International Journal of Innovative Research in Computer Science and Technology (IJIRCST)
ISSN (Online): 2347-5552, Volume-14, Issue-2, March 2026
DOI: https://doi.org/10.55524/ijircst.2026.14.2.1
Article ID IRP-1721, Pages 1-8
www.ijircst.org

Threat Defensive Intelligent Trust Framework for Secure FANET Clustering

Shikha Gupta[1], and Deepak Gupta[2]

[1, 2] Assistant Professor, Department of Computer Science and Engineering, Engineering College Ajmer, Ajmer, India

Correspondence should be addressed to Shikha Gupta; shikhagupta@ecajmer.ac.in

Received: 17 January 2026; Revised: 6 February 2026; Accepted: 18 February 2026

ABSTRACT- Flying Ad Hoc Networks facilitate UAV-to-UAV communication for exchanging data to support many real-time applications such as surveillance, intelligent transportation, disaster response, and other critical services. Clustering is commonly utilized to support efficient communication for information collection and processing as the network expands. However, malicious UAVs may deliberately gain access to clusters and disrupt network operations by dropping packets, spreading false information, or by forwarding attacks, thereby severely degrading network reliability. To address these challenges, this paper proposes a trust-aware and secure cluster head selection mechanism, named TTSCH, designed to enhance overall network security by early identifying and removing malicious node from the network. The proposed scheme evaluates UAV behavior using multiple trust metrics, including packet forwarding ratio, communication reliability, energy consistency, and mobility stability. These trust values are integrated with traditional clustering parameters to securely elect reliable cluster heads while excluding malicious UAVs from the election process. Furthermore, a dynamic malicious node isolation mechanism is incorporated to handle on–off and insider attacks. When compared to state-of-the-art clustering systems in the presence of variable malicious UAVs, simulation results show that the proposed TTSCH significantly improves packet delivery ratio, throughput, and network stability while lowering delay.

KEYWORDS- FANET, UAV, Trust, Cluster Head, Malicious Node, NS-2.35.

I. INTRODUCTION

The deployment of cooperative multi-UAV systems for a range of objectives, such as intelligent transportation, border surveillance, environmental monitoring, and disaster response, has been made feasible by the rapid advancement of UAV technologies. A Flying Ad Hoc Network (FANET), that facilitates independent communication and coordination between flying nodes, is created when several UAVs operate together without the need for standard infrastructure [1]. Due to the high mobility, dynamic topology, and three-dimensional movement of UAVs, FANETs differ significantly from mobile and vehicular ad hoc networks [2]. Therefore, FANETs present unique design and security challenges. Clustering has evolved into an efficient organizing strategy to improve scalability and lower communication costs in large-scale FANETs. UAVs are organized into clusters, and each cluster is headed by a cluster head (CH), responsible for data collection, routing coordination, and communication between clusters. Communication security, reliability, and overall network performance are all directly impacted by effective cluster head selection. Consequently, a large body of research has focused on optimizing CH election based on parameters such as residual energy, mobility stability, node degree, and link quality [3]. Despite these advances, the security of cluster head selection remains a largely overlooked aspect of FANET design. FANETs are frequently set up in open environments where malicious nodes may be introduced by attackers. Malicious UAVs acting as insider nodes have control over authentic identification and can actively participate in network communication. Such nodes can purposefully act as cluster heads and take control of important network operations by taking advantage of vulnerabilities in CH election procedures. Such malicious UAV may seriously damage network operations by discarding packets, modifying routing data, injecting fake control messages, or initiating other categories of attack operations after being chosen as a cluster head [4]. The challenge becomes stronger as the FANETs' consists of high mobility UAV nodes as well as frequent topology changes, which need periodic CH reconstitution and give attacker UAVs plenty of opportunities to utilize the benefit of the election process. Conventional safety measures are ineffective to solve this issue as they are dependent of cryptographic authentication and encryption and primarily designed to protect against external threats and do not identify malicious activities by inner UAV nodes. Additionally, due to the restricted network for communications, latency, and resource limits of UAV platforms, the centralized intrusion detection systems are not feasible in FANETs. [5]. Therefore, FANET security solutions must be lightweight, decentralized, adaptive, and capable of identifying malicious behavior in real time. To address these challenges, this paper proposes a trust-aware secure cluster head selection framework that explicitly considers malicious UAV behavior during the clustering process. The proposed framework evaluates UAV reliability using multiple behavioral trust metrics, including packet forwarding behavior, mobility consistency, and energy reporting honesty. The TTSCH framework minimizes the network's attack exposure by

eliminating suspicious or low-trust UAVs from being chosen as cluster heads by directly including trust evaluation during the CH election procedure.

