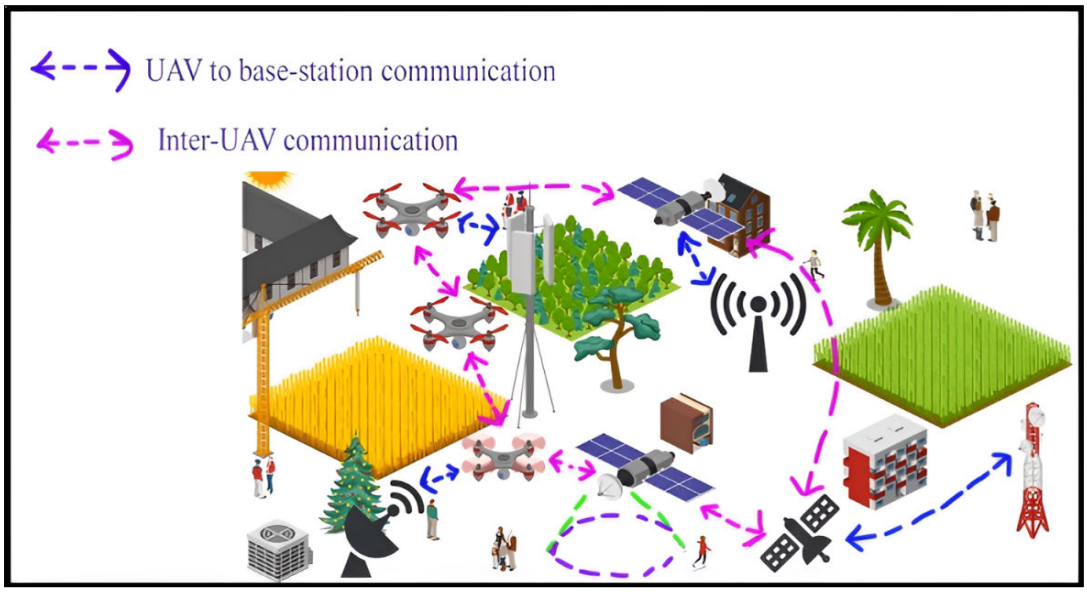

FIGURE 1. Flying Ad-hoc network system.

which signifies that a trust evaluating procedure can be stated to be helpful in terms of securing ad-hoc-based networks from malicious attacks [8], [9], [10]. Hence, for securing a FANET-based network, the ideology of trust management should be incorporated [11], [12]. The trust management system is responsible for maintaining the trust-based relationships in-between the major intermediate nodes. It focuses on multiple prospects regarding trust-based computational methodologies that can also be incorporated within FANETs.

A UAV is essentially a flying ad-hoc network, which primarily connects multiple UAVs to communicate with each other within such a network. FANET is the result of advances in technological perspectives and improvements in infrastructure-less network schemes for integrating automated flight-based units. A key component of such a network is the UAV, which primarily contains 'drones', 'balloons', 'light aircraft', 'ground controllers, etc. FANET's intercommunication architecture assists the end user with two integrated communication methods for UAV control. These methods include inter-UAV communication and communication between the ground station and to UAV shown in Fig. 1. The other classification parameters about the UAV are based on weight, length, principle of operation, and shape of wings. Such capabilities can result in distinguishing traits for UAVs in terms of making themselves familiar with various rescue, search, and any types of emergency crises due to their enhanced scalability and comprehensive height.

Such a device has enhanced their fame to numerous civilian usage, including wind-related research, forest fire detection, agricultural applications, civilian security-based applications, critical traffic examination, and furnishing internet-based services in a disaster-like situation.

FANETs are volatile networks with limited resources and energy, requiring prompt responses for jobs. Communication is crucial in FANET systems, despite challenges like density, topology, energy consumption, radio propagation design, computational power, and mobility. Communication protocols are essential for reliable, resilient, and on-demand communication between UAVs and base stations due to their unique features and complex deployment environment. This review analyzes several trust management techniques in FANETs which focus on trust components, trust building, trust evaluation, and trust propagation stages. It investigates multiple trust management systems and evaluates them based on key factors like security, scalability, dynamicity, and complexity. The survey highlights the need for innovating methods to improve the routing, security, and quality of service (QoS) of FANETs. It outlines research gaps in areas including different trust calculation techniques and parameters, trust evaluation approaches, and trust-based schemes in FANETs. The mathematical computational strategies for trust and parametric-based simulation analysis are also explored in this article. It also covers QoS in trust-based FANETs, which cover cooperative routing, dependable data transfer and resource distribution, etc. Lastly, the survey identifies issues and discusses open research challenges, including potential solutions like node mobility, resource availability etc.

The article consists of ten sections. Trust based communication mechanisms have been described in section II. In Section III, an analysis of the knowledge gap has been discussed. Communication protocols for FANETs have been discussed in Section IV. Trust computational mechanism in FANET has been introduced along with its different methodology in section V. An extensive review of the trust-based FANET routing protocol on the bases of different parameters has been analyzed in section VI. The overall discussion about the various types of FANET-based trust routing protocols and open research trends are summarized in sections VII & VIII respectively. Research challenges are in section IX. Lastly, section X concludes the paper.

II. TRUST-BASED COMMUNICATION AMONG THE UAVS

Assuming that numerous UAV networks interacting among themselves are being accomplished entirely based on the well-endowed framework, as a result, that particular satellite or terrestrial station will be capable of having a functional province that is inaccessible throughout the communicative coverage of the framework. In the event of ineffective inter-UAV interaction with the foundation, the implementation may fall flat [26], [27], [28], [29], [30], [31], [32], [33], [34], [35].

Trust development between the transmitting UAVs and electing the most reliable UAV (the leader UAV) with a significant chance of data retention and adequate energy for the remainder of the operation. An additional objective is to make use of the chosen monitor to get around any broadcast storm problems that may arise from interest packet distribution. The data packet is transferred back to the requester UAV using the quickest and most reliable way when the data generator or a node with a duplicate of the demanded information (i.e. data) is identified as being used. This type of authentication mechanism is then executed based on how reliable the data producer is. Fig. 2 [34] has explained a compact data authentication mechanism focused on inter-trustor to present the stated inter-UAV trust formation and administration data authentication mechanism focused on inter-trustor to present the stated inter-UAV trust formation and administration. However, the flying network system is the methodology of inter UAVs message conveyance rather than UAV-base station data conveyance. Perhaps, it may be utilized to elongate the coverage of the complete range of execution. However, a FANET node may not be utilized to demonstrate a communication connection with the configuration, yet can still be employed to advance under communication via individual UAVs. The foremost intention of the cluster-based FANETs is to establish a trust-based prototype. The methodology of the prototype may be used to minimize the achievable requirements of the disadvantageous or ill-disciplined nodes that are being nominated as an intermediate node. A node surrounded by a collected FANET miniature can be conveniently recognized as a Cluster Head (CH) or a Cluster Member (CM). Members of a collection can straightforwardly intercommunicate with their CH. CH can uncomplicatedly transfer the discriminative data to the primary base station via other CHs. It is believed that every single node is systematized among the group with the assistance of a recommended grouping program [10], [20]. It is furthermore presumed that every node has an exceptional distinctiveness, which is indistinguishable from the presumptions. In numerous sensor-based networking replicas, nodes do not acquire an exceptional individuality identical to the internet-based propriety of conventional networks. Although, to individually recognize the particular nodes one must execute an inter-communication for the particular ambiances, a class-based emphasizing proposed action [36], [37], [38], [39] is being utilized. A protected transmission medium is being inaugurated to defend the rust score from obstruction origination or inspection at the moment of relocation from one node to an alternative one accompanied by the guidance of fundamental administration strategies [40], [41], [42], [43], [44], [45], [46], [47], [48], [49]. Furthermore presumed that every node has an exceptional distinctiveness, which is indistinguishable from the presumptions. In numerous sensor-based networking replicas, nodes do not acquire an exceptional individuality identical to the internet-based propriety of conventional networks. circumstance regarding the network malleability, is the ranking-based decorum. Currently, the network embodies a certain proportion of clusters from distinguishable ground provinces. Every single cluster has its corresponding cluster head, and every single node inside the cluster is conveyed by a direct route in the radius of the leader node. The leader is affiliated with the UAVs in conditions of characterizing the whole cluster. Furthermore, the leader node is similarly responsible for propagating data during the time of transmitting together with its cluster associates. This miniature can satisfy a superior presentation regarding the consequences when the objective region is enormous and the proportion of UAVs is more prominent as well. Amongst the most pivotal design-based circumstances for categorized routing is necessitated with cluster configuration Motility augury aggregating is inherently a cluster configuration algorithm in particular that is being designed for FANET [20]. It immensely adaptable FANET node can evolve in a recurring cluster advancement, and the Motility augury clustering also deliberates in deciphering this hindrance by consolidating the foretelling-based network computational refurbishment. It foretells the movable configurations of UAVs with the assistance of a dictionary Tree-configuration foretelling algorithm [28] and associates termination time movability strategy. It acquires a discriminatory accumulation of every miniature and the UAV, especially having the utmost prominence to each of its adjacent UAVs, is being designated as the leader. The complete simulation studies advance the notion that the leader node determination approach can amplify the invariability of the groups and the CHs.

The existence of an aerial ad hoc-based infrastructure demonstrates an equivalent relationship as a means for assisting Cooperation and Association amongst the UAVs.

Over and beyond, it is observed in most of the events that FANET is accountable for data accumulation from its circumstances and relies on the instructions being handled by the management headquarters. FANET can homogenize peer-to-peer relationship mediums and must also be responsible for gathering the congestion at that present time. Multi-UAV processes may assimilate a diverse category of radars, in which each radar may be accountable for various propositions in the phenomenon of data consignment. Interaction-based technologies are the most crucial design aspects when they deal with multiple UAVs in FANET. Ad-hoc connections among UAVs are examined in this work as a specific kind of network called Flying Ad-hoc Network.

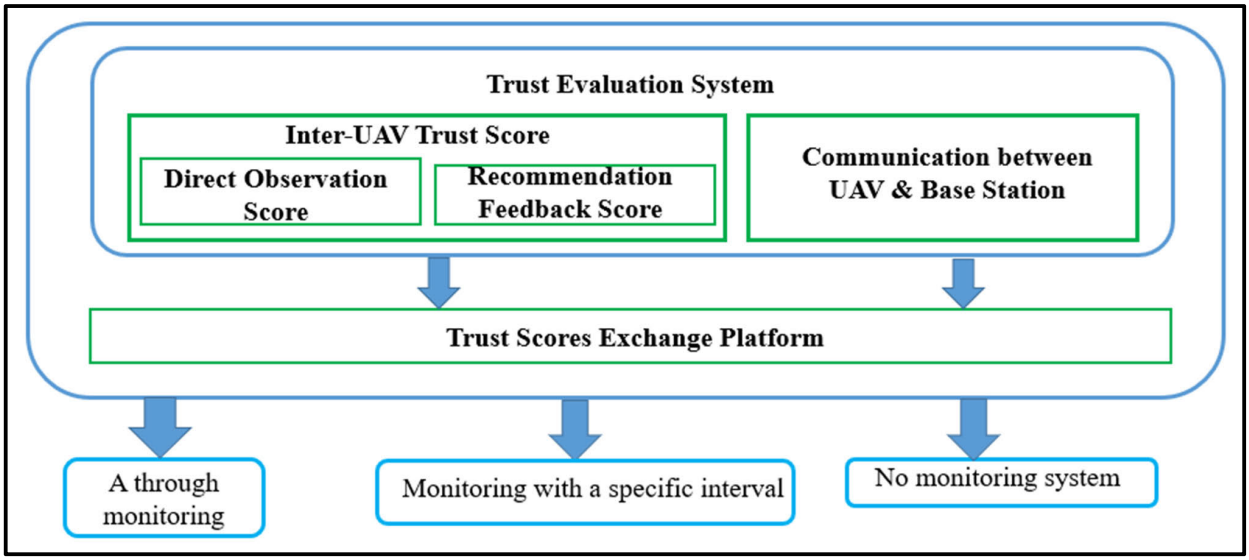

FIGURE 2. Trust based inter UAV data communication system.

This type of network application has been discussed, along with the FANET concept regarding the density of the UAVs, scalability, topological modification, power efficiency, processing power, localization and the differences between flying ad-hoc networks along with the other traditional types of ad hoc network have also been explored. FANET technology factors such as adjustability, sustainability, response time, UAV platform restrictions, and bandwidth are also examined. A thorough analysis of current data on FANETs has been surveyed and associated topics using a layered architecture. The presently used FANET simulation environments along with simulators are explored also. The main objectives of such a paper are to outline the multiple UAV ad-hoc system difficulty and also to inspire further experts to concentrate on such obstacles that are yet unsettled. The primary objectives of this research are to introduce distinct obstacles and design restrictions for FANET and define it as a unique dynamic network category. This is the initial in-depth evaluation of trust-based FANETs, despite the existence of different types of mechanisms that address some particular concerns of multi-UAV technologies along with the open research trends [50], [51], [52], [53], [54], [55], [56], [57], [58], [59], [60].

III. ANALYSIS OF THE RESEARCH GAP

The selected review articles covered a variety of features, such as the fundamental ideas of different trust-based models, communication protocols, trust assessment systems, and trust-based computing techniques by employing mathematical operations and simulation methods.

