Chhatrapani Gautam, 2026, 14:4
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

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

A Novel Flooding based Heuristic Security Approach for Vampire Attack in FANET

Chhatrapani Gautam, Dr. Ankur Pandey Associate Professor
Computer Science & Engineering, LNCT University
Bhopal (M.P.)

Abstract- FANET Flying ad hoc networks are a promising technology and have enormous potential to be working in critical situations in farming, land investigation, habitat monitoring, smart homes, and many more scenarios. One of the major challenge in FANET facing today is security. In this paper, we propose a flooding identification-based heuristic scheme against vampire attackers in FANET. These types of attacks flood the network with unnecessary packets, consuming bandwidth and affecting data delivery due to high energy consumption. The main aim is to visualize the effect of a vampire attack on the network and identify the UAVs that are affecting its performance. The heuristic security scheme checks the profile of each UAV in the network, and if an attacker is identified as one of the UAV or UAVs that flooding unnecessary packets and the security scheme has blocked that attacker's malicious functioning. The functioning of heuristic based flooding scheme has blocked the performance of the attacker. The attacker aim is only to disturb the normal communication among the UAVs in FANET. The performance of a network is measured on the basis of performance metrics such as routing load, throughput, and end to end delay. The simulation results indicate that the performance is the same for both normal routing and the heuristic scheme, demonstrating that the security scheme is effective and shows better performance. This effectiveness highlights the robustness of the security scheme for vampire attackers in maintaining network integrity, even in the face of potential threats.

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

I. INTRODUCTION

The Flying Ad Hoc Network (FANET) is a dynamic network where the UAVs communicate and share information [1][2]. UAVs do not need to communicate data but the network needs field data to respond. This flexibility leads to more efficient data management and improved network responsiveness. This allows FANETs to adapt to fluctuating operational conditions and optimize performance. Each UAV in FANET is quick and has sufficient memory to store data [3]. UAVs use batteries, therefore optimal power utilization prolongs communications [4] [5]. Network problems include attackers and lack of processing capacity [6].

Figure 1 displays UAV communication. UAV-1 transmits data to UAV-2 through cellular base station. IUAVs only gather data from the transmitter and forward it to the network receiver.

Bandwidth issues can be rectified; however, identification is difficult because of the malevolent nature of network intruders. Blackhole, wormhole and Sybil attacker [7] [8] aim to drop packets during routing. FANET communicates mostly by energy. All UAVs require energy [4] [5]. ECH UAVs have a set battery capacity, and need energy to manoeuvre, transmit, receive, and sense neighbours to transfer data packets. Every attacker has an effect on the energy source [7][8]. Once a path is established, malicious operations don't start but drop or fail to forward data packets to the destination.

FANET routing techniques are used to transport data from sender to receiver if they are not in range [9][10]. Routing methods should be secure to provide dependable communication. Encryption, authentication and anomaly detection are used to

decrease network threats and protect data transfer. Intermediate UAVs are important.

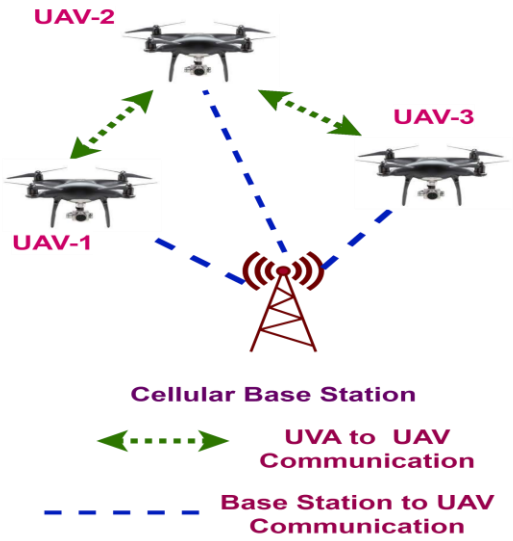

Figure 1 Example of FANET

The security scheme detects the attacker and blocks the vampire attacker's malicious infection from the network in this research. The flooding based calculates the unwanted flooding in the network. The trust factor depends on data forwarding and dropping. Vampire attackers impersonate real UAVs and commit crimes. Proposed approach adapts to changing threats and maintains aerial vehicle communication by analysing behaviour patterns. 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 vampire attacker 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

Flying Ad hoc networks are vulnerable to security attacks [10][11][12] due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. Basically, attacks are classified as active attacks and passive attacks.

1. Passive Attacks

The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. The Attacks against privacy is passive in nature.

Attacks against Privacy

The main privacy problem is not that FANET enable the collection of information. In fact, much information from sensor networks could probably be collected through direct site surveillance. Rather, UAV networks intensify the privacy problem because they make large volumes of information easily available through remote access. Hence, adversaries need not be physically present to maintain surveillance. They can gather information at low-risk in anonymous manner [13][14][15]. Some of the more common attacks against UAVs privacy are:

Monitor and Eavesdropping

This is the most common attack to privacy. By snooping to