II. RELATED WORK

Because FANETs can be used in mission-oriented and time-sensitive situations, they have garnered a lot of research interest. Clustering has been frequently used to increase communication reliability, lower routing overhead, and improve network scalability because of the high mobility of UAVs and their dynamic topology changes [6]. The cluster head (CH) is essential to gathering data, routing organization, and among-cluster communication in cluster-based FANETs. Early clustering techniques for FANETs and MANETs focused on energy efficiency and topology stability, selecting CHs based on metrics [7]. Although these techniques enhance network performance, they ignore security risks and presume a secure environment. They are therefore extremely susceptible to insider threats in which bad UAVs appear as authorized users on the network and interfere in the clustering mechanism. To address security challenges, several trust-based mechanisms have been proposed for UAV and ad hoc networks [8]. These approaches evaluate node behavior using packet forwarding ratio, acknowledgment success rate, and communication reliability. Although trust models help in identifying malicious nodes, most existing works treat trust evaluation as a separate process from clustering [9]. Consequently, malicious UAVs may still be elected as CHs before being detected, allowing them to severely disrupt network operations. Recent studies have attempted to integrate trust into routing and forwarding decisions [10]. By eliminating low-trust nodes when selecting a path, trust-aware routing techniques enhance packet delivery efficiency. However, the cluster head election step is still a significant issue that is not expressly secured by current systems, which are generally routing-centric. Furthermore, trust values in highly dynamic FANETs fluctuate rapidly due to mobility-induced link failures, leading to false positives and unstable decisions [11]. Blockchain-based security frameworks have been proposed to ensure tamper-proof trust management and decentralized decision-making [12], [13]. By maintaining immutable trust records, blockchain can prevent false trust manipulation by malicious UAVs [14]. However, consensus mechanisms, block generation delays, and communication overhead introduce latency and energy consumption, making such solutions less suitable for highly mobile FANET environments where rapid CH re-election is frequently required [15]. Some recent works have explored hybrid approaches, combining clustering with trust, fuzzy logic, or optimization techniques [16], [17]. Fuzzy-based trust models help handle uncertainty in trust evaluation, while swarm intelligence algorithms optimize CH selection. Nevertheless, many of these schemes either lack a well-defined attack model and may fail to address specific attacks like on–off attacks, where malicious UAVs behave normally during the selection phase and misbehave afterward [18]. The proposed trust-aware secure cluster head selection framework integrates malicious behavior detection directly into the clustering process, ensuring that only reliable UAVs are elected as CHs [19]. By combining multi-metric trust evaluation with mobility and energy awareness, the proposed solution provides a lightweight, adaptive, and robust defense against malicious UAVs while maintaining high network performance in FANET environments.

III. PROPOSED TTSCH

The proposed threat-aware clustering architecture TTSCH is designed to securely organize UAVs in a Flying Ad Hoc Network while mitigating the influence of malicious nodes during the cluster head selection process. Initially, UAVs perform neighbor discovery and cluster formation based on proximity and mobility information in the three-dimensional network space. Behavioral observations collected during communication are then forwarded to the trust evaluation module, which computes dynamic trust values by analysing packet forwarding behavior, mobility consistency, and energy reporting honesty. These trust values are continuously updated using historical aging to capture long-term node behavior and to mitigate on–off attacks. A malicious UAV detection engine applies trust thresholding to identify and isolate suspicious nodes, ensuring that only reliable UAVs participate in leadership roles. The most reliable and stable UAV is then chosen as the cluster head by the secure cluster head selection module, which combines trust scores with residual energy and motion stability. Lastly, the chosen cluster heads monitor inter-cluster routing and secure data aggregation, and regular evaluation allows for adaptive cluster head re-election in response to recognized malicious activity or changes in the topology. In extremely dynamic FANET contexts, this modular design maintains effective communication while providing strong, decentralized, and lightweight security.

A. System Model

Consider a FANET consisting of N UAVs deployed in a three-dimensional space where each UAV is equipped with the wireless transceiver, GPS for position, mobility tracking, battery and other computation resources. Set of N UAVs that is U are shown through (1), such that the UAVs communicate in an ad hoc and decentralized manner and a subset of UAVs may act as insider attackers with valid credentials, while the network periodically forms clusters to enable scalable and efficient communication. Figure 1 shows the workflow for TTSCH.