Communication plays a significant role in designing the inter UAVs protocol system. A survey has been done on trust-based UAV-connected flying ad-hoc networks. The amount of trust can be explained in the context of FANET and its present application scenarios. It has also been discussed the different types of trust management schemes i.e. mobility, topology change, density of the UAV, transmission radio, residual energy, power consumption of drone, and distance [61], [62], [63], [64], [65], [66], [67], [68], [69], [70], [71], [72], [73], [74], [75], [76], [77], [78], [79], [80].

UAVouch [52] developed a scheme that combines movement plausibility tests for UAV groups with public-key-based authentication to validate identity and position. It supplied the authentication technique by regularly confirming that the locations of neighbouring UAVs make sense. The invaders that are unable to follow projected trajectories were also detected.

This kind of network design is affected by several factors in terms of adaptability, latency, scalability, UAV platform constraints, and bandwidth. The comparison of different features of the existing schemes has been described in Table 1. Furthermore, it has been discussed the issues of the research gaps regarding such kinds of networks with their various computation technique in Table 2.

IV. COMMUNICATION PROTOCOLS FOR FANETS

FANET can provide a network system that is disposable, portable, and self-composable with comparatively low operating costs. In case of turbulence, the normal communication infrastructure is unavailable. On the contrary, communication between UAVs in ad-hoc mode becomes a salient task. Numerous ad-hoc routing protocols have been designed to establish reliable and efficient communication between FANET nodes. The motivation is to provide a thorough overview of existing communication protocols.

Communication network among UAVs is one of the hardest configuration issues. Communication among UAVs upon FANET can operate on motility, node density, alteration in geography, radio propagation miniature, energy utilization, computational energy, and pinpoint. Because of this uniqueness and the compound implementation environment of FANET, communication procedures perform a crucial part

TABLE 1. Comparison of features with different existing techniques.

Existing schemes	Scope	Core findings	Advantages	Disadvantages
TBCS [53]	To increase efficiency and security by dynamically choosing the leader drone.	hybrid trust evaluation score with indirect and direct interactions.	Increase the accuracy of identifying and isolating non-cooperative nodes.	High energy consumption.
UNION[54]	To identify and separate non-cooperative UAVs.	Trust establishment via interaction.	Lightweight inter-UAV trust score evaluation.	Unable to protect against unapproved drones.
SECRIP[56]	To protect the UAVs while they are transmitting data along the routes.	To provide a secure route during transmission based on bio-inspired algorithms	Improves the network's longevity, mobility of drones and signal reception strength.	Unable to secure the transmitted data.
UAVouch[52]	Detection of malicious drones.	Authentication and position validation.	To find odd activity, anomaly detection methods were also used.	Unable to provide UAVouch position validation technique.
BOLD[55]	To provide dynamic cluster leader selection	To select the cluster head among several drones at different times.	Decreasing the energy required for communication, thereby increasing the lifespan of the network.	Unable to consider the high transmission range and frequency during data communication
SEEDRP[59]	To provide a safe, effective, and dynamic routing.	Secure the UAVs based routes from the external attacks during data transmission.	Improve the throughput and packet delivery ratio and delay among the UAVs during transmission	Unable to secure the nodes along with the trajectories during communication.
RRPRS[57]	Dependable predictive routing scheme.	Robust and dependable predictive route selection scheme	Enhanced the active-path lifespan.	Unable to provide efficient implementation and functioning in practical situations.

in incorporating trustworthy and strong communication and expanding strategy expertise by strengthening connectivity among UAVs.

Nodes in Flying Ad-Hoc Network (FANET) ways and means are extremely adjustable, crucially expandable, extendable, esteemed, and concurrent peer-to-peer communication between UAVs and terrestrial stations. experimentation matters are stated for the different layers as illustrated in Table 3.

V. TRUST EVALUATION MECHANISMS IN FANET

Trust management can be pondered as the creation of a trust, evaluating the value based on their trust, and updating the value of trust score and revocation. The complete elaboration of the f trust computational procedure has been described below.

A. INTRODUCTION OF TRUST

The process of initializing trust is the first step in a trust-based management system because when nodes start interacting, they don't yet have enough information about one another to determine the trust value. Based on this situation, nodes are further categorized into trusted, non-trusted, and undefined. According to record-based communication, as shown in Fig. 3 [30], this value is updated more precisely in the context of trust status.

A schematic diagram of the trust computation method is shown in Fig. 4 [30] for a fuzzy logic-based trust evaluation model i.e. TBCS [53]. This fuzzy classification scheme can be able to segregate the drones within such a network. Several components have been shown in the fuzzy-based trust computation scheme for computing a drone's trust value within such a network. This scheme has provided services in terms of quality and social parameters. The quality of service parameters includes performance along with reliability. The drone's experience can be achieved from the social environment and also performance can be obtained from the drone's quality parameter. This scheme divides the classes of drones into three categories i.e. best, worst, and moderate based on their performance. It can be able to form clusters with suitable drones and select the most trusted drones as cluster heads within such networks. The drone within the cluster can calculate the trust values of all neighborhood drones based on this methodology. Whenever an unknown drone outside the network wants to meet with such network first sends a joining request message to the leader drone which takes the responsibility in terms of acceptance.

TABLE 2. Research gaps based on previously published articles for trust Based FANET.

Trust Computation Method	Research gaps
TBCS [53]	• It has a shortcoming in the high consumption of energy without having a proper solution to fix that. • It has failed in the respect of selecting the optimal leader drone at different geographical hindrances dynamically with respect to both high and low ranges of transmission.
UNION[54]	• This Model is unable to provide full security from the unauthorized drones
SEEDRP[59]	• It does not provide a trustworthy route or path for the drones when communicating data. • This plan failed to invent a remedy for the broadcast storm difficulty during the interest diffusion.
Fuzzy based FANET [64]	• It is incapable to mitigate incomplete information concerning uncertainty in dynamic soundings. • Expert knowledge of the inclusion aids in enhancing the fuzzy based application scheme for FANETs. • Fuzzy logic-based trust models in the current scenario are termed to be highly dynamic, scalable along with less complex, and enhanced security.
BOLD[55]	• This scheme proposed to select a drone(leader/head) operator from the cluster-based FANET by an optimization scheme (nature-based). • The computational model of the BOLD algorithm is based on the natural optimization process. • Stimulation was performed considering the three-dimensional state (width, length, height) of the UAV instead of the two-dimensional state.
ATS-LIA [66]	• This smart and efficient optimization technique can be used to deal with different types of uncertain real-time problems. • It contains three types of variants and also focuses on hybrid versions. • Additionally, results of applications using this algorithm in applied science are provided in the areas of image processing, machine learning, networking, etc.
LOR-FANET[67]	• Geocasting allows delivering of information to a subset of targets on the network determined by nodes' geographic location. • It is also known as Location Aware Routing. Messages are distributed to nodes within a geographic position within such a network. • It uses several routing methods based on flooding, non-flooding, beaconing, forwarding, etc. Location-aware routing is primarily focused on energy usage and genuine message delivery and also works on multi-dimensional topologies of the network. • Evaluation of geocast routing protocols includes message and storage complexity, robustness, and the ability to forward geocast packets over evenly localize networks.
NDN-VANET [68]	• This protocol is aimed at improving the security of NDN-driven VANETs (VNDN). • The selected cluster heads are then in charge of disseminating interest packets to protect from the situations like broadcasting storms among the intermediate problem. • When the destination has been located, the data is returned to its sender most quickly and securely possible. • As a result, the calculation complexity and time are reduced.
LAKAS-IoD[76]	• The algorithm starts by obtaining the location of the starting node, inter-network link node, and sink based on the positional monitoring system. • Attempt count points to the route development procedure that demands at least two nodes to utilize the first route. • The convey management pattern is accountable for the individual dynamic routing method while AES with distinct dynamic key watches out for shielding the packets before conveyance.
BWOA [70]	• 'Whale optimization Algorithm' computes the reliability score based on the fitness scores of the multiple routes within such a system. • The whole mechanism incorporated in such kind of bio-inspired algorithm is listed below: i) Evaluate the trust scores along with the benchmark i.e., distance for each drone within such system; ii) Establishment of kth disjoint route; iii) Computing the most desirable route based on its trust score about the distance within such a system. Applying parameters, power, frequency, and packet distribution proportion, the representation of the trust-based 'Whale optimization Algorithm' is assessed.

TABLE 2. *(Continued.)* **Research gaps based on previously published articles for trust Based FANET.**

LCBSI[71]	• A fusion technique of communication framework that makes use of both the low energy necessity of 802.15.1 and the high data rate abilities of 802.11. • Improves network throughput and delay efficiency. • In addition, the proposed scheme significantly reduces the cost of communication, and simulation results employing OPNET seconds illustrate the effectiveness of the strategy. • A fusion wireless communication technology that enhances the network representation in terms of frequency and latency by integrating the low energy usage of 802.15.1 with the huge data transfer proportion of 802.11. Further, the proposed program significantly reduces communication expenses, and a simulation outcome utilizing OPNET confirms the efficiency of the approach.
MBMP[72]	• Network performance will be reduced by increasing the no. of UAVs due to the problem of broadcasting storms with the network. • This problem can be solved by an algorithm based on the selection of neighbors dynamically. • It was modified and validated based on field experiments and computer simulations. • When the message redundancy falls significantly, then message delivery will be increased to flooding scenarios, FANET can alleviate the real-world problem of broadcast storms. • This allows traditional broadcasting storm traffic techniques to be used in FANET.
OCOSCD[63]	• This system can be able to use the computational power from the other cluster for the drone of another cluster to operate a specific task. • If a drone having multiple computational activities within a cluster co-exists with another cluster that has sufficient compute resources within range or is dormant, the proposed scheme would consider switching off the cluster head opportunistically to decide whether to load or not.

TABLE 3. **Analysis of various layers of FANET.**

Name of the Layers	Subjects with respect of analysis implementation
Physical	• In a real FANET-based entreaty, nodes are three-dimensional structures. • Few presiding research materials presume that space is a 2D-based FANET topology. • Previous FANET-based investigations showcased that the antenna characteristics of 3D networks differ from those of 2D-based networks and can primarily affect the physical layer. • Process-oriented inspection of subsisting these layers and enlargement of such layer designs for 3-dimensional networks. This topic in FANET is to be explored further.
Medium access control	• FANET has some distinctive challenges and some enhancements to how the MAC layer is designed. • Energy is one of the key factors connected with peripheral conditions in most ad-hoc-based designs. However, the FANET protocol must act on UAVs, and UAVs have no real power limit. • FANET nodes may comprise and function with additional innovative hardware than a node with the ad-hoc based protocol. This possibility can also be utilized for demonstrating a more systematic FANET-MAC layer.
Network-based	• Peer-to-peer intercommunication is indispensable for multi-UAV system collaboration and collision avoidance. • This kind of network can be formed by gathering information from the environment i.e. an ad-hoc-based network generating a variety of traffic patterns. • All the data is transferred to a predefined number of UAVs directly attached to the network configuration. • Enhancing new routing protocols that assist the end-to-end communication and assemble cast conveyance which has not been explored yet.
Cross-layer architectures	• This productive technique can meet the requirements of FANETs as with different types of supremely dynamic wireless networks. • Despite some research on cross-layer FANETs, is wide open to new protocols. • Communications between layers can be used to upgrade FANET performance. • The quality of link status associated with the physical layer plays an important parameter for further upper layers.

B. DIRECT OR INDIRECT COOPERATION OF TRUST

The second stage in the context of managing the trust can be pondered to be the gathering of evidence. Evidence can be classified in the context of collection that may include indirectly or directly. Direct evidence is the evidence that is gathered with the help of the direct observation method

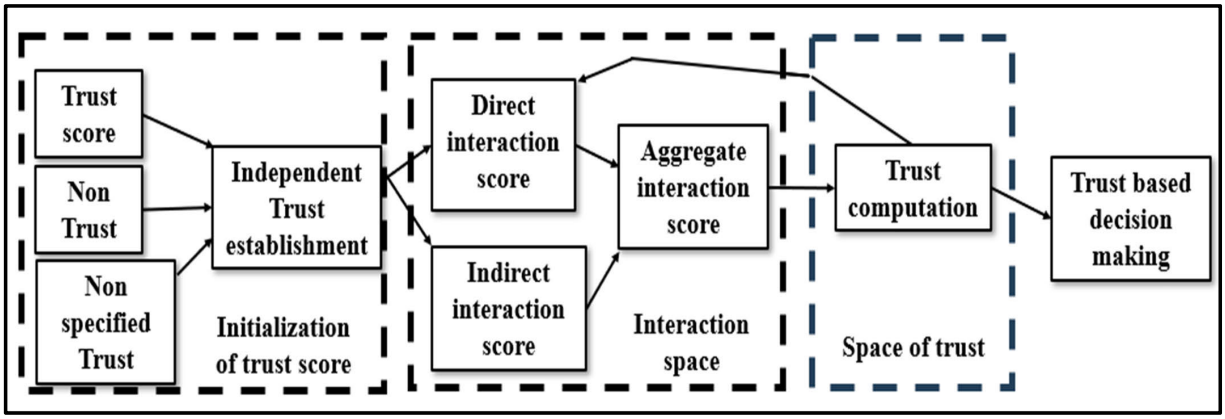

FIGURE 3. Mechanism of trust evaluation scheme in FANET.

