Avinash Singh, 2026, 14:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Trust Based Routing Security against Sybil Attacker in FANET

Avinash Singh[1], Dr. Ankur Pandey[2]
[1]PhD Scholar, Dept. of CSE, LNCT University, Bhopal, M.P, India
[2]Associate Professor, Dept. of CSE, LNCT University, Bhopal, M.P, India

Abstract- FANET UAVs temporarily connect to other UAVs to transfer data. UAVs have limited memory and capability. In dynamic networks, UAV routing and packet transfer pose security issues. UAVs are subject to assaults and have variable speeds. FANET attacks vary. The malicious nodes isolation or Syble attacker is a packet-dropping assault that steals other nodes' unique identity (ID) and exploits it for network attacks. This paper provided two modules: attacker confirmation and detection and prevention. FANET's first Route and Data Security for Hostile Behaviour Prevention (RDSBP) method for Sybil attacker. Implement a base station device behavior analysis route security mechanism to detect this type of malicious conduct. The attacker node alters the routing table to choose a bogus path and diverts the route by altering the routing packet's next hop address. The main purpose of RDSPB is to identify the attacker. Comparing RDSBP to LOAD and LPAR, innovative security solution performs better. The attacker detection and prevention approach calculates UAV trust based on network function in the second module. The Trust & Energy Aware Secure Routing (TEASR) solution isolates FANET Sybil malicious nodes. Due of its limited energy, UAVs cannot replace batteries instantly. Attackers created retransmission potential, affecting energy. The attacker targets many real UAVs. Novel TEASR outperforms secure and trusted AODV. Secure AODV outperforms Trusted AODV and pure AODV routing. RDSBP and TEASR have the highest PDR and use less energy while routing.

Keywords: Energy, Sybil Attacker, Routing, RDSBP, TEASR, FANET

I. INTRODUCTION

The Flying Ad Hoc Network (FANET) is a dynamic network where UAVs interact and share information [1][2]. UAVs don't have to transfer data, but the network needs field data to respond. This flexibility streamlines data management and improves network responsiveness. It allows FANETs to adapt to changing operational conditions and optimize performance. Every FANET UAV is fast and has enough memory to store data [3]. UAVs use batteries, therefore efficient power use extends communications [4] [5]. Attackers and inadequate processing capacity are network issues [6]. Figure 1 illustrates UAV communication. S UAV provides data to D UAV via intermediate UAVs. Intermediate UAVs just collect data from the transmitter and send it to the network receiver.

Bandwidth concerns can be solved, but network attackers' nefarious conduct makes detection difficult. Dropping packets during routing is the goal of blackhole, wormhole, and Sybil attackers [7] [8]. FANET communicates mostly via energy. All UAVs need energy [4] [5]. ECH UAVs have a fixed battery capacity and need energy to move, send, receive, and sense neighbours to forward data packets. Every attacker affects the energy source. After establishing a route, attackers drop or fail to forward data packets to the destination, rather than starting harmful actions. FANET routing protocols convey data from sender to recipient since they are not in range [9][10]. These routing methods must be secure to enable reliable communication. Encryption, authentication, and anomaly detection reduce network threats and protect data transmission. Intermediate UAVs are critical.

The security scheme detects the attacker and blocks the Sybil attacker's malicious infection from the network in this research. Trust & Energy Aware Secure Routing (TEASR) calculates the trust factor while routing. The trust factor depends on data forwarding and dropping. Sybil attackers impersonate real UAVs and commit crimes. To stop the attacker, UAV behaviour history is crucial. Before stopping a node, check its past and present trust calculation. If the past and present behavior is

normal, the node is real; otherwise, it may be an attacker or infected. High network packet drops required extra energy for sending and receiving data packets. FANET routing using TEASR is reliable. By limiting data transmission to valid nodes, this technique improves network security and energy efficiency. TEASR adapts to changing threats and maintains aerial vehicle communication by analysing behaviour patterns. Route and Data Security for Hostile Behaviour Prevention (RDSBP) method for Sybil attacker to calculate trust factor and improve routing performance. The RDSBP monitors, controls, generates alerts, and filters packets for the entire network. The flying device calls the AODV routing packet and broadcasts it to the network to convey data to the receiver or base station. As soon as it detects a modification, the base station blocks the modifier node and discards the modified packet from the network. This proactive strategy protects data and secures communication. The base station logs these instances for study, improving network security protocols.