$$U = \{u_1, u_2, \dots, u_N\} \quad (1)$$

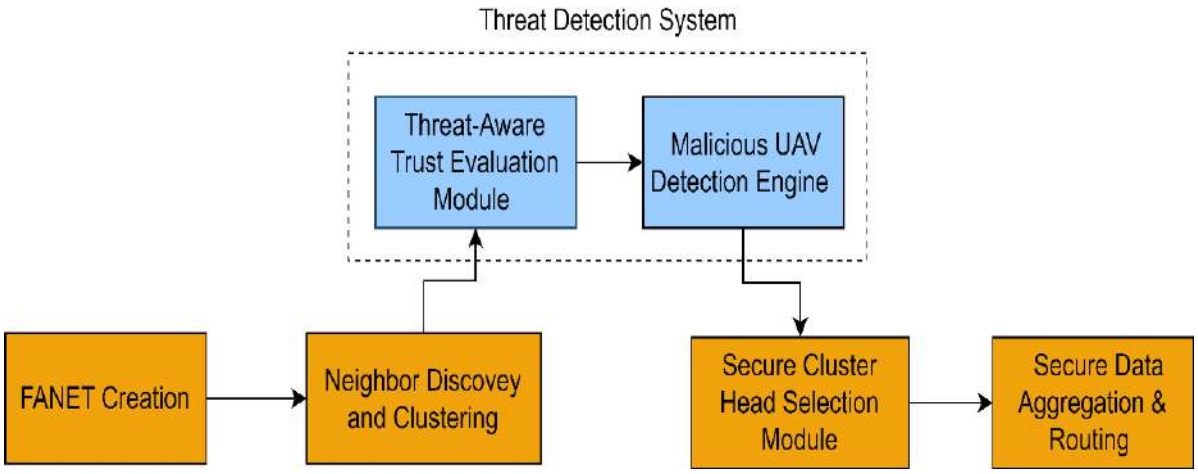

Figure 1: TTSCH workflow

B. Threat Model

The proposed clustering model explicitly considers multiple malicious behaviours that threaten the security of cluster-based FANETs. It accounts for gray hole attacks, where a malicious UAV selectively drops data packets after being elected as a cluster head, thereby disrupting data forwarding while avoiding immediate detection. It also addresses on–off attacks, in which a UAV alternates between normal and malicious behaviour to evade trust-based detection mechanisms. Additionally, the model considers false metric advertisement attacks, where malicious UAVs deliberately report incorrect residual energy or mobility information to increase their likelihood of being selected as cluster heads and gain control over critical network operations. Let the set of malicious UAVs UM among N UAVs from set U are given by (2).

$$U_M \subset U \tag{2}$$

C. Threat Aware Trust Evaluation Model

To counter malicious behaviour, each UAV $u_i$is assigned a dynamic trust score $T_i(t)$, computed using multiple behavioral indicators. A Packet Forwarding Trust (PFT) is computed for using (3), where $P_i^{forwarded}$ are the packets forwarded by u_i and $P_i^{received}$ are the packets received for forwarding. Next the Mobility Consistency Trust (MCT) which measures deviation from expected mobility behavior is given by (4) for UAV current velocity $v_i(t)$, average velocity $\bar{v}_i$ and maximum UAV speed v_{max}. Finally, the composite trust score (Ti) is computed using (5), subject to the condition where $w_1 + w_2 = 1$ and $T_i \in [0,1]$.

$$PFT_i = \frac{P_i^{forwarded}}{P_i^{received}} \tag{3}$$

$$MCT_i = 1 - \frac{|v_i(t) - \bar{v}_i|}{v_{max}} \tag{4}$$

$$T_i = w_1 \cdot PFT_i + w_2 \cdot MCT_i \tag{5}$$

D. Secure Cluster Head Election Model

This approach incorporates reliable cluster head (CH) identification, adaptive trust adjustment, and malicious UAV detection into a single trust-oriented scheme. A node is considered malicious if its trust drops under a particular threshold, i.e., $T_i < T_{th}$; UAVs that consistently exhibit low trust during repeated intervals of monitoring are removed from the network. Only trusted UAVs satisfying the eligibility condition given in (6) are allowed to participate in the CH election process. For each eligible UAV, a CH fitness value is computed by jointly considering trust, and mobility consistency as given in (7), where $\alpha + \gamma = 1$. The UAV with the maximum CH_ivalue is selected as the cluster head, ensuring both reliability and stability. To counter on–off attacks, trust values are dynamically updated using an exponential aging mechanism given by (8), where $\lambda \in [0,1]$controls the influence of historical behavior. This adaptive trust update prevents malicious UAVs from rapidly regaining trust and reinforces long-term security in the cluster formation process. Figure 2 shows the model of approach TTSCH. Algorithm 1 represents the approach for creation of UAVs cluster, while algorithm 2 for secure cluster head selection.