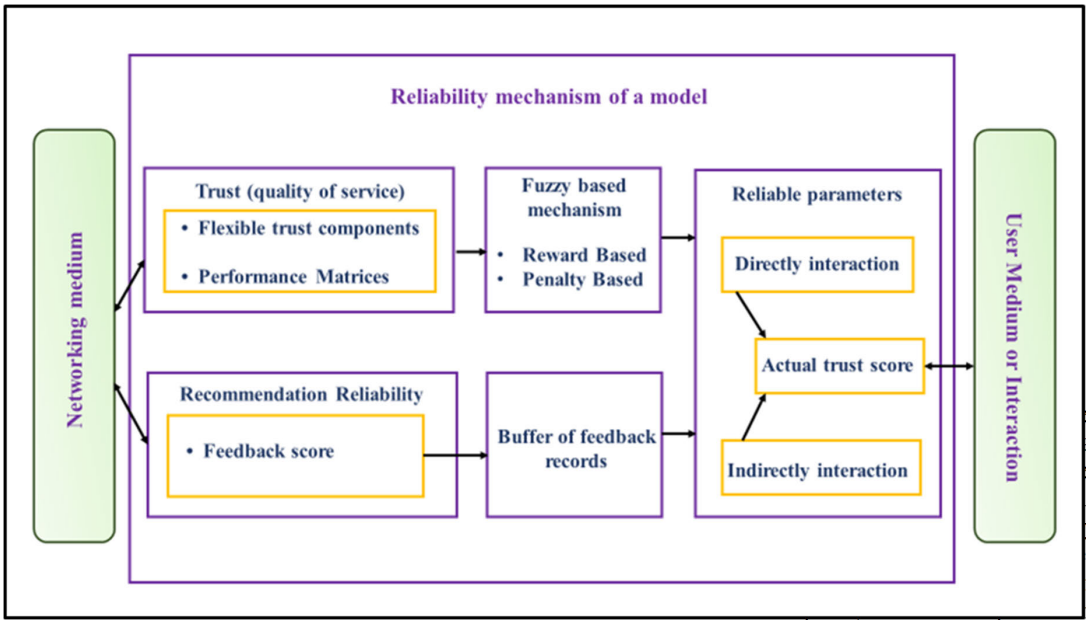

FIGURE 4. UAV based trust establishment scheme communication system.

processed on directly connected UAVs. Evidence obtained from other people's observations is referred to as indirect evidence [19]. Trust values are being reassessed based on this direct and recommendation evidence which may be the cause of an increase or reduction in trust values. Nodes are further categorized as trusted or untrusted based on this result.

C. DYNAMIC NATURE OF TRUST

In infrastructure-less UAVs connected networks, trustworthiness is a factor that is being calculated in the aspect of an individual drone because there is the absence of a base/ground station to compute the trust score for such kind of network. Different formats can be used to express the trust factor. For instance, a vector-based representation that shows the interaction at any point is based on agent, window time, subject, job or action, and consequence [20]. It shows that the topic is being considered in a manner that the agent interprets as to whether the action was successful or unsuccessful at a particular point in time. Another method for expressing the positive feedback, k, and negative number, n, that a subject thinks about an agent is t [subject, agent, action, k, n] [23]. An individual node that is based on the trust score that is computed with the aid of the evidence space incorporates a mapping from an evidence-based space to a trust-based space. It can also be done using a beta distribution [21].

D. BENEFITS OF TRUST IN TERMS OF APPLICATION

In a trust management entity, the decision relies upon the kind of communication channel being used in-between the nodes. A sum of trustworthy nodes is being updated based on the outcome that is being calculated from the earlier phases. The decision-making procedure can be used to classify the nodes in the context of trustworthiness or non-trustworthiness based on the value of the trust score.

E. TRUST MECHANISM STEPS IN FANET

In FANET, a trust evaluation entity involves multiple numbers of segments. These segments have been further categorized into multiple groups according to their

usage. In accordance with the literature used, the classification of trust computation is being processed in five different stages from the aspect of dimensionality which can be trust formation, trust composition, trust propagation, trust calculation, and trust modernization. Fig. 5 [30] depicts various stages that are involved in trust-based management.

1) ***TRUST LAYOUT IN FANET:*** Trust composition refers to the constituents that are being pondered for a trust-based evaluation; it might consist of social and environmental trust and trust based on service excellence.
   - **Quality of service-based trust:** In FANET, this kind of [22] trust refers to the execution of UAVs within the networks based on node reliability, node competence, task performance, and cooperativeness among multiple UAVs.
   - **Social environmental trust:** The social trust [23] factor in FANET can be evaluated based on the social relationship of multiple UAVs. The social relationship factors of UAVs within the FANET are as follows, i.e., good cooperation, data privacy, non-cooperative.
2) ***ESTABLISHMENT OF TRUST:*** Trust formation implies the procedure for identifying the trust score values within a node of a network. There are two factors (observation as well as property) on which trust formation depends in the FANET network.
   - **Experienced-based trust score:** Three methods are available for a node to determine the trustworthiness of another node in the network: Direct, Recommendation, and Hybrid [24]. A trustor node monitors another node's characteristics during their interaction under direct observation. When a trustee node communicates with the other nodes in such a network, a trustor node is tasked with watching the trustee node's trail in indirect observation. According to the suggestion, the trustor node has access to a variety of data about the trustee node from other nodes in the network.
   - **Hierarchy-based trust score:** The trust factor of network drones can be evaluated based on some distinct features that can be partitioned into two classes: multi-trust and single-trust [25]. Single trust refers to the ideology that only one trust-based property can be pondered to compute the trust score about a particular UAV, whereas multi-UAV trust depicts that multiple trusted properties can be used for evaluating trust values about the UAVs in FANET.
3) ***TRUST COMPUTATION PROCESS:*** The process by which a network node's total trust score is calculated is referred to as trust computation. Trust accumulation and prediction procedures are the two methods primarily utilized to calculate a node's trust score within an ad-hoc network.
   - **Trust forecasting:** Trust prediction is a technique for predicting the trust score within a node by examining the past and present characteristics of nodes inside the network. The trust score is predicted using the trust-based prediction algorithm, which considers suggestions from other nodes. Models are used to implement mathematical induction-based models [26], Markov chain models [27], and fuzzy logic-based prediction techniques.
   - **Total trust:** Trust aggregation is another procedure that is being used to compute the trust score at the time when the network-based trust score gets propagated along multiple pathways. So, the aggregation procedure sums up these multi-valued pathways to procure a unit of trust score for a drone in such an environment. Literature stating the Bayesian approach, game theory, fuzzy, and the weighted sum is classified as an aggregation trust-based methodology [26], [27], [28].
4) ***ENHANCEMENT OF TRUST SCORE:*** Trust propagation is a trust-based procedure in a network that states how the transmission of nodes is processed within a network. Trust propagation aids in conserving resources by reusing the trust score of a node which will also help in avoiding the issue of recalculation. Two factors are responsible at the time of node trust propagation which include centralized and distributed within a network.
   - **Collective trust:** The distribution of trust in the distributed paradigm can take the form of trusted chaining or recommendations [26]. In the chaining approach, the trust score is transmitted from one node to another which resembles a chain. When making a recommendation, a node shares its trust value with another intermediate node, that either directly or indirectly possesses pertinent information about the node in question.
   - **Consolidate trust:** In centralized trust-based propagation methodology, a node can be pondered as a centralized propagating entity to work as a trust propagating element within the network for all remaining nodes [25].
5) ***MODIFICATION/IMPROVEMENT OF TRUST:*** Trust updating is a process of updating the trust scores at the time of any network alteration. There are two procedures, event-based and time-based, that can be applicable at the time of updating the node's trust within a network.
   - **Based on period:** In the time-based framework [29], trust scores depending on property or observation are being updated by two different methods namely continuous modification and periodic updation.
   - **Based on evidence:** Every time an event is triggered in such a framework, a network node's

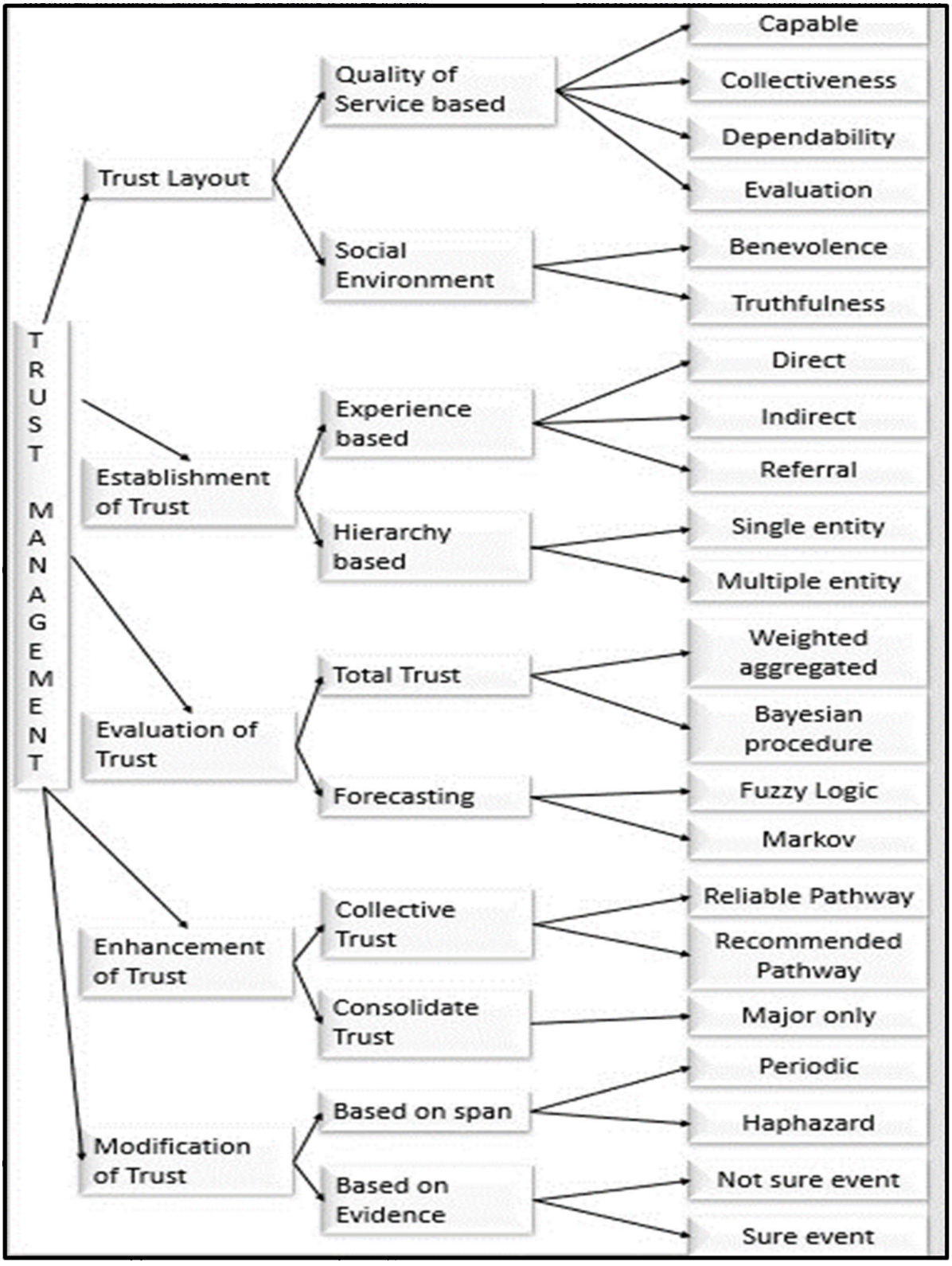

FIGURE 5. Expanding the scalibility of Flying Ad-hoc-based network entity.

trust score is updated [30]. Uncertain events and definite events are the two additional categories that can be used for event-based updation mechanisms. In some event-based methodologies, trust scores are only updated when a particular or predetermined event takes place. The trust scores

TABLE 4. Methodologies of trust evaluation mechanism.

Trust Computation Method	Advantages	Context	Attacks considered	Trust models example
Fuzzy model	1. The model can effectively handle any incomplete information because the entire data is being represented over a certain continuous range. 2. Integration of feedback within the fuzzy model aids in achieving an improved result. 3. This model aids in keeping track of previous information. 4. Information from knowledge experts and specialists can be incorporated into it to produce the best results.	The model aids in securing the entire route along with malicious node detection.	Message Modification Black hole, Gray hole, and wormhole.	TBCS [53]
Bayesian technique	1. This model makes us of the past and present traits for computing the trust score. 2. In contrast, the malicious node can also formulate its trust score by furnishing a more truthful rating within a short time frame.	Malicious node, Enforcing secure routing.	Man in the middle attack, DOS, Bad mouthing,	GA based trust[50]
Game Theory	1. Furnishes scheme-based evaluation. 2. Aids in identifying the rational trait of a node. 3. Enforces the property of updating the trust score over a while interval by making use of "dynamic cyber security games".	Malicious node detection.	Gray hole, Spoofing, and black Hole.	GT based trust[74]
Weightage technique	1. Integration of indirect-based and direct-based trust scores, which would aid in constructing a hybrid model. 2. The model can't stand alone as a representation of sophisticated computing.	Aids in segregating malicious nodes.	DOS, black hole and jellyfish, selfish node, link spoofing.	Lightweight based trust[34]
Markov Chain technique	1. Aids in identifying the trait of dynamic nodes. 2. Aids in evaluating the rate of change of agent's trait. 3. The model is also pondering time as its component in order to segregate malicious nodes.	Enhancing the security over the pathway in transmission.	Malicious node, packet dissipation.	Markov Chain technique based trust [78]
Beta Distribution technique	1. Optimal usage of resources by making use of only two parameters. 2. Aids in evaluating the cumulative trust score along different traits. 3. Integration of the beta method and respective properties aids in evaluating the direct trust and recommended trust simultaneously. 4.It is a time-independent model rather it relies on the achieved rating for trust computation.	Misleading nodes.	Misleading nodes, bad-mouthing.	Beta Distribution technique based trust [80]

of network nodes are updated during the time of occurrence in the context of an uncertain scheme, however.