II. ATTACKS IN FANET

The role of UAVs in FANET is to collect information and transfer it either to the base station or to a satellite. This capability enhances real-time data analysis and decision-making processes, particularly in remote or inaccessible areas. As technology advances, the integration of UAVs with other communication systems will likely improve their efficiency and coverage. The use of collected information is important for taking action or only delivering to the destination for investigation and research purposes. Attackers harm the network because they conceal their misbehavior from genuine UAVs during data transfer after connection establishment [7][8]. The active attacker and passive attacker are of two types of attack in FANET [7][8].

Active Attackers

The malevolent UAVs are not singular in the network; instead, multiple UAVs can also be active in engaging in misbehaviour. The active attackers do not openly perform malicious functions; instead, they participate in routing clandestinely, and after establishing a connection, they begin dropping data. Their coordinated efforts complicate detection, as the malicious transmissions easily mask legitimate traffic. Consequently, it becomes increasingly challenging for security protocols to differentiate between normal operations and harmful activities within the network. These packet-dropping attackers, such as Sybil attackers, wormhole attackers, and blackhole attackers are dropped valuable data during the transfer between the source and destination [7][8]. Similar to flooding, these attackers do not participate in routing; instead, they directly initiate unwanted packet flooding in the network to consume bandwidth and the processing capabilities of UAVs. The DoS attacker and selfish node attacker are responsible for these types of malicious activities [8]. These disruptive tactics hinder efficient communication and compromise the integrity of the network. As a result, it becomes crucial to implement robust security measures to mitigate the impact of such threats and ensure reliable data transmission.

Passive Attackers

Passive attacks in FANET (Flying Ad Hoc Networks) are security threats where an attacker intercepts or monitors data transmissions without actively interfering with the network's operations. Unlike active attacks, passive attacks do not alter the contents of data or disrupt communication but focus on unauthorized data collection and eavesdropping. Eavesdropping is the passive attack that listen to the communication between UAVs (Unmanned Aerial Vehicles) to capture sensitive information such as location, flight paths, or mission details. Attackers analyze the pattern, frequency, and size of transmitted data to gather intelligence about network activities, identities, or operational relationships is done by traffic analysis attack. Attackers continuously observe network traffic to collect metadata, usage habits, or detect key events without altering the data flow is the monitoring attacker behavior.

III. LITERATURE SURVEY

Previous work gives knowledge about security from threats and improves vehicular communication. In this section discussing earlier VANET security work.

Xianfeng Li et al. [11] invented LB-OPAR routing. This approach chooses pathways based on network traffic, duration, and length. This SDN portion doesn't route traffic like OPAR. Linear programming (LP) optimization can solve SDN-based cooperative UAV routing problems. The optimization model considers network length, duration, and traffic. The path has the shortest link lifetime. Paths last longer since this problem reduces length and burden. The key problem of research is lowering PDR at constant speed and lacking UAV location information relative to others.

V. Chandrasekar et al. [12] suggested a fitness function that includes metrics like anchor node hops, ToA distance estimate error, and transmission delay. Due to their enormous coverage, current methods may struggle to produce correct data in vast aquatic ecosystems like seas and oceans. Water level and pressure oscillations complicate under-water sensor networks, requiring comprehensive examination. In response, sensor network designers recommend using machine learning and pseudo coding to create prediction models that can handle these complexities. Lack of example for trust value computations is the primary issue. TOPCM, proposed by W. Buksh et al. [13], is trust-oriented. First is the Peer-to-Peer Trust Evaluation Module, then the Decision-Maker Module. TOPCM isolates hostile nodes by analysing their trustworthiness, speeding packet transmission. Nodes with trust values below the threshold are malicious and added to the malicious list. Only trustworthy nodes should be in the dynamic network for reliable data transfer, thus if its trust value above the threshold, it is trustworthy. The biggest downside of research is lacking trust value calculation for malicious nodes and normal nodes table. Infection of malicious nodes is not stated.