$$u_i \in CH_{eligible} \iff T_i \geq T_{th} \tag{6}$$

$$CH_i = \alpha T_i + \gamma MCT_i \tag{7}$$

$$T_i(t) = \lambda T_i(t-1) + (1-\lambda) T_i^{new} \tag{8}$$

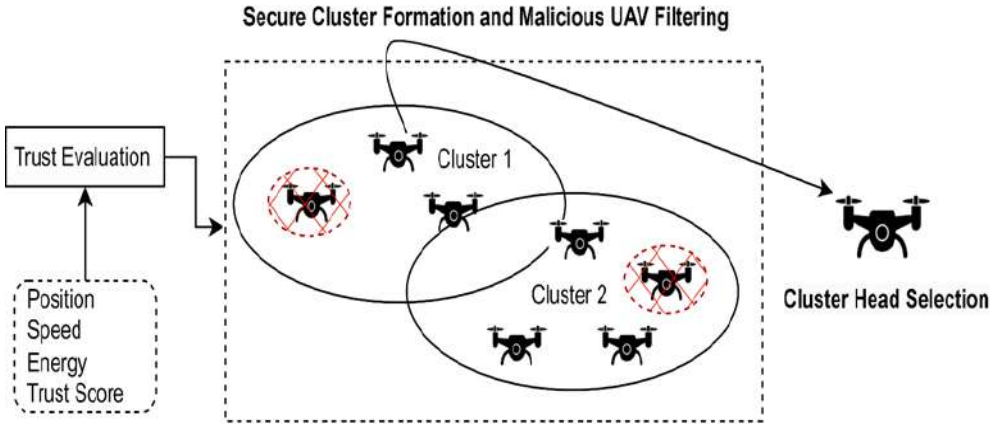

Figure 2: Proposed model for TTSCH

Algorithm 1: Trust-Aware Cluster Creation

Input: Set of UAVs U = {u_1,u_2,…..,u_N},

trust threshold T_{th}

Output: Formed clusters C

Initialize empty cluster set C;

For (each UAV $u_i \in U$)

{

if ($T_i >= T_{th}$)

{

Discover neighboring UAVs

Select neighbors with $T_i >= T_{th}$

Cluster Formation:

Group u_i with selected neighbors

}

else

{

Exclude u_i from cluster formation

}

}

Return C

IV. EXPERIMENTAL EVALUATION

To validate the effectiveness of the proposed method TTSCH, extensive simulation-based 02 experiments were conducted and compared against two representative clustering approaches BTAM [20] and FUBA [21]. The evaluation was performed under identical network conditions, including varying numbers of UAVs, malicious nodes.

Experiment 1 examined the key performance metrics such as packet delivery ratio (PDR), end-to-end delay, and throughput. Consider parameters and their values for experiment are shown in Table 1. The simulation parameters are selected to realistically model a dynamic FANET environment and to evaluate the proposed TTSCH under varying network conditions. A 1000 m^2 area with 30–100 UAVs ensures moderate to high node density, while the Random Waypoint mobility model capture frequent topology changes. A communication range of 250 m and IEEE 802.11s MAC protocol support multi-hop wireless communication. All experiments are conducted using the NS-2.35 simulator to ensure consistent and reproducible results. Figure 3, Figure 4, Figure 5, Figure 6, Figure 7 & Figure 8 represents the outcome of experiment 1 under variable simulation time and variable malicious node during cluster head selection process.

Algorithm 2: Secure Cluster Head Selection

Input: Set of UAVs U = {u_1,u_2,…..,$u_{N;}$}

Output: Secure Cluster Head CH;

Initialize trust score $T_i = 1$ for each UAV u_i

For (each UAV u_i)

{

Compute Packet Forwarding Ratio PFR_i

Measure mobility stability M_i

Update trust score: $T_i = w_1 \cdot PFT_i + w_2 \cdot MCT_i$

}

For (each cluster C_j)

{

Exclude UAVs with $T_i < T_{th}$

For (each remaining UAV $u_i \in C_j$)

{

Compute CH score: $S_i = \alpha \cdot T_i + \gamma \cdot M_i$

}

Select UAV with maximum S_i as Cluster Head

}

Isolate UAVs with persistently low trust scores

Return CH

Table 1: Simulation Parameters

Parameter	Value
Simulation Area	1000 m × 1000 m
Number of UAVs	30 – 100
Mobility Model	Random Waypoint
UAV Speed	10 – 30 m/s
Communication Range	250 m
MAC Protocol	IEEE 802.11s
Traffic Type	CBR
Packet Size	512 bytes
Simulation Time	500 s
Clustering Method	Proposed TTSCH
Simulator	NS-2.35