VI. TRUST BASED ROUTING SCHEMES IN FANET

Trust-based management entity generally possesses a wide range of applications from the perspective of distributed systems, e-commerce systems, sensor networks, information technology, and ad-hoc networks. Reputation and trust are being computed by several trust-based computation techniques that may include the Bayesian trust model, fuzzy model, game theory model, and so on. Existing trust evaluation strategies in FANET are explained in Table 4.

A. COMPARISON ANALYSIS OF VARIOUS TRUST-BASED COMPUTATION METHODS IN FANET

The concept of reliability has been perceived to be the principal field for study because it serves as a crucial parameter in terms of security in the case of the FANET network. Researchers have proposed many trustworthy management solutions for maintaining security in moving ad-hoc networks in the current environment. A comprehensive analysis is being processed concerning various state-of-the-art trust management schemes such kinds of networks. This review aids researchers by focusing on the context of the security-based aspect of FANETs. Several types of trust management schemes along with their necessary parameters in FANET are shown in Table 4. The comparison analysis is based on several essential parameters i.e. computation method, scalability, etc., of FANET in Table 5. The analysis of various trust computation schemes is shown in Table 6.

B. ANALYTICAL VIEW OF VARIOUS TRUST COMPUTATION METHODS IN FANET

An agent subjectively anticipated another's future behavior based on their past interactions is known as trust [15]. The phrase ''ability'' is used in another definition by Grandison and Sloman [16] that states, trust is a strong belief in an entity's ability to function consistently, securely, and dependably in a certain setting. Trust is reliant on feedback based on prior encounters, as defined by Mui et al. [15] and generally in computer science. Trust is developed in online systems as well based on prior interactions and experiences. The two categories of trust are direct observation trust and recommendation trust. Direct observation trust value is such a trust score that the user experiences directly while interacting with the system. When there is indirect trust, another user divulges their personal experience which is known as recommended trust. Trust is a crucial component of FANET. The mathematical trust computation method has been listed in Table 7.

C. REVIEW OF SIMULATION TECHNIQUES FOR FANET

Testing is required before actually implementing or deploying any communication system. Therefore, a network simulator has been used before live deployment. Several types of network simulators are available for flying ad-hoc network communication systems. Some are designed primarily for wireless networks, while others are designed for both wired and wireless networks. This study explores a comprehensive overview of simulation techniques used in flying ad-hoc communication systems to enable network and communications professionals to identify suitable simulators such as REAL network simulator, network simulator (NetSim), network simulator-2 & 3 (NS-2 and NS-3), JavaSim (J-Sim), OMNet++, SensorSim etc has shown in Table 8.

VII. DISCUSSION AND ANALYSIS

Various trust computation scheme has been designed by several researchers to mitigate cyber-attacks for a flying ad-hoc based network. Table 2 and Table 3 depict the performance matrix of various schemes i.e., the table 4 also includes domain which will furnish information in the context of security and safety. It can also be observed that Game theory model, Fuzzy logic, and Markov model are the best suitable models for FANETs [81], [82], [83], [84], [85], [86], [87].

It has been observed that Fuzzy based mechanism plays an important role for the uncertain network with insufficient information about the intermediate nodes. Such network system is inherently scalable, resulting in high uncertainty and high risk of information leakage. Fuzzy based scheme can be viewed as an appropriate trust computation model which can be used such highly dynamic environment. Fuzzy based computational models can contain the knowledge of multiple human experts and are useful to deal with unknown situations that may arise during the time of disaster situations in FANET. In network communication, major attacks often occur during the routing process. These attacks include various types such as wormhole attacks, gray-hole attacks, and black-hole attacks. The Fuzzy model has the capability to mitigate these routing attacks effectively.

Bayesian models are considered a type of trust management model that falls under probabilistic models. However, Bayesian models have limitations when it comes to handling the mimicking behavior of malicious nodes in a network. These models primarily focus on past and current behaviors of a node, which means they may not effectively detect a malicious node that has intentionally built a negative reputation before launching an attack. Additionally, trust decay based on current traits is often slow in Bayesian models. Therefore, these models may not be suitable or justified for use in FANETs.

Instead, game theory-based models can be considered to address these limitations. Game theory provides a framework for understanding the strategic behavior of nodes within a network. By employing game theory, it becomes possible to detect nodes that deviate from the expected network behavior. Game theory-based models can also assist in developing strategies and policies to enhance network security. Therefore, using game theory-based models can be a helpful approach for detecting selfish nodes within FANETs.

Markov models utilize stochastic processes to calculate trust scores for UAVs (Unmanned Aerial Vehicles). These

TABLE 5. Analysis of various trust computation methods.

Proposed scheme	Types of Trust Factors	Attacker's types	Parameters considered during the time of Performance measure	Trust computation methods
TBCS [53]	Direct and recommendation trust	Malicious nodes	Transference Delay, Adaptability, Packet drop ratio (PDR)	Takagi–Sugeno–Kang fuzzy inference method
UNION [54]	Inter-UAV trust reliability	Intended and unintended UAV misdeed.	Inter-UAV packet-based delivery scheme, Inter-UAV energy, mobility-based pattern, and enqueued packets, End-to-end delay	New context-aware trust-based computation
BOLD [55]	Fitness score	Malicious cluster leading drone	Distance and left-over energy at distinct time frames	Social media optimization (SMO), which is reliant on how close together the drones are, Bio-inspired optimized leader selection for multiple drones, Two AI-based optimization Scheme, bio-inspired optimization Scheme
SECRIP [56]	Compute the solution for each search element.	Malicious cluster leading drone	Energy utilization levels, The lifespan of the network, node mobility, reception strength of the signal, delay incurred, packet delivery ratio	Chaotic algae algorithm and a dragonfly algorithm
RRPRS [57]	Computation of the expected connection timestamp, a utility module for path selection, directional dissemination with a fresh reformed mechanism	Environmental hindrances, high-speed mobility, and terrain structures	Dynamic angle-based adjustment for transmitting data delivery ratio, Path lifespan and service disruption time	hybrid usage of geo-casting and unicasting based on routing protocol using trajectory and location-based information
TLCS-FANET [34]	Inter-UAV Trust Establishment, Direct Reliability, Inter-Friend Score.	Identification of Malicious UAV	End-to-end delay is aggregate-based engrossed energy.	A novel trust-aware monitor-based communicating architecture
SEEDRP [59]	Efficient Forwarder link, Round Trip Time(RTT), Packet Lifetime	Malicious nodes	Rate of data transmission, speed of the nodes, node direction	Distinct dynamic key generation scheme
OCSEES-FANET [60]	The estimation time of link, Energy of Drone, Drone`s Key Execution, Drone`s Final Significant Weight	Malicious UAV	Packet feedback ratio, hop to hop delay, utilization of energy, throughput, time complexity	Optimization of link-state protocol based on 'Whale optimization' routing protocol.
HCSELD-FANET [61]	Throughput and delay	Malicious nodes	High data transmission rate, low-power consumption	A hybrid wireless communication scheme
BSP-FANET [62]	Computation of messages replication within a destined interval	Malicious UAV	Broadcast storm problem, message redundancy, message delivery ratio	Broadcast storm problem dynamic neighborhood-based algorithm.
OCOS [63]	communication delay, computing delay, estimated time consumed for finishing all tasks	limited battery and computing power	Operating time, response time, elapsed response time, offloading	opportunistic computational offloading system

TABLE 6. Analysis of various trust computation parameters in FANET.

Trust Model	Trust evaluation Method	Scalability of the model	Nature of Dynamicity	Time The complexity of the system	Storage Complexity	Level of Security
TBCS [53]	Fuzzy	Peak Level	Peak Level	Moderate Grade	Peak Level	Moderate Grade
UNION[54]	Game theory	Moderate Grade	Moderate Grade	Moderate Grade	Moderate Grade	Moderate Grade
BOLD[55]	Fuzzy	Moderate Grade	Moderate Grade	Below Average	Below Average	Below Average
SECRIP[56]	Markov Chain	Peak Level	Moderate Grade	Below Average	Moderate Grade	Peak Level
RRPRS[57]	Markov Chain	Peak Level	Moderate Grade	Standard Grade	Moderate Grade	Peak Level
TLCSF [34]	Fuzzy	Moderate Grade	Moderate Grade	Below Average	Moderate Grade	Below Average
SEEDRP[59]	Markov Chain	Peak Level	Peak Level	Moderate Grade	Peak Level	Peak Level
OCSEES [60]	Fuzzy	Moderate Grade	Moderate Grade	Moderate Grade	Below Average	Below Average
HCSELD [61]	Markov Chain	Moderate Grade	Moderate Grade	Moderate Grade	Below Average	Moderate Grade
BSP [62]	Fuzzy	Moderate Grade	Peak Level	Moderate Grade	Below Average	Moderate Grade
OCOSCD [63]	Game theory	Peak Level	Peak Level	Below Average	Below Average	Standard Grade

models are capable of determining the rate at which a node changes its trait, which can help identify deceptive nodes within a network. Consequently, the Markov model appears to be well-suited for application in Future Aerial Network Systems (FANETs). On the other hand, weightage-based models and subjective trust models are relatively straightforward models that may not adequately capture the complexity of FANETs when used in isolation. These models may lack the necessary sophistication to effectively address the unique challenges and dynamics of FANETs. Therefore, relying solely on weightage-based models or subjective trust models is generally not considered suitable for FANETs. In summary, while Markov models offer benefits such as analyzing trait changes and detecting deceptive nodes, weightage-based and subjective trust models alone may not be sufficient for FANETs due to their limited complexity. Integrating various trust management models and combining them with other approaches can lead to more robust trust management solutions for FANETs.

The beta distribution model shares similar issues with Bayesian models as it primarily focuses on trust ratings and does not consider the time component. Consequently, the beta distribution model is not well suited for use in FANETs. Table 3 provides brief comments on the main findings of a review of various trust computation methodologies. One of the observations made is the existence of a research gap after analyzing several trust-based schemes in FANETs. For example, the TBCS [53] fails to incorporate the consideration of energy consumption. It also lacks an optimized approach for dynamically selecting a leader drone in different geographical hindrances, which can result in other drones being disregarded regardless of their transmission range. SEEDRP [59] is mentioned as being incapable of ensuring reliability in terms of both drone and route when communicating data. It is also unsuitable for addressing the broadcast storm issue during interest dissemination. Furthermore, the concept of scanning and protecting sensitive areas from unauthorized drones has not been introduced in SEEDRP. Table 9 likely presents a compilation of the underlying thoughts and concepts related to trust computation models.

Using real-time streaming protocol and multi-processing, the suggested solution dramatically decreases false positives in fuzzy films caused by UAV vibrations. Using ResNet-101, the modified faster Region-Based Convolutional Neural Network (R-CNN) performed better than the base network in detecting tiny flaws [65]. To lessen the load of traffic

TABLE 7. Various trust based mathematical computational techniques for FANET.

Trust management Approach	Trust score Approach	Type(s) of Trust used	Performance framework about the model
TBCS [53]	$Total_c^{final} = aTotal_c^{direct} + bTotal_c^{reputation}$ ……..(1) $Total_c^{direct} = m.n^y$….(2) $Total_c^{reputation} = \frac{1}{x}\sum_{d=1}^{x} Total_{cd}^{reputation}$.(3) The direct trust and recommendation trust factor are conveyed as a and b respectively, where a+b=1, Each node (say node p) calculates direct trust score with respect to its one-hop neighbors by $Total_c^{direct}$ & The drone request for the indirect observation to its neighbor drone (say node c) using $T_c^{reputation}$	Direct observation Trust Indirect recommendation Trust, Hybrid mode of Trust (collection of both the trust)	Signal effectiveness, node's power, packet delivery ratio (PDR) and past interactions about the adjacent node
RRPRS - FANET[57]	$FS(c,d,) = Trust(c,d).LD(c,d)$ $Trust(c,d)$ $= \{\left[\left(1-\frac{1}{\#int+1}\right).DT(c,d)\right]$ $+\left[\frac{1}{\#int+1}.IT(c,d)\right] if No\_GS\ GSE(GS,d)\ Else$ $DT(c,d)\frac{\#S(c,d)}{\#T(c,d)+\#S(c,d)}.(1-\frac{1}{\#S(c,d)+1})$ $FS(c,d)$ and $LD(c,d)$ symbolize the trust estimation of the link duration between these two nodes, respectively $DT(c,d)$ and $IT(c,d)$ are the direct and indirect trust estimation, respectively, calculated by a UAV c regarding another UAV d. Inter-UAV Trust $\frac{1}{\#int+1}$.GS is Ground Stations. Legal (S) and malicious (T) interrelations between two UAVs c and d.	Inter-UAV mode of Trust, Direct observation Trust, Indirect or Recommendation-Based Trust, Ground Station-to-UAV Trust	Non-cooperative node detection ratio, False positive (FP) ratio, Mean end-to-end interval(s), Content consignment ratio (CDR), Energy efficiency (W.s), Generated Overhead
BOLD[55]	The fitness score D_{opt} of individual drone is evaluated by the formula fitness score $D_{opt} = (u.n_{avg}) + ((0.5).v_{energy})$ n_{avg} is the average interval between two drones, v_{energy} is residual energy factor, u is a variable whose value belongs to the range from 0.2 to 0.4, $n_{avg} = \frac{n_1+n_2+n_3+..n_{BS}}{x+1}$, x is the quantity of drones, n_{avg} is the interval between drone along with base station	fitness trust score about the drone	Energy utilization levels, existence of the network, delay encountered, Reception strength of the signal, Node mobility
ATSLIA[66]	$W_{cd}(h) = \frac{1}{1+e^{-(\sum_{u=1}^{x} r_u e_u - r_0)}}$ Here, r_u is weight factor about various types of shared data on the global trust score, r_0 state the threshold value of the trust score about this model and also h states the transition-duration time about the system. Input and output of this function are expressed as individual value of the F_d (error set) and the assessment of the trust score W_{cd} during the time of data transmission from UAV K_c to UAV k_d. $B_{cd}(h) = \frac{1}{x}\sum_{k\varepsilon z_x}^{x} W_{cd}\ W_{kd}$. where, $B_{cd}(h)$ represents the UAV about the quality of its application, W_{cd} states the direct reliability score of UAV K_c to UAV K_k. W_{kd} also represents the direct reliability score of UAV $K_k$to UAV k_d . $L_{cd}(h)$ is the global reliable score of the overall UAV. $L_{cd}(h) = B_{cd}(h-1) + W_{cd}(h) + \sum_{k=1,k\neq c,d}^{x} (B_{cd}.(h-1))$	Local & global trust score about the drone, Energy trust score, Comprehensive trust value	Drone's power, packet delivery of drone's ratio (PDR), Recommendation interactions about the adjacent node