C. Hutchins et al. [14] construct offline FANET IDSs for fast threat detection and accurate categorization. These IDSs can detect new threats in real time but need more data before making a conclusion. This contrasts with delayed IDSs, which need a fixed information window to decide. SAR applications require speedy threat classification to protect important systems. Interestingly, no offline IDS systems met this SAR criteria. The author of [15][16] are also contribute in the field of security to improve routing performance.

IV. SECURITY APPROACH FOR SYBIL ATTACKER DETECTION AND PREVENTION.

In this section mention the two modules for attacker detection and prevention. Route and Data Security for Hostile Behavior Prevention (RDSBP) method for Sybil attacker. The Trust & Energy Aware Secure Routing (TEASR) solution isolates FANET Sybil malicious nodes.

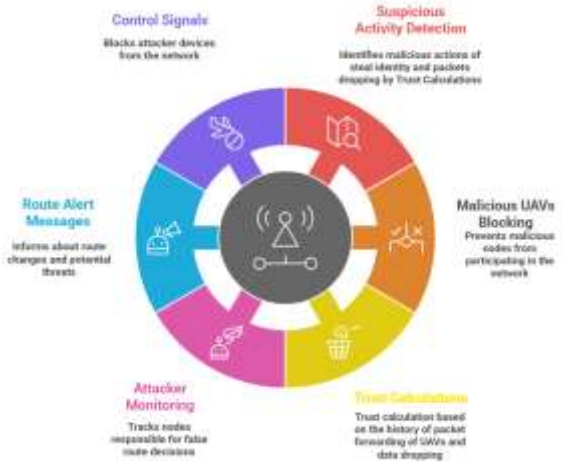

Figure 1 Security Scheme Action Against Sybil Attacker.

Required steps of Sybil Attacker Detection and prevention are as follows:

1. Initialize Trust Values: Assign an initial trust score to each node in the network.
2. Monitor Node Behaviour: Continuously observe the actions and interactions of all nodes.
3. Collect Interaction Data: Record successful and failed interactions between nodes.
4. Evaluate Interaction Outcomes: Analyze the results of node interactions to adjust trust values.
5. Update Trust Scores: Increase trust for successful, honest interactions; decrease for failures or suspicious actions.
6. Identify Anomalies: Flag nodes with abnormally low trust scores or rapid trust fluctuations.

7. Assess Social Connections: Check for nodes with unusually high connectivity or identical behavior patterns, which are common Sybil characteristics.
8. Cross-verify Trust Reports: Compare trust evaluations from multiple independent nodes to spot inconsistencies.
9. Apply Thresholds: Mark nodes as potential Sybil attackers if their trust score falls below a defined threshold.
10. Isolate or Limit Suspicious Nodes: Restrict network access or privileges for identified Sybil nodes to prevent further damage.

The RDSBP monitors, controls, generates alerts, and filters packets for the entire network. The flying device calls the AODV routing packet and broadcasts it into the network to convey data to the receiver or base station. As soon as it detects a modification, the base station blocks the modifier node and discards the modified packet from the network. The base station watches the attacker node, which diverts or makes fraudulent routing decisions. To divert the route, the attacker node modifies the routing table and updates the next hop address field in the routing packet. The procedure section involves deploying the network and using input parameters to establish secure and energy-aware TEASR routing. The proposed algorithm step detects the sybil attacker using direct and indirect trust-based methods and provides safe, energy-efficient data transfer. Finally, specify all necessary output parameters to analyze TEASR routing results in terms of throughput and end to end delay. The less packet dropping is normal in network because the reason is common congestion or collision happened in the network.