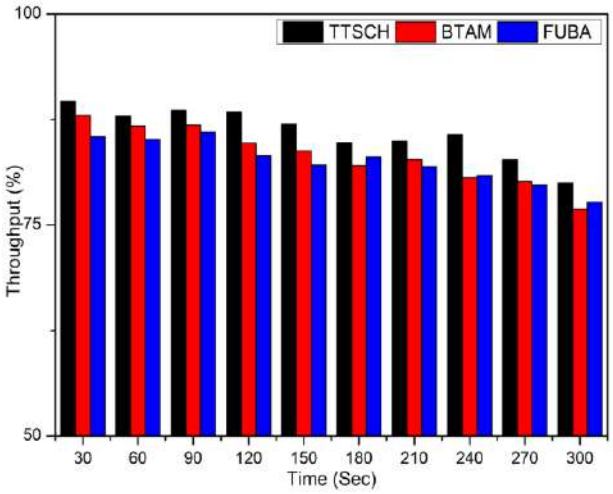

Figure 3: Throughput with simulation time

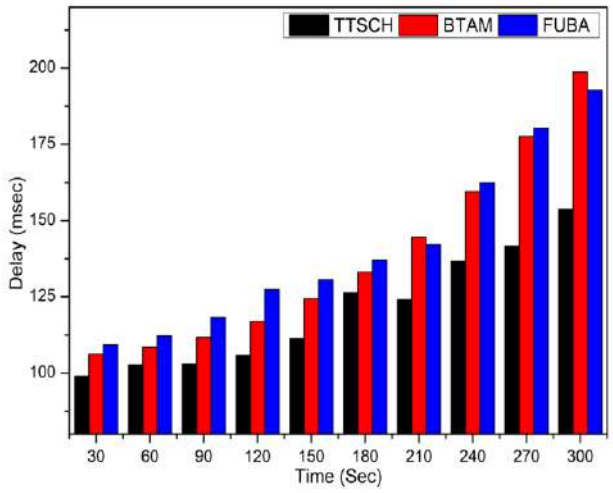

Figure 4: End to end delay with simulation time

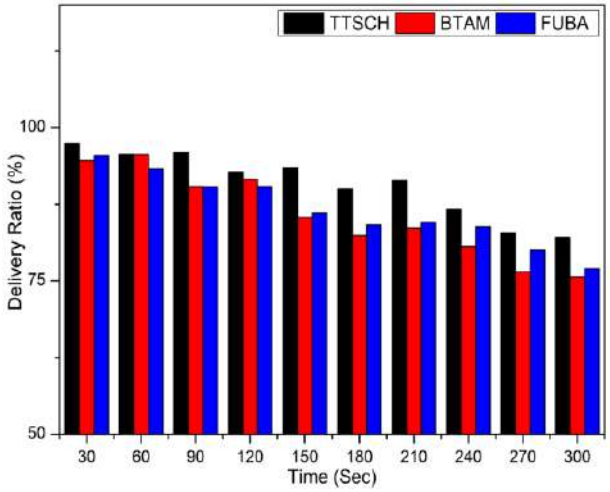

Figure 5: Ratio of packet delivery with simulation time

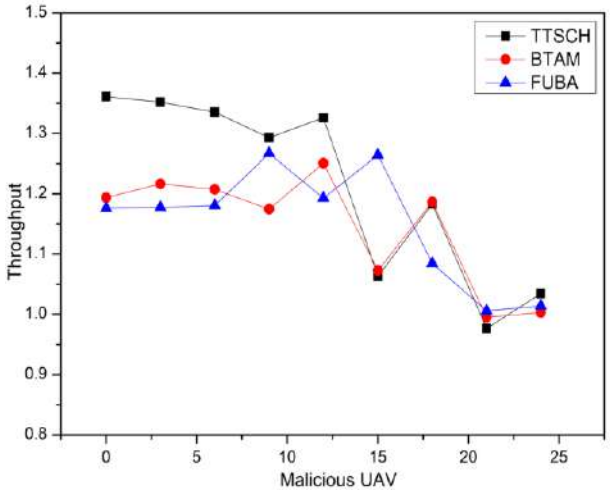

Figure 6: Throughput with malicious units

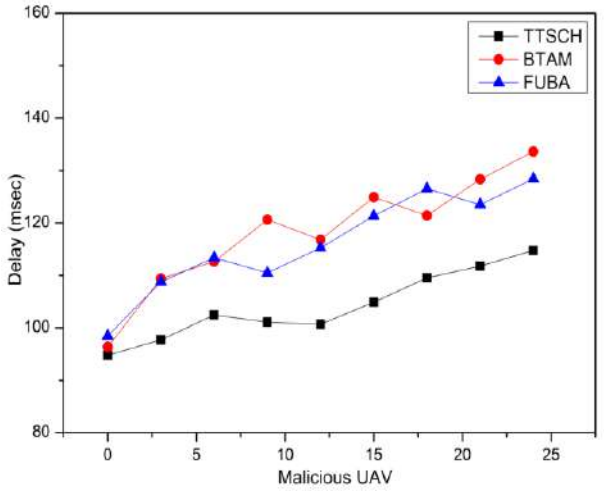

Figure 7: End to end delay with malicious units

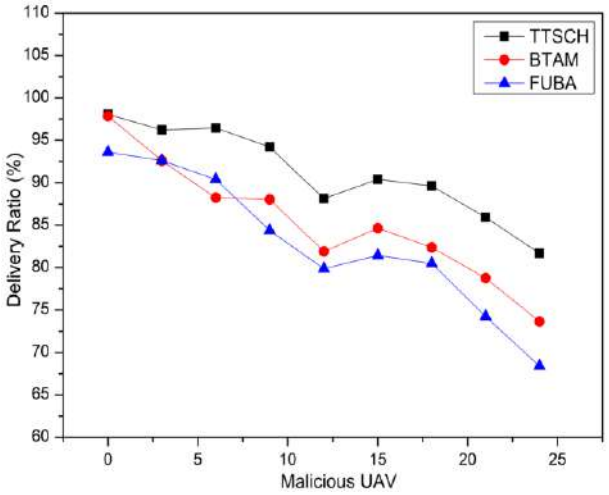

Figure 8: Ratio of packet with malicious units

Experiment 2 examines the attack resilience and durability of TTSCH approach by examining the valid identification of defined UAV classes for UAVs up to 480 nodes varies in the time periods from 0 and 150 seconds during the simulation to cover the real time and practical situations. Attacker UAVs were explicitly labeled, constituting 1% to 10% of the total UAV population, to assess both detection accuracy and response time. This setup enables a detailed examination of how efficiently and promptly the proposed approach identifies malicious UAV behavior. Table 2 presents the identification score, which reflects the threat identification efficiency for various attack categories classes, and Figure 9 shows the associated findings.

Table 2: Test cases for identification score assessment

Time (Seconds)	UAV Instance Count	Considered Count for Class		Accurately Classified		Identification Score (%)
		Ordinary	Attacker	Ordinary	Attacker	
0	80	75	5	74	4	80
30	160	145	15	141	13	86.67
60	240	216	24	212	21	87.5
90	320	292	28	288	25	89.28
120	400	361	39	357	36	92.3
150	480	432	48	429	45	93.75