regulation, the Internet of Vehicles (IoV) is separated into fogs, and it suggests a new security authentication system called fog-based identity authentication (FBIA) [42]. The scheme has two levels: one for cars outside the fog and another for everything else. The accuracy and flexibility of the FBIA scheme are superior to existing techniques. A safe elliptic curve cryptography (ECC)-based Internet of drones (IoD) authentication technique was created using FANET in [35]. ProVerif2.03, the random oracle model, and practical illustration were used for verification. The scheme's efficacy and efficiency were demonstrated by its performance evaluation, which qualified it for use in real-world IoD contexts.

A. QUALITY OF SERVICE IN TRUST BASED FANET

Trust can play a key role in enhancing the parameters of quality-of-service (QoS) in a FANET by encouraging

TABLE 8. Analysis of simulation-based trust management schemes in FANET.

Trust management model(scheme)	Parameters used for simulation							
	UAVs number	Type of Traffic	UAVs velocity	UAVs Placement nature	Power Transmission	System Mobility	Area of Transmission	Tools used for Simulator
TBCS [53]	100	CBR	0 - 20m/s	Random	-	Random Waypoint	50-300m	Omnet++
UNION[54]	100	CBR	0 - 30m/s	-	-		250m	NS-2.35 s
BOLD[55]	35	CBR	50–70 mph	-	Residual energy Renergy 11.1 V Transmitter Pack 27.75 Wh Energy squandered Eelec 0.0000005 nJ/bit	-	1 mile	MATLAB 2018a
SECRIP[56]	200	CBR	0 - 50m/s	-	-	Random Waypoint	-	NS2
RRPRS[57]	Not defined	CBR	10-200m/s	-	1000mW	-	-	C++ to perform Monte Carlo simulations
SEEDRP[59]	150	CBR	0 - 50m/s	-	-	Random Waypoint	-	NS3.26

dependability, efficiency, and cooperation among participating UAVs which has shown in Fig. 6. Trust can affect the quality of service (QoS) parameters [50], [51], [52], [53], [54], [55] in FANETs in various ways which has been described below:

1) **Reliable Data Transmission:** Nodes in FANETs can create dependable communication channels thanks to trust. Nodes are more likely to share data reliably and without tampering or unauthorized modifications when they trust one another. The QoS parameters are directly impacted by this reliability. Trust makes sure that data is transmitted reliably, which improves QoS in FANETs. Trust-based FANET can increase the reliability of data transfer by choosing trustworthy data sources, prioritizing trustworthy nodes for packet forwarding, building secure communication channels, identifying and thwarting misbehavior, and implementing trust-aware routing methods.
2) **Collaborative Routing and Resource Allocation:** Collaboration in FANETs is facilitated by node trust, which improves resource allocation and routing decisions. Trustworthy nodes can cooperate to exchange routing data and alter the network topology dynamically to optimize routes. This cooperative method facilitates resource utilization, the identification of efficient routes, and the reduction of traffic. The trust can enhance collaborative routing and resource allocation in FANET by encouraging group decision-making, facilitating trustworthy information exchange, incorporating reputation-based mechanisms, enabling load balancing and optimal resource utilization, and assisting in the detection and mitigation of misbehavior. The FANET's resource allocation and routing are made more effective and efficient by these trust-enhanced techniques.
3) **Congestion Control:** Nodes in FANETs can work together to successfully manage network congestion thanks to trust. Cooperative congestion control strategies are made possible by the ability of trusted nodes to communicate information about their current traffic loads and network circumstances. The nodes can collectively modify their transmission rates, provide priority to important data, and steer clear of busy areas by exchanging this information. The trust-based FANET enhances congestion control by enabling trustworthy information sharing, encouraging cooperative behavior, enabling reputation-based procedures, providing trust-aware routing, and making it easier to identify and isolate problematic nodes. Nodes in FANET can share precise and trustworthy information on the state of their

TABLE 9. Discussion about inherit thoughts about various trust-based models.

Trust Computation Method	Explanation
Fuzzy	The Fuzzy model is useful for FANETs because it can handle • partial information • uncertainty in dynamic contexts • addition of expert knowledge. • highly scalable system
Bayesian	• More continuous processing is needed for Bayesian models, which increases complexity and decreases dynamicity. • The Bayesian models' level of security is decreased by their propensity to mimic attacks
Game theory	• Models in the literature show that these models are quite good at identifying selfish nodes and coming up with straightforward strategies. • Game theory models are appropriate for FANETs because of their high security, scalability, and dynamicity properties.
Markov chain	• Investigating the speed at which a node alters its behavior is made possible by trust assessment using Markov chains. • There is a description of the scalable, dynamic, low-complexity trust management models. • Therefore, Markov models are suitable for FANETs for trust propagation.
Beta distribution	• Beta distribution's security is decreased since it is vulnerable to misleading assaults. • The models that may be found in the literature lack a lot of flexibility and scalability. • Additionally, the computation complexity is too complicated.
Subjective logic	• Subjective logic can deal with ambiguous and partial data about the UAVs.

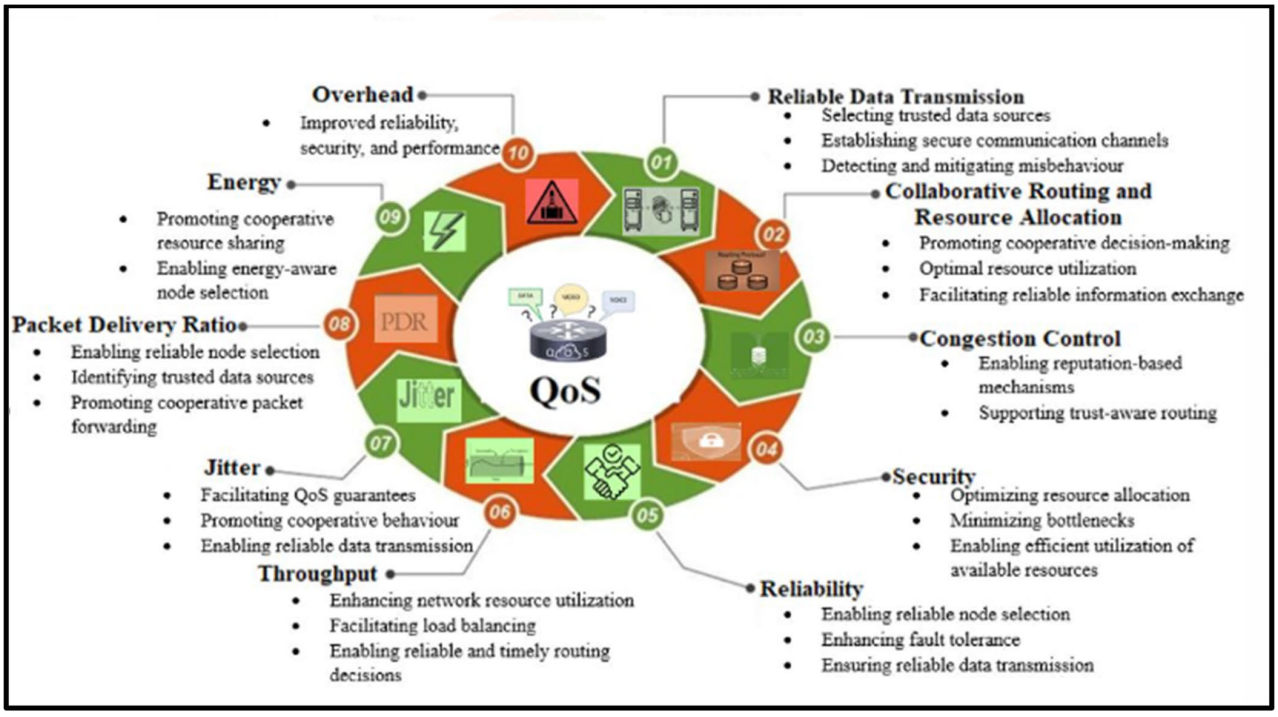

FIGURE 6. Quality of service parameters in trust based FANET.

networks, the volume of traffic, and congestion levels thanks to trust. Other nodes can use this information to make knowledgeable congestion control decisions. In FANET, trust promotes cooperative conduct among nodes. In order to jointly reduce congestion, trusted nodes are more likely to cooperate and coordinate their congestion control strategies, such as modifying their transmission rates or route selections. Reputation-based methods, in which nodes construct and maintain reputations based on their prior actions, can be used to generate trust. A more effective and efficient congestion management system results from nodes with greater reputations since they are more likely to be trusted and their congestion control judgements may

be given more weight. Routing protocols that are cognizant of trust take nodes' level of trust into account. Congestion-aware routes can be created by taking node trust levels into account and avoiding nodes with lower trust that might cause congestion or faulty forwarding.

4) **Security**: In FANETs, the trust is essential for providing safe and dependable resource sharing between nodes. When sharing resources with other nodes, such as bandwidth or processing power, the trustworthy nodes are more likely to do so in a fair and effective way. The overall QoS can be improve by maximizing resource allocation, reducing bottlenecks, and enabling optimal use of available resources, secure resource sharing. Trust enhances security in FANET by enabling secure node selection, facilitating intrusion detection and prevention, identifying reliable data sources, establishing secure communication channels, assisting in the detection and isolation of malicious behavior, and incorporating reputation-based security mechanisms. These trust-enhanced procedures help create a FANET environment that is more secure and robust.
5) **Reliability:**Trust enhances reliability by establishing a sense of dependability and predictability among UAVs in the network. Trusted UAVs are more likely to follow protocols and agreements, minimizing the chances of communication failures or malicious behavior. The network can rely on the participating UAVs to maintain consistent connectivity and uphold their commitments, leading to improved reliability by fostering trust. The trust improves reliability in FANET by enabling reliable node selection, promoting cooperative behavior, ensuring reliable data transmission, enhancing fault tolerance, and incorporating reputation-based reliability mechanisms. These trust-enhanced mechanisms contribute to a more reliable and robust FANET operation.
6) **Throughput:**Trust has an impact on throughput by promoting effective and cooperative behavior among UAVs. UAVs are more likely to cooperate when they trust one another to share network resources, such bandwidth, to increase throughput. Trusted UAVs can use effective routing, dynamic spectrum access, and congestion control techniques to improve network throughput and maximize the use of available resources. Trust can also increase throughput in FANET by maximizing the use of network resources, encouraging cooperative data interchange, enabling accurate and timely routing decisions, facilitating load balancing, and implementing reputation-based resource sharing. Higher throughput and better network performance are a result of these trust-enhanced methods in FANET.
7) **Jitter:**The trust helps to reduce jitter by encouraging dependable and predictable communication between UAVs. Consistent and stable connections are anticipated from reliable UAVs, minimizing changes in packet delivery delays. This communication reliability aids in lowering the variability in delay (jitter), providing smoother real-time data transfer and enhancing the performance of applications that depend on constant delay, such video streaming or remote sensing. Trust can also reduce jitter in FANET by permitting dependable data transmission, encouraging cooperative behavior, facilitating QoS guarantees, including reputation-based path selection, and supporting efficient congestion control. The jitter in FANET is decreased as a result of these trust-enhanced methods' contribution to more predictable and consistent network activity.
8) **Packet Delivery Ratio:**The trust encourages cooperation and wise routing choices among UAVs, which has a good influence on the packet delivery ratio. Even in difficult network settings, trusted UAVs are more likely to cooperate in relaying packets. They can exchange precise and current network state information, choose effective routes, and help forward messages to the right places. The FANET's total packet delivery ratio is improved by this cooperative conduct. The trust increases packet delivery ratio in FANET by enabling reliable node selection, identifying trusted data sources, encouraging cooperative packet forwarding, boosting reliable routing decisions, and assisting in the identification and mitigation of misbehavior. These trust-enhanced procedures let FANET transmit packets more successfully and reliably, which eventually enhances PDR.
9) **Energy:**Trust can improve the energy efficiency of FANETs by encouraging collaboration and resource optimization. In order to conserve energy, trusted UAVs can establish protocols and agreements between themselves, such as coordinated sleep scheduling, adaptive power control, or efficient routing methods. UAVs can reduce energy consumption, extend the life of the network, and prevent node energy imbalances by working together. Trust improves energy efficiency in FANET by promoting cooperative resource sharing, implementing trust-aware routing, enabling energy-aware node selection, encouraging energy-saving behaviours, and leveraging reputation-based energy management. FANET becomes more energy-efficient and uses less energy as a result of these trust-building techniques.
10) **Overhead:**Thetrust can reduce the overhead by enabling effective communication and coordination among the UAVs. Instead of needing frequent route updates and a lot of control signaling, trusted UAVs can rely on the reliable information supplied by other nodes. The network can devote more resources to the actual data transmission, enhancing system performance as a whole and QoS by reducing unnecessary overhead. It has been observed that the advantages of trust in terms of increased dependability, security, and performance frequently surpass the related costs. However, developing trust may add some overhead to

FANET. The impact on FANET operations can be lessened by using scalable and effective trust mechanisms and considering trade-offs between overhead and trust advantages.