V. RESULT ANALYSIS

In this section measure the performance of novel RDSBP and TEASR are compared with previous approaches for attacker detection and prevention.

End to End Delay Analysis

Table 1 summarizes every approach's end-to end delay performance analysis. When compared to the earlier Secure AODV, Trust AODV, and AODV routing protocols in FANET, the suggested TEASR performs better. Packet loss or excessive traffic brought on by additional network load are the primary causes of delays. Receivers are waiting at the destination end because the attacker's goal is to drop the data packets. TEASR is displaying 0.04 ms less delay in the scenario with 20 UAVs, and this number is nearly identical in other node density scenarios as well. The innovative method can both improve speed and secure routing.

Table-1: End to End Delay Analysis

Number of nodes	End to End Delay (ms)			
	AODV	Trust AODV	Secure AODV	TEASR
20	0.21	0.18	0.16	0.12
40	0.23	0.2	0.18	0.14
60	0.24	0.22	0.19	0.15
80	0.28	0.24	0.2	0.17
100	0.29	0.25	0.22	0.19

Throughput Analysis

Throughput performance analysis is mentioned in table 2. The performance of LOAD and LPAR is poor but RDSP showing better performance. Sybil malevolent nodes' routing misbehavior lowers packet reception and throughput. Throughput performance is lowest with LOAD, slightly improved with LPAR, and best with RDSBP. The suggested RDSBP has better throughput due to reliable link setup. A new security strategy manages Sybil attacker-affected routing performance, improving performance. Table 2 gives through performance details.

Table-2: Throughput Analysis

Speed	Routing Protocol		
	LAOD	LPAR	RDSBP
10	5.95	6.46	7.23
20	5.73	6.64	7.23
40	4.96	6.45	6.73
60	4.54	5.99	6.33

Data Drop Analysis

The Sybil attacker is a routing layer attack that drops data packets by generating numerous phony identities in the dynamic network. A routing attacker

diverts data packets to unrecognized UAVs or drops them at the attacker node, disrupting data receipt. LOAD, LPAR, and RDSBP data drop percentages are shown in table 3. The decline in LOAD at 60 m/s is about 50%. LPAR dropped less than LOAD, whereas RDSBP dropped 35%. Drop percentages show that this reduction hurts routing performance. The new security method eliminates the attacker's drop percentage, eliminating their presence in FANET. Table 3 shows data lowering performance in exact numbers.

Table-3: Data Drop Analysis

Speed	Protocol		
	LAOD	LPAR	RDSBP
10	36.39	27.67	16.47
20	42.89	31.05	22.68
40	46.74	35.71	24.6
60	50.47	41.38	34.21

VI. CONCLUSION

FANET UAVs share data with other UAVs or base stations. Malicious UAVs just discard data packets. The innovative RDSBP technique improves routing and network security. This dynamic technique streamlines data collecting and allows real-time analysis and decision-making. In critical situations, UAVs increase response times and situational awareness in such networks. Network performance is affected by malicious UAVs. Sybil attackers steal UAV identities to drop data, making them the worst. This paper proposes FANET sybil attacker RDSBP security. The main purpose of RDSBP is to identify the attacker. Network integrity and fleet communication depend on this identity verification method. The suggested system uses advanced behavior analysis to strengthen FANETs against misleading tactics. The second Trust & Energy Aware Secure Routing approach (TEASR) calculates the trust factor during the routing and improve routing performance. Comparing RDSBP to LOAD and LPAR, the novel security method performs better. The suggested RDSBP improved PDR by 5% and throughput by 20% above LPAR. The overhead performance of RDSBP is 20% better than LOAD and LPAR. Minimum 5% improvement in delay and hop-count. This breakthrough builds trust in the network, making all nodes' operations safer.