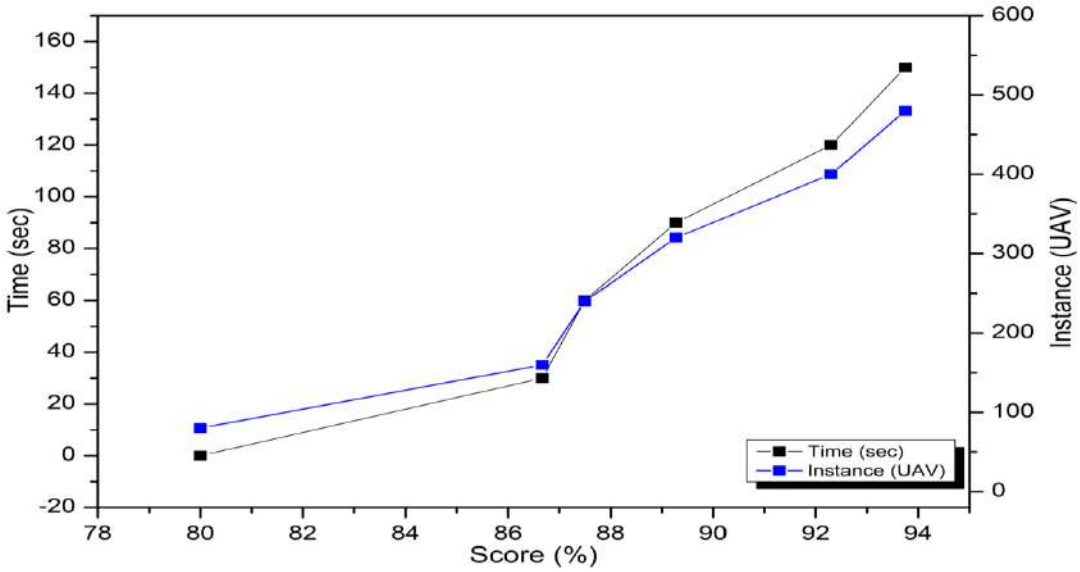

Figure 9: Identification Score achieved through TTSCH

V. CONCLUSION

This paper presented a threat-aware clustering model for FANETs that explicitly considers malicious UAV behavior during the cluster head selection process to enhance network security and reliability. By integrating multi-metric trust evaluation with clustering and cluster head election, the proposed model effectively prevents malicious and low-trust UAVs from assuming cluster head roles within the network. The dynamic trust update mechanism further enables the framework to moderate insider attacks in highly mobile environments. Simulation results demonstrate that method TTSCH consistently achieves a higher delivery ratio than methods BTAM and FUBA, particularly under increasing malicious node density, due to its trust-aware exclusion of unreliable

UAVs during cluster formation and cluster head selection. In terms of delay, TTSCH exhibits lower average end-to-end latency by preventing malicious cluster heads that cause packet drops and route disruptions, whereas BTAM and FUBA suffer from frequent retransmissions. Furthermore, attack scenarios show that TTSCH maintains stable performance with minimal degradation, while the baseline methods experience significant performance deterioration as attack intensity increases. Experiment 2 evaluates attacker UAV detection accuracy under varying time intervals (0–150 s) and network sizes of up to 480 UAVs. The results show that TTSCH effectively identifies attacker UAVs even when their proportion increases from 1% to 10%. Overall, these results confirm that integrating trust-based security mechanisms into the clustering process significantly enhances communication reliability.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] O. Ceviz, S. Sen, and P. Sadioglu, "A survey of security in UAVs and FANETs: Issues, threats, analysis of attacks, and solutions," *IEEE Communications Surveys & Tutorials*, 2024. Available from: https://ieeexplore.ieee.org/abstract/document/10793113

[2] D. Gupta and R. Rathi, "A novel spider monkey optimization for reliable data dissemination in VANETs based on machine learning," *Sensors*, vol. 24, no. 7, p. 2334, 2024. Available from: https://doi.org/10.3390/s24072334

[3] J. Kundu, S. Alam, J. C. Das, and A. Dey, "Trust-based flying ad hoc network: A survey," *IEEE Access*, vol. 12, pp. 99258–99281, 2024. Available from: https://ieeexplore.ieee.org/abstract/document/10574806

[4] J. V. Ananthi, "Implementation of an energy-efficient secure clustering algorithm with trusted path for flying ad hoc networks," *Wireless Networks*, vol. 31, no. 8, pp. 4929–4943, 2025. Available from: https://link.springer.com/article/10.1007/s11276-025-04032-z

[5] K. Singh and A. K. Verma, "TBCS: A trust-based clustering scheme for secure communication in flying ad-hoc networks," *Wireless Personal Communications*, vol. 114, no. 4, pp. 3173–3196, 2020. Available from: https://link.springer.com/article/10.1007/s11277-020-07523-8

[6] D. Gupta and S. Gupta, "PV-DVMC: A novel path visibility based reliable data dissemination in VANETs using machine learning with layered clustering," *Cluster Computing*, vol. 28, no. 11, p. 700, 2025. Available from: https://link.springer.com/article/10.1007/s10586-025-05484-w

[7] 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. Available from: https://ieeexplore.ieee.org/abstract/document/9739713

[8] S. O. Ajakwe, K. L. Olabisi, and D. S. Kim, "Multihop Intruder Node Detection Scheme (MINDS) for secured drones' FANET communication," *IET Intelligent Transport Systems*, vol. 19, no. 1, e70080, 2025. Available from: https://doi.org/10.1049/itr2.70080

[9] S. Gupta and N. Sharma, "A novel cluster based reliable security enhancement in FANET directed by game theory," *Soft Computing*, pp. 1–16, 2025. Available from: https://link.springer.com/article/10.1007/s00500-025-10502-5

[10] M. Zhang, C. Cheong, Y. Cao, L. Zhang, H. Lin, and A. A. Abd El-Latif, "A UAV-assisted traceable and hierarchical trust management in VANET for disaster data collection," *IEEE Transactions on Network and Service Management*, 2025. Available from: https://ieeexplore.ieee.org/abstract/document/11104826

[11] S. Benfriha, N. Labraoui, H. B. Salameh, and H. Saidi, "A survey on trust management in flying ad hoc networks: Challenges, classifications, and analysis," in *Proc. 2023 10th Int. Conf. Software Defined Systems (SDS)*, 2023, pp. 107–114. Available from: https://ieeexplore.ieee.org/abstract/document/10329156