The trust in FANETs improves QoS parameters by encouraging dependable data transmission, facilitating cooperative routing and resource allocation, enabling cooperative congestion control, assuring secure and dependable resource sharing, and supporting trust-based service differentiation. FANETs can improve QoS performance and increase the overall effectiveness and dependability of the network by encouraging trust among participating nodes. In conclusion, trust is crucial to raising QoS standards in FANETs. It supports energy efficiency, dependability, throughput enhancement, jitter reduction, packet delivery ratio improvement, and superfluous overhead reduction. FANETs can achieve more dependable and efficient communication, leading to an overall improvement in QoS by establishing trust among participating UAVs.

VIII. OPEN RESEARCH TRENDS

FANETs can be visualized as a dynamic network with constrained resources dependent on energy. The majority of FANET tasks necessitate prompt and precise responses [80], [81], [82], [83], [84], [85], [86], [87]. The security of the current network is essential in such circumstances. Finding a lightweight solution that can indirectly help to meet the majority of the security-related goals is essential for improving the security of FANET-based schemes. One of the simple solutions has been recognized as trust management. The sessional questions will make it easier to investigate if the current trust management solution can be used in the context of FANETs. Based on their contributions to other ad hoc environments, complexity, mobility, security, and scalability. This review article evaluates several existing trust management technologies. It is difficult to choose one strategy as the best; nonetheless, the following unresolved problems and research difficulties must be considered when creating the trust-based solution in FANETs.

FANETs can be visualized in the form of dynamic networks with limited energy-based resources. Most of the tasks in FANETs require timely and accurate responses [88], [89], [90]. In such a situation, the security for the current network, serves to be a crucial aspect. In order to enhance the secure prospect of FANET-based scheme, identification of a lightweight solution is indispensable that would indirectly can aid to achieve most of the security concerned aspects. Trust management has been identified as one of the lightweight solutions. It will make it easier to investigate if the current trust management solution can be used in the context of FANETs. The review article evaluates several existing trust management technologies based on their contributions to other ad hoc networks environments i.e. its complexity, mobility, scalability, dynamicity and security. It is challenging to identify the one optimal method. However, the following open issues and research challenges should be considered when designing the trust management solution in FANETs and are summarized below:

- For future research, the trust score metric should have employed the suitable trust components, such as quality of service and social trust, as well as trust formation strategies, such as drone observation and property base, and trust propagation methods, such as distributed and centralized approaches. Incorporating exceptional security measures may be necessary to obtain the conveyed information.
- It can be expected to empower analysts and specialists to investigate more roads for approaching with further developed UAV remote correspondence frameworks. Existing FANET system(s) essentially depend on straightforward highlight point correspondence over the illegitimate band such as ISM 2.4 GHz. This type of band has a low data transmission rate that works on the restricted reach. The number of drones and its related implementation are ready to cover sooner rather than later. This further pressure the need to foster new half and half plans like 5G, long-term evolution and Worldwide Interoperability for Microwave Access at the backhaul to empower upgraded UAV to base station correspondences.
- In future, researchers can pay attention to secure the drones along with the multiple routes by which the information being communicated. This will allow the FANET system an opportunity to distinguish the malevolent drones from the genuine ones and will help in accomplishing the network objectives of such network completely.
- A trust management system can be improved in further by considering the incorrect information supplied in an recommendation-based manner by an evil intermediate nodes.
- There is a research scope when tasks or processes are changes abruptly for the different purpose based on the scenario to successful data transmission. Consequently, a trust evaluation scheme should be tailored to the objective or job at hand. Performance, security, and reliability requirements for the particular operation or mission should all be supported.

In future, a trust evaluating system should able to evaluate both the trust i.e. individually and group trust within the cluster parallelly. A trust management scheme should address other attacks like message modification, false information forwarding, and rushing.

IX. RESEARCH CHALLENGES

In FANET, achieving the needed security with the fewest faults possible is of utmost importance. It is possible to provide a novel trust-based context-aware approach that can distinguish among both intended and unintended misbehavior in FANETs. Additionally, it selects the best packet forwarders by employing the numerous calculated parameters.

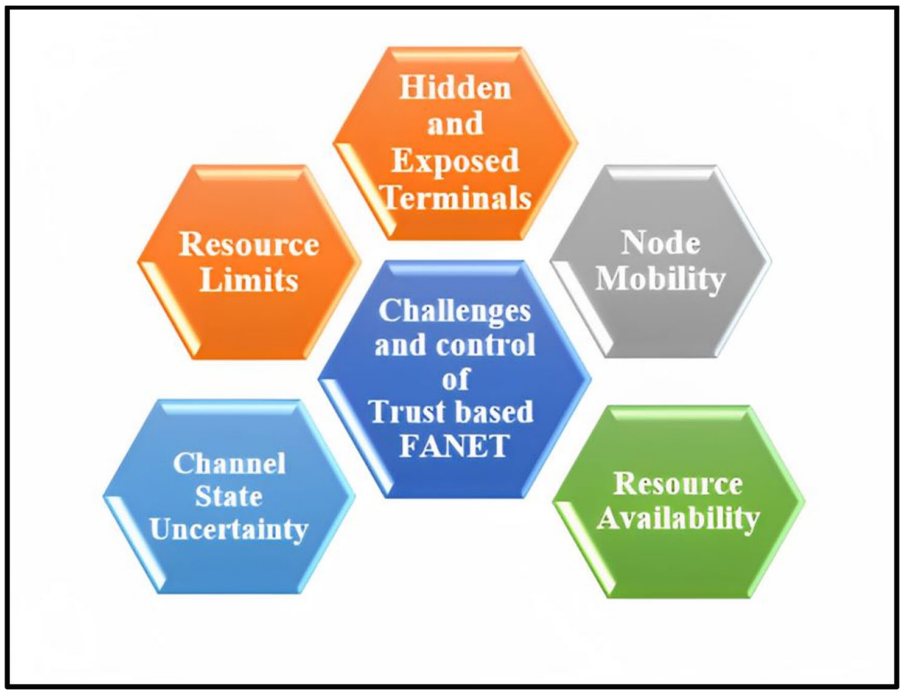

FIGURE 7. Challenges and controls of trust based FANET.

It can provide dependable inter-UAV connections in this way. Without considering the aforementioned three circumstances, it first evaluates the UAVs' trust while simultaneously evaluating their buffer occupation, energy consumption, and motion patterns. The system then generates a final evaluation index called honesty index by introducing a trust correction factor to the inter-UAV trust evaluation that we call trust if it detects that any neighboring UAVs have unintentionally dropped packets. This second one is compared with a predefined detection threshold direct trust below which UAVs are viewed as dishonest. Therefore, A light weight trust aware computational scheme will be developed by evaluating inter-UAV trust score, which can be done, by estimating the recent context of drone's energy, flexible trust score pattern, thereby helps in the overall confirmation about the actual judgment

A. TRUST BASED FANET RESEARCH CHALLENGES SOLUTION

Existing commercial drones are changeable against a few essential security assaults, which may plainly cause between UAV network disturbance with regards to FANETs. In correspondence with the advancement of ineradicable frameworks, these culminated in diminishment of microelectronic-based mechanistic machines or equipment's, which made it achievable to cause inconsiderable sized UAVs at an inexpensive and reasonable expenditure. But in spite of that, from the viewpoint of proficiency, a solitary miniature-based UAV is genuinely near to the ground. Cooperation and association that is being envisioned in the situation of numerous UAVs during the course of designing a methodology, which is nowhere near the pre-eminence of a sole UAV. The crucial privileges of UAVs surrounded by a network can be a linked as stated below:

- **Expenditure/cost-** the expense of framework in the matter of the preservation of a miniature UAV is inferior in contrast to the expense of an oversized UAV.
- **Adaptability**-the utilization of oversized and well-designed. UAVs are accountable for embellishing the compensation adequate for a specific quantity. Despite that, a multi-UAV framework can intensify the procedure from the viewpoint of the adaptability element.
- **Sustainability**-If the UAV seizes up at the instant of fulfilling an enlisted assignment, at the moment the operation will be unsuccessful. But in spite of that, if one way or another an UAV advances in a clone based on multi-UAV configuration, the mission can further bloom at that situation too with adjacent UAVs.
- **Gain Momentum**- It is being perceived that the accomplishment interval for an operation diminishes with the increasing number of UAVs.
- **Small sensor cross-section**- Rather than utilizing a solitary large sensor-based cross-section, a multi-UAV configuration consists of a compact sensor-based cross-section that handles a critical cause in military attributes.

Trust can be used to overcome issues with hidden and exposed terminals, node mobility, resource availability, channel state ambiguity, and resource limitations in a trust-based FANET which is shown in Fig. 7. The following is how trust-based FANETs can address these issues:

- **Challenge 1: Hidden and Exposed Terminals**
  Description- When nodes cannot immediately detect each other's presence or are within each other's

transmission range but are unaware of it, it is said that they are in a hidden or exposed terminal.
Solution- Trust-based FANETs can overcome these difficulties through trust-aware routing and communication protocols. To ease communication between hidden terminals, nodes with established trust relationships can take on the role of mediators or relays. To increase overall connection and lessen the impact of hidden terminals, trust information can be utilized to direct the selection of trustworthy relay nodes.

- **Challenge 2: Node Mobility**
  Description- Routing and resource allocation in FANETs are difficult due to the frequent changes in the network topology caused by node mobility.
  Solution- Trust-based FANETs can use adaptive routing protocols that consider the network topology and nodes' level of trustworthiness. FANETs can dynamically choose routes that are more likely to be dependable and stable despite node mobility by including trust measures in the routing decisions. It may be also used trust-based mobility prediction techniques to foresee node migrations and proactively modify the routing plans.
- **Challenge 3: Resource Availability**
  Description- Resource allocation, and adaptive networking protocols are most challengeable issues for effective drone power management, performance, and network sustainability in FANET. Thus, by taking trustworthiness into account while allocating resources, trust-based FANETs can alleviate the problems associated with resource availability.
  Solution- Access to resources like bandwidth or power may be prioritized for nodes with greater trust ratings. Mechanisms for allocating resources based on trust can maximize resource use and make sure that trusted nodes have access to the resources they require to sustain QoS and dependable communication.
- **Challenge 4: Channel State Uncertainty**
  Description- The channel state in wireless communication can be unpredictable due to elements like interference, fading, and noise.
  Solution- Trust-based FANETs can reduce the effects of channel state uncertainty by using adaptive modulation and coding techniques. As a result, nodes can dynamically modify their transmission characteristics, such as the modulation scheme and coding rate, depending on the dependability of the channel by using trust metrics to evaluate the reliability of communication links. Even in the face of ambiguous channel conditions, this adaptability aids in the maintenance of trustworthy communication.
- **Challenge 5: Resource Limits**
  Description- UAVs in FANETs are constrained by their bandwidth (length), processing capability, and battery. These limitations make it more challengeable to communicate, impede effective energy management, and complicate local processing. Thus, creative solutions are required to optimize the resource use and improve performance.
  Solution- Trust-based FANETs can address resource limits by optimizing resource usage based on trust levels. Nodes with higher trustworthiness can be allocated more resources or given preferential treatment in resource sharing. Additionally, trust-based congestion control mechanisms can regulate the resource usage of nodes to prevent resource exhaustion or unfair resource consumption. FANETs can effectively manage resource limits and ensure fair and efficient resource utilization by considering trust in resource allocation and congestion control.

Trust-based FANETs address issues including hidden and exposed terminals, node mobility, resource availability, channel state uncertainty, and resource restrictions through the integration of trust measures into routing, resource allocation, mobility prediction, and modulation techniques.

FANETs can improve connection, adjust to node mobility, optimize resource allocation, reduce the effects of channel state uncertainty, and assure effective resource utilization in dynamic and resource-constrained contexts through the use of trust mechanism.