REFERENCES

1. O. Ceviz, S. Sen and P. Sadioglu, "A Survey of Security in UAVs and FANETs: Issues, Threats, Analysis of Attacks, and Solutions," in IEEE Communications Surveys & Tutorials, vol. 27, no. 5, pp. 3227-3265, Oct. 2025.
2. Santosh Kumar Amol Vasudeva Manu Sood, "Security Issues in the Routing Protocols of Flying Ad Hoc Networks," International Conference on Innovative Computing and Communications, 2023.
3. Kashish Khullar, Ishu Malhotra, Anupam Kumar, "Decentralized and Secure Communication Architecture for FANETs using Blockchain, Procedia Computer Science Vol. 173, pp. 158-170, 2020.
4. G. Soni, A. Singh Kaurav, R. Verma, A. Manhar, J. P. Singh Mathur and A. C. Patak, "Design and Develop Hybrid Multipath Routing Approach for Proficient Energy Consumption in FANET," 2025 IEEE 5th International Conference on ICT in Business Industry & Government (ICTBIG), pp. 1-7, 2025.
5. K. Chandravanshi, G. Soni and D. K. Mishra, "Design and Analysis of an Energy-Efficient Load Balancing and Bandwidth Aware Adaptive Multipath N-Channel Routing Approach in MANET," in IEEE Access, vol. 10, pp. 110003-110025, 2022.
6. J. Kundu, S. Alam, J. C. Das, A. Dey and D. de, "Trust-Based Flying Ad Hoc Network: A Survey," in IEEE Access, vol. 12, pp. 99258-99281, 2024.
7. G. Soni, K, Chandravanshi, N. Kunhare, M. Bhargava "Data Receiving Analysis for Secure Routing from Blackhole Attack in a Spontaneous Network Using Blockchain Method," Proceedings of International Conference on Network Security and Blockchain Technology. ICNSBT 2023. Lecture Notes in Networks and Systems, vol 738, pp. 513-524, 2023.
8. Ashish Chourey, Sitesh Kumar Sinha, "Analysis of packets dropping attackers, security schemes

and routing protocols in VANET," CRC Press, pp. 1-11, 2024.

9. J. Carvajal-Rodríguez, W. Moposita, C. Tipantuñna, L. F. Urquiza and D. Vega-Sanchez, "FANET Networks: Analysis of Routing Protocols," 2024 IEEE Eighth Ecuador Technical Chapters Meeting (ETCM), Cuenca, Ecuador, 2024, pp. 1-6.
10. J. Jiang, G. Han, "Routing Protocols for Unmanned Aerial Vehicles. IEEE Communication Magine, Vol. 56, pp. 58–63, 2018.
11. Xianfeng Li, Haoran Sun, "Prediction-based Reactive-Greedy Routing Protocol for Flying Ad Hoc Networks," Wireless Network, Vol. 31, pp. 2893–2907, 2025.
12. V. Chandrasekar, V. Shanmugavalli, T. Mahesh, R. Shashikumar, N. Borah 4, V. V. Kumar, S. Guluwadi, "Secure Malicious Node Detection in Flying Ad-hoc Networks using Enhanced AODV Algorithm," Scientific repot, 2024.
13. W. Buksh, Y. Guo, S. Iqbal, K. Naseer Qureshi, J. Lloret, "Drust-oriented Peered Customized Mechanism for Malicious Nodes Isolation for Flying Ad Hoc Networks, "Transactions on Emerging Telecommunication Technologies, Wiley, 2022.
14. C. Hutchins, L. Aniello, E. Gerding, Halak, A Flying Ad-Hoc Network Dataset for Early Time Series Classification of Grey Hole Attacks, Sci Data 12, 1431, 2025.
15. Shikha Gupta, Neetu Sharma, "SCFS-securing Flying Ad hoc Network using Cluster-based trusted Fuzzy Scheme," Complex & Intelligent Systems, Vol. 10, pp. 3743–3762, 2024.
16. Charles Hutchins, Leonardo Aniello, Enrico Gerding & Basel Halak, "A Flying Ad-hoc Network dataset for Early Time Series Classification of Grey hole Attacks," Scientific Data, Volume 12, Article No. 1431, 2025.