[12] N. Kolokotronis, S. Brotsis, G. Germanos, C. Vassilakis, and S. Shiaeles, "On blockchain architectures for trust-based collaborative intrusion detection," in *Proc. 2019 IEEE World Congress on Services*, vol. 2642, 2019, pp. 21–28. Available from: https://ieeexplore.ieee.org/abstract/document/8817140

[13] S. Gupta and N. Sharma, "Machine learning driven threat identification to enhance FANET security using genetic algorithm," *The International Arab Journal of Information Technology*, vol. 21, no. 4, pp. 711–722, 2024. Available from: https://tinyurl.com/yvfhadj7

[14] J. Gao, C. Cheong, M. Zhang, Y. Cao, T. Peng, and S. Pervez, "A trust model with fitness-based clustering scheme in FANETs," in *Proc. 2024 IEEE 23rd Int. Conf. Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2024, pp. 978–985. Available from: https://ieeexplore.ieee.org/abstract/document/10944812

[15] S. Danesh and J. Akbari Torkestani, "CLARA: Clustered learning automata-based routing algorithm for efficient FANET communication," *Cluster Computing*, vol. 27, no. 7, pp. 9569–9585, 2024. Available from: https://link.springer.com/article/10.1007/s10586-024-04299-5

[16] W. Buksh, Y. Guo, S. Iqbal, K. N. Qureshi, and J. Lloret, "Trust-oriented peered customized mechanism for malicious nodes isolation for flying ad hoc networks," *Transactions on Emerging Telecommunications Technologies*, vol. 35, no. 4, e4489, 2024. Available from: https://doi.org/10.1002/ett.4489

[17] S. Ghanghas, S. Kumar, D. Kumar, and K. Dutta, "Exploring security threats in FANETs: A study of vulnerabilities and attacks," in *Proc. Int. Conf. Information and Communication Technology for Intelligent Systems*, Singapore: Springer Nature Singapore, 2025, pp. 381–402. Available from: https://link.springer.com/chapter/10.1007/978-981-96-9275-0_33

[18] S. Gupta and N. Sharma, "SCFS—Securing flying ad hoc network using cluster-based trusted fuzzy scheme," *Complex & Intelligent Systems*, vol. 10, no. 3, pp. 3743–3762, 2024. Available from: https://link.springer.com/article/10.1007/s40747-024-01348-9

[19] R. Rehyadd and D. Gupta, "Intelligent cluster-based routing framework for 5G integrated flying ad hoc networks," in *Proc. 2025 Int. Conf. Next Generation of Green Information and Emerging Technologies (GIET)*, 2025, pp. 1–7. Available from: https://ieeexplore.ieee.org/abstract/document/11234769

[20] K. N. Qureshi, H. Nafea, I. T. Javed, and K. Z. Ghafoor, "Blockchain-based trust and authentication model for detecting and isolating malicious nodes in flying ad hoc networks," *IEEE Access*, vol. 12, pp. 95390–95401, 2024. Available from: https://ieeexplore.ieee.org/abstract/document/10589383

[21] S. Benfriha, N. Labraoui, R. Bensaid, H. B. Salameh, and H. Saidi, "FUBA: Fuzzy-based unmanned aerial vehicle behaviour analytics for trust management in flying ad hoc networks," *IET Networks*, vol. 13, no. 3, pp. 208–220, 2024. Available from: https://doi.org/10.1049/ntw2.12108

ABOUT THE AUTHORS

Dr. Shikha Gupta was born in 1982. She received her Bachelor (Hons.) and Master (Hons.) degrees in Engineering from Rajasthan University, Jaipur, and Bhagwant University, Ajmer. She earned her Doctorate (Ph.D.) in Engineering from Bikaner Technical University. In 2006, she joined Govt. Engineering College Ajmer as a full-time Assistant Professor in the Department of Computer Science and Engineering. She has published numerous research papers in reputed journals and conferences. Her research interests include the Internet of Things (IoT), vehicular ad hoc networks (VANETs), and flying ad hoc networks (FANETs).

Dr. Deepak Gupta was born in 1978. He received his bachelor's and master's degrees in engineering from Jai Narain Vyas Engineering University (MBM College), Jodhpur, and Bhagwant University, Ajmer. He earned his Doctorate (Ph.D.) from Bikaner Technical University. He has been serving as an Assistant Professor in the Department of Computer Science and Engineering since 2006. He has published extensively in reputed journals and conferences, guided several master's theses, and delivered expert talks in WSN, vehicular and flying ad hoc networks, UAV to UAV communication.