X. CONCLUSION

The management of trust inside networks is crucial in defending FANETs against various threats brought on by selfish and unruly nodes. To identify trustworthy nodes and identify malicious and uncooperative nodes in the network, trust management algorithms can be employed to identify the network's malicious and uncooperative nodes. There is a very high likelihood that messages or information will be lost because of the unpredictability and tremendous scalability of these networks. As a result, the implementation of trust-based management systems in FANETs proved to be advantageous and fruitful for the accomplishment of the intended purpose. In this survey, a number of trust management strategies that are already used in conventional flying ad-hoc networks have been examined. It has been found that Markov model-based trust schemes, fuzzy logic, and game theory are the ones that work best for FANETs. These methods give the ability to deal with ambiguity, lack of cooperation, and frequent behavioral changes. The approaches for resolving open research difficulties, such as efficient forwarder links, round trip times, packet lifetimes, link estimation times, drone's key execution times, drone's final substantial weight times, etc., have been thoroughly addressed for upcoming FANET research.

ACKNOWLEDGMENT

The authors would like to thank VIT-AP University, Amaravati, Andhra Pradesh, India, for supporting this work.

REFERENCES

[1] M. Hosseinzadeh, A. H. Mohammed, F. A. Alenizi, M. H. Malik, E. Yousefpoor, M. S. Yousefpoor, O. H. Ahmed, A. M. Rahmani, and L. Tightiz, "A novel fuzzy trust-based secure routing scheme in flying ad hoc networks," *Veh. Commun.*, vol. 44, Dec. 2023, Art. no. 100665.

[2] O. T. Abdulhae, J. S. Mandeep, and M. Islam, "Cluster-based routing protocols for flying ad hoc networks (FANETs)," *IEEE Access*, vol. 10, pp. 32981–33004, 2022.

[3] Y. Liu, J. Xie, C. Xing, and S. Xie, "Topology construction and topology adjustment in flying ad hoc networks for relay transmission," *Comput. Netw.*, vol. 228, Jun. 2023, Art. no. 109753.

[4] Z. Ye, K. Wang, Y. Chen, X. Jiang, and G. Song, "Multi-UAV navigation for partially observable communication coverage by graph reinforcement learning," *IEEE Trans. Mobile Comput.*, vol. 22, no. 7, pp. 4056–4069, Jul. 2023.

[5] K.-Y. Tsao, T. Girdler, and V. G. Vassilakis, "A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks," *Ad Hoc Netw.*, vol. 133, Aug. 2022, Art. no. 102894.

[6] K. Messaoudi, O. S. Oubbati, A. Rachedi, A. Lakas, T. Bendouma, and N. Chaib, "A survey of UAV-based data collection: Challenges, solutions and future perspectives," *J. Netw. Comput. Appl.*, vol. 216, Jul. 2023, Art. no. 103670.

[7] F. Tlili, L. C. Fourati, S. Ayed, and B. Ouni, "Investigation on vulnerabilities, threats and attacks prohibiting UAVs charging and depleting UAVs batteries: Assessments & countermeasures," *Ad Hoc Netw.*, vol. 129, Apr. 2022, Art. no. 102805.

[8] T. Gui, C. Ma, F. Wang, J. Li, and D. E. Wilkins, "A novel cluster-based routing protocol wireless sensor networks using spider monkey optimization," in *Proc. IECON 42nd Annu. Conf. IEEE Ind. Electron. Soc.*, Oct. 2016, pp. 5657–5662.

[9] W. Zhai, L. Liu, Y. Ding, S. Sun, and Y. Gu, "ETD: An efficient time delay attack detection framework for UAV networks," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 2913–2928, 2023.

[10] A. Srivastava and J. Prakash, "Future FANET with application and enabling techniques: Anatomization and sustainability issues," *Comput. Sci. Rev.*, vol. 39, Feb. 2021, Art. no. 100359.

[11] J. Kundu, S. Alam, and A. Dey, "Fuzzy based trusted malicious unmanned aerial vehicle detection using in flying ad-hoc network," *Alexandria Eng. J.*, vol. 99, pp. 232–241, Jul. 2024.

[12] Y. Lu, W. Wen, K. K. Igorevich, P. Ren, H. Zhang, Y. Duan, H. Zhu, and P. Zhang, "UAV ad hoc network routing algorithms in space–air–ground integrated networks: Challenges and directions," *Drones*, vol. 7, no. 7, p. 448, Jul. 2023.

[13] M. Zhang, C. Dong, P. Yang, T. Tao, Q. Wu, and T. Q. S. Quek, "Adaptive routing design for flying ad hoc networks," *IEEE Commun. Lett.*, vol. 26, no. 6, pp. 1438–1442, Jun. 2022.

[14] B. Zheng, K. Zhuo, H. Zhang, and H.-X. Wu, "A novel airborne greedy geographic routing protocol for flying ad hoc networks," *Wireless Netw.*, vol. 30, no. 5, pp. 4413–4427, Jul. 2024.

[15] N. Qi, Z. Huang, W. Sun, S. Jin, and X. Su, "Coalitional formation-based group-buying for UAV-enabled data collection: An auction game approach," *IEEE Trans. Mobile Comput.*, vol. 22, no. 12, pp. 7420–7437, Oct. 2022.

[16] A. Abu-Baker, H. Shakhatreh, A. Sawalmeh, and A. H. Alenezi, "Efficient data collection in UAV-assisted cluster-based wireless sensor networks for 3D environment: Optimization study," *J. Sensors*, vol. 2023, pp. 1–21, Apr. 2023.

[17] J. Hu, Y. Zhang, D. Zhao, G. Yang, F. Chen, C. Zhou, and W. Chen, "A robust deep learning approach for the quantitative characterization and clustering of peach tree crowns based on UAV images," *IEEE Trans. Geosci. Remote Sens.*, vol. 60, 2022, Art. no. 4408613.

[18] H. Bastami, M. Moradikia, A. Abdelhadi, H. Behroozi, B. Clerckx, and L. Hanzo, "Maximizing the secrecy energy efficiency of the cooperative rate-splitting aided downlink in multi-carrier UAV networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 11, pp. 11803–11819, Nov. 2022.

[19] J. Kundu, S. Alam, and C. Koner, "TCSFANET: Trusted communication scheme for FANET system," in *Proc. Int. Conf. Mach. Learn., Comput. Syst. Secur. (MLCSS)*, Aug. 2022, pp. 353–357.

[20] R. Alkadi and A. Shoufan, "Unmanned aerial vehicles traffic management solution using crowd-sensing and blockchain," *IEEE Trans. Netw. Service Manage.*, vol. 20, no. 1, pp. 201–215, Mar. 2023.

[21] S. A. H. Mohsan, N. Q. H. Othman, Y. Li, M. H. Alsharif, and M. A. Khan, "Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends," *Intell. Service Robot.*, vol. 16, pp. 109–137, Jan. 2023.

[22] G. Bansal, Naren, V. Chamola, and B. Sikdar, "SHOTS: Scalable secure authentication-attestation protocol using optimal trajectory in UAV swarms," *IEEE Trans. Veh. Technol.*, vol. 71, no. 6, pp. 5827–5836, Jun. 2022.

[23] G. Khayat, C. X. Mavromoustakis, A. Pitsillides, J. M. Batalla, E. K. Markakis, and G. Mastorakis, "On the weighted cluster S-UAV scheme using latency-oriented trust," *IEEE Access*, vol. 11, pp. 56310–56323, 2023.

[24] W. Wei, J. Wang, Z. Fang, J. Chen, Y. Ren, and Y. Dong, "3U: Joint design of UAV-USV-UUV networks for cooperative target hunting," *IEEE Trans. Veh. Technol.*, vol. 72, no. 3, pp. 4085–4090, Mar. 2023.

[25] R. Fotohi, E. Nazemi, and F. S. Aliee, "An agent-based self-protective method to secure communication between UAVs in unmanned aerial vehicle networks," *Veh. Commun.*, vol. 26, Dec. 2020, Art. no. 100267.

[26] A. Zilberman, A. Stulman, and A. Dvir, "Identifying a malicious node in a UAV network," *IEEE Trans. Netw. Service Manage.*, vol. 21, no. 1, pp. 1226–1240, Feb. 2024.

[27] Y. Cui, Z. Feng, Q. Zhang, Z. Wei, C. Xu, and P. Zhang, "Toward trusted and swift UAV communication: ISAC-enabled dual identity mapping," *IEEE Wireless Commun.*, vol. 30, no. 1, pp. 58–66, Feb. 2023.

[28] D. Kumar and S. Sonia, "Resources efficient dynamic clustering algorithm for flying ad-hoc network," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 11, no. 2s, pp. 106–117, Jan. 2023.

[29] A. M. Tadkal and S. V. Mallapur, "Red deer optimization algorithm inspired clustering-based routing protocol for reliable data dissemination in FANETs," *Mater. Today, Proc.*, vol. 60, pp. 1882–1889, Jan. 2022.

[30] K. Singh, A. K. Verma, and P. Aggarwal, "Analysis of various trust computation methods: A step toward secure FANETs," in *Computer and Cyber Security*. Boca Raton, FL, USA: Auerbach Publications, 2018, pp. 171–193.

[31] Y. Wang, Z. Su, T. H. Luan, J. Li, Q. Xu, and R. Li, "SEAL: A strategy-proof and privacy-preserving UAV computation offloading framework," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 5213–5228, 2023.

[32] P. Pekarcík, E. Chovancová, M. Havrilla, and M. Hasin, "Security analysis of attacks on UAV," in *Proc. IEEE 21st World Symp. Appl. Mach. Intell. Informat. (SAMI)*, Jan. 2023, pp. 57–62.

[33] S. Tangade, R. A. Kumaar, M. S, M. S, and F. Azam, "Detection of malicious nodes in flying ad-hoc network with supervised machine learning," in *Proc. 3rd Int. Conf. Smart Technol. Comput., Electr. Electron. (ICSTCEE)*, Dec. 2022, pp. 1–5.

[34] E. Barka, C. A. Kerrache, R. Hussain, N. Lagraa, A. Lakas, and S. H. Bouk, "A trusted lightweight communication strategy for flying named data networking," *Sensors*, vol. 18, no. 8, p. 2683, Aug. 2018.

[35] S. U. Jan, I. A. Abbasi, F. Algarni, and A. S. Khan, "A verifiably secure ECC based authentication scheme for securing IoD using FANET," *IEEE Access*, vol. 10, pp. 95321–95343, 2022.

[36] S. M. A. Huda and S. Moh, "Survey on computation offloading in UAV-enabled mobile edge computing," *J. Netw. Comput. Appl.*, vol. 201, May 2022, Art. no. 103341.

[37] G. Alsuhli, A. Fahim, and Y. Gadallah, "A survey on the role of UAVs in the communication process: A technological perspective," *Comput. Commun.*, vol. 194, pp. 86–123, Oct. 2022.

[38] Z. Cheng, M. Liwang, N. Chen, L. Huang, X. Du, and M. Guizani, "Deep reinforcement learning-based joint task and energy offloading in UAV-aided 6G intelligent edge networks," *Comput. Commun.*, vol. 192, pp. 234–244, Aug. 2022.

[39] P. Zhang, C. Wang, N. Kumar, W. Zhang, and L. Liu, "Dynamic virtual network embedding algorithm based on graph convolution neural network and reinforcement learning," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 9389–9398, Jun. 2022.

[40] X. Qiu, Y. Yang, L. Xu, J. Yin, and Z. Liao, "Maintaining links in the highly dynamic FANET using deep reinforcement learning," *IEEE Trans. Veh. Technol.*, vol. 72, no. 3, pp. 2804–2818, Mar. 2023.

[41] C. Wang, L. Liu, C. Jiang, S. Wang, P. Zhang, and S. Shen, "Incorporating distributed DRL into storage resource optimization of space-air-ground integrated wireless communication network," *IEEE J. Sel. Topics Signal Process.*, vol. 16, no. 3, pp. 434–446, Apr. 2022.

[42] L. Song, G. Sun, H. Yu, X. Du, and M. Guizani, "FBIA: A fog-based identity authentication scheme for privacy preservation in Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5403–5415, May 2020.

[43] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for VANETs with batch verification," *Wireless Netw.*, vol. 21, no. 5, pp. 1733–1743, Jul. 2015.

[44] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in UAV communication networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1123–1152, 2nd Quart., 2016.

[45] C. Lin, D. He, N. Kumar, K. R. Choo, A. Vinel, and X. Huang, "Security and privacy for the Internet of Drones: Challenges and solutions," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 64–69, Jan. 2018.

[46] Y. Tian, J. Yuan, and H. Song, "Efficient privacy-preserving authentication framework for edge-assisted Internet of Drones," *J. Inf. Secur. Appl.*, vol. 48, Oct. 2019, Art. no. 102354.

[47] L. Chen, S. Qian, M. Lim, and S. Wang, "An enhanced direct anonymous attestation scheme with mutual authentication for network-connected UAV communication systems," *China Commun.*, vol. 15, no. 5, pp. 61–76, May 2018.

[48] Y. Zhang, D. He, L. Li, and B. Chen, "A lightweight authentication and key agreement scheme for Internet of Drones," *Comput. Commun.*, vol. 154, pp. 455–464, Mar. 2020.

[49] J. Srinivas, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of Drones environment," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6903–6916, Jul. 2019.

[50] X. Wei, H. Yang, and W. Huang, "A genetic-algorithm-based optimization routing for FANETs," *Frontiers Neurorobotics*, vol. 15, Jun. 2021, Art. no. 697624.

[51] L. YanB, G. XueH, and F. YanF, "Trust evaluation method based on behavior detection of Internet of Things nodes," *J. Commun.*, vol. 35, no. 5, pp. 8–15, 2014.

[52] C. F. E. de Melo, T. D. e Silva, F. Boeira, J. M. Stocchero, A. Vinel, M. Asplund, and E. P. de Freitas, "UAVouch: A secure identity and location validation scheme for UAV-networks," *IEEE Access*, vol. 9, pp. 82930–82946, 2021.

[53] K. Singh and A. K. Verma, "TBCS: A trust based clustering scheme for secure communication in flying ad-hoc networks," *Wireless Pers. Commun.*, vol. 114, no. 4, pp. 3173–3196, Oct. 2020.

[54] E. Barka, C. A. Kerrache, N. Lagraa, A. Lakas, C. T. Calafate, and J.-C. Cano, "UNION: A trust model distinguishing intentional and unintentional misbehavior in inter-UAV communication," *J. Adv. Transp.*, vol. 2018, pp. 1–12, Jan. 2018.

[55] R. Ganesan, X. M. Raajini, A. Nayyar, P. Sanjeevikumar, E. Hossain, and A. H. Ertas, "BOLD: Bio-inspired optimized leader election for multiple drones," *Sensors*, vol. 20, no. 11, p. 3134, Jun. 2020.

[56] V. Bhardwaj, N. Kaur, S. Vashisht, and S. Jain, "SecRIP: Secure and reliable intercluster routing protocol for efficient data transmission in flying ad hoc networks," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 6, Jun. 2021, Art. no. e4068.

[57] G. Gankhuyag, A. P. Shrestha, and S.-J. Yoo, "Robust and reliable predictive routing strategy for flying ad-hoc networks," *IEEE Access*, vol. 5, pp. 643–654, 2017.

[58] I. A. Kapetanidou, P. Mendes, and V. Tsaoussidis, "Enhancing security in information-centric ad hoc networks," in *Proc. NOMS IEEE/IFIP Netw. Oper. Manage. Symp.*, May 2023, pp. 1–9.

[59] V. Bhardwaj and N. Kaur, "SEEDRP: A secure energy efficient dynamic routing protocol in fanets," *Wireless Pers. Commun.*, vol. 120, no. 2, pp. 1251–1277, Sep. 2021.

[60] M. Namdev, S. Goyal, and R. Agarwal, "An optimized communication scheme for energy efficient and secure flying ad-hoc network (FANET)," *Wireless Pers. Commun.*, vol. 120, no. 2, pp. 1291–1312, Sep. 2021.

[61] M. Khan, I. Qureshi, and F. Khanzada, "A hybrid communication scheme for efficient and low-cost deployment of future flying ad-hoc network (FANET)," *Drones*, vol. 3, no. 1, p. 16, Feb. 2019.

[62] R. M. Pires, A. S. R. Pinto, and K. R. L. J. C. Branco, "The broadcast storm problem in FANETs and the dynamic neighborhood-based algorithm as a countermeasure," *IEEE Access*, vol. 7, pp. 59737–59757, 2019.

[63] R. Valentino, W.-S. Jung, and Y.-B. Ko, "Opportunistic computational offloading system for clusters of drones," in *Proc. 20th Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2018, pp. 303–306.

[64] K. Singh and A. K. Verma, "A fuzzy-based trust model for flying ad hoc networks (FANETs)," *Int. J. Commun. Syst.*, vol. 31, no. 6, Apr. 2018, Art. no. e3517.

[65] R. Ali, D. Kang, G. Suh, and Y.-J. Cha, "Real-time multiple damage mapping using autonomous UAV and deep faster region-based neural networks for GPS-denied structures," *Autom. Construct.*, vol. 130, Oct. 2021, Art. no. 103831.

[66] X. Du, Y. Li, S. Zhou, and Y. Zhou, "ATS-LIA: A lightweight mutual authentication based on adaptive trust strategy in flying ad-hoc networks," *Peer Peer Netw. Appl.*, vol. 15, no. 4, pp. 1979–1993, Jul. 2022.

[67] S. Kumar, R. S. Raw, A. Bansal, M. A. Mohammed, P. Khuwuthyakorn, and O. Thinnukool, "3D location oriented routing in flying ad-hoc networks for information dissemination," *IEEE Access*, vol. 9, pp. 137083–137098, 2021.

[68] H. Khelifi, S. Luo, B. Nour, H. Moungla, Y. Faheem, R. Hussain, and A. Ksentini, "Named data networking in vehicular ad hoc networks: State-of-the-art and challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 320–351, 1st Quart., 2020.

[69] R. Denis and P. Madhubala, "Evolutionary computing assisted visually-imperceptible hybrid cryptography and steganography model for secure data communication over cloud environment," *Int. J. Comput. Netw. Appl.*, vol. 7, no. 6, p. 208, Dec. 2020.

[70] Y. Yan, X. Xia, L. Zhang, Z. Li, and C. Qin, "A clustering scheme based on the binary whale optimization algorithm in FANET," *Entropy*, vol. 24, no. 10, p. 1366, Sep. 2022.

[71] M. Y. Arafat and S. Moh, "Localization and clustering based on swarm intelligence in UAV networks for emergency communications," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8958–8976, Oct. 2019.

[72] J. Liu, W. Wang, X. Li, T. Wang, and T. Wang, "A motif-based mission planning method for UAV swarms considering dynamic reconfiguration," *Defence Sci. J.*, vol. 68, no. 2, p. 159, Mar. 2018.

[73] V. Sharma, R. Kumar, and N. Kumar, "DPTR: Distributed priority tree-based routing protocol for FANETs," *Comput. Commun.*, vol. 122, pp. 129–151, Jun. 2018.

[74] M. M. Mehdi, I. Raza, and S. A. Hussain, "A game theory based trust model for vehicular ad hoc networks (VANETs)," *Comput. Netw.*, vol. 121, pp. 152–172, Jul. 2017.

[75] M. Usha, J. Sathiamoorthy, R. Ashween, and B. N. Ramakrishnan, "EEMCCP–A novel architecture protocol design for efficient data transmission in underwater acoustic wireless sensor network," *Int. J. Comput. Netw. Appl.*, vol. 7, no. 2, p. 28, Apr. 2020.

[76] F. Khelifi, A. Bradai, K. Singh, and M. Atri, "Localization and energy-efficient data routing for unmanned aerial vehicles: Fuzzy-logic-based approach," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 129–133, Apr. 2018.

[77] P. Gope and B. Sikdar, "An efficient privacy-preserving authenticated key agreement scheme for edge-assisted Internet of Drones," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13621–13630, Nov. 2020.

[78] F. A. Ali and K. R. E. Dhanapal, "Topology based energy efficient routing using integration of fuzzy based Markov chain cluster-optimized novel ant bee colony approach in FANET," *Concurrency Comput., Pract. Exper.*, vol. 34, no. 23, Oct. 2022, Art. no. e7175.

[79] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Design and analysis of secure lightweight remote user authentication and key agreement scheme in Internet of Drones deployment," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3572–3584, Apr. 2019.

[80] S. S. Priya and M. Mohanraj, "Flying ad-hoc networks rely on trust-aware route selection for efficient packet transmission," *J. Algebr. Statist.*, vol. 13, no. 3, pp. 682–692, 2022.

[81] O. S. Oubbati, M. Atiquzzaman, P. Lorenz, M. H. Tareque, and M. S. Hossain, "Routing in flying ad hoc networks: Survey, constraints, and future challenge perspectives," *IEEE Access*, vol. 7, pp. 81057–81105, 2019.

[82] S.-Y. Park, C. S. Shin, D. Jeong, and H. Lee, "DroneNetX: Network reconstruction through connectivity probing and relay deployment by multiple UAVs in ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11192–11207, Nov. 2018.

[83] S. Lateef, M. Rizwan, and M. A. Hassan, "Security threats in flying ad hoc network (FANET)," in *Computational Intelligence for Unmanned Aerial Vehicles Communication Networks*. Cham, Switzerland: Springer, 2022, pp. 73–96.

[84] T. Feng, W. Fan, J. Tang, and W. Zeng, "Consensus-based robust clustering and leader election algorithm for homogeneous UAV clusters," *J. Phys., Conf. Ser.*, vol. 1168, Feb. 2019, Art. no. 032073.

[85] N. Zhang, Q. Jiang, L. Li, X. Ma, and J. Ma, "An efficient three-factor remote user authentication protocol based on BPV-FourQ for Internet of Drones," *Peer Peer Netw. Appl.*, vol. 14, no. 5, pp. 3319–3332, Sep. 2021.
[86] K. A. Darabkh, M. G. Alfawares, and S. Althunibat, "MDRMA: Multi-data rate mobility-aware AODV-based protocol for flying ad-hoc networks," *Veh. Commun.*, vol. 18, Aug. 2019, Art. no. 100163.
[87] R. Rahim, S. Murugan, S. Priya, S. Magesh, and R. Manikandan, "Taylor based grey wolf optimization algorithm (TGWOA) for energy aware secure routing protocol," *Int. J. Comput. Netw. Appl.*, vol. 7, no. 4, p. 93, Aug. 2020.
[88] S. Z. Arnosti, R. M. Pires, and K. R. L. J. C. Branco, "Evaluation of cryptography applied to broadcast storm mitigation algorithms in FANETs," in *Proc. Int. Conf. Unmanned Aircr. Syst. (ICUAS)*, Jun. 2017, pp. 1368–1377.
[89] J. Sathiamoorthy and B. Ramakrishnan, "A competent three-tier fuzzy cluster algorithm for enhanced data transmission in cluster EAACK MANETs," *Soft Comput.*, vol. 22, no. 19, pp. 6545–6565, Oct. 2018.
[90] D. Sharma and A. Jameel, "Enhancement of security in flying AD-HOC network using a trust based routing mechanism," *Int. J. Innov. Technol. Exploring Eng.*, vol. 9, no. 1, pp. 253–257, Nov. 2019.

JOYDEEP KUNDU is currently pursuing the Ph.D. degree with the Department of Computer Science and Engineering, Maulana Abul Kalam Azad University, West Bengal, India. He is also an Assistant Professor with the Department of Computer Science and Engineering, Brainware University, Barasat, Kolkata, India. His research interest includes flying ad-hoc networks.

SAHABUL ALAM received the M.Tech. degree in computer science and engineering from the National Institute of Technology (NIT), Hamirpur, Himachal Pradesh, India, and the Ph.D. degree in computer science and engineering from Maulana Abul Kalam Azad University, West Bengal, India. He is currently an Associate Professor with the Department of Computer Science and Engineering, Brainware University, Barasat, Kolkata, India. He has published various number of research articles in highly reputed journals and conferences. His research interests include wireless sensor networks, the IoT, and flying ad-hoc networks.

JADAV CHANDRA DAS received the M.Tech. degree in multimedia and software systems and the Ph.D. degree in computer science and engineering (nanotechnology) from West Bengal University of Technology, West Bengal, India, in 2011 and 2019, respectively. He is currently an Assistant Professor with the Department of Information Technology and HOD, Ph.D. Cell, Maulana Abul Kalam Azad University of Technology, Simhat, Haringhata, Nadia, West Bengal. Previously, he was associated with the Department of CSE, UEM, Kolkata, and SVIST, Sonarpur, Kolkata. He has more than 12 years of teaching experiences and has ten years of research experience during which he has published more than 70 research papers in peer-reviewed journals and conferences. He has more than 40 SCI journals publications. He received many prestigious honours for best papers publication in SCI journals and conferences. He has good scholarly records. His research interests include cryptography, steganography, QCA-based image processing, reversible logic design with QCA, nanocommunication network design, the IoT, and quantum computing. He is one of the top researchers in his institute as per AD Scientific Index, in 2023. He received IET Premium Award for best journal article in *IET Circuits Devices & Systems* journal, in 2018, and J. C. Bose Memorial Award for best journal article in *IETE Journal of Research*, in 2016.

ARINDAM DEY received the B.Tech. degree in computer science and technology from the Netaji Subhash Engineering College, Garia, India, and the M.Tech. and Ph.D. degrees from NIT Durgapur, India, in 2012, and 2018, respectively. He is currently an Associate Professor with the School of Computer Science, VIT-AP University, India. He has more than 14 years of teaching and research experience. His research interests include fuzzy optimization and genetic algorithms. Till date, he has published more than 50 research articles in national and international peer-reviewed journals.

DEBASHIS DE (Senior Member, IEEE) received the M.Tech. degree from the University of Calcutta, in 2002, and the Ph.D. degree from Jadavpur University, in 2005. He is currently a Professor with the Department of Computer Science and Engineering, Maulana Abul Kalam Azad University of Technology, West Bengal, India. He is a fellow of IETE and a Life Member of CSI. He was awarded the prestigious Boyscast Fellowship by the Department of Science and Technology, Government of India, to work at the Heriot-Watt University, Scotland, U.K. He received the Endeavour Fellowship Award, from 2008 to 2009, by DEST Australia to work with the University of Western Australia. He received the Young Scientist Award, in 2005, at New Delhi and, in 2011, in Istanbul, Turkey, from the International Union of Radio Science, Belgium. In 2016, he received the JC Bose Research Award from IETE, New Delhi. In 2019, he received the Shiksha-Ratna Award from the Government of West Bengal. He established the Center of Mobile Cloud Computing (CMCC) for IoT Applications. He has published in 390 journals and 200 conference papers, 15 books, and filed ten patents and four granted. He has projects sponsored by AICTE, UGC, WBDST, DST, WBDST, World Bank, AWS, and MeitY. His H-index is 44, the citation is 9325. He supervised 22 Ph.D. students. His research interests include mobile cloud computing, AI, the IoT, and quantum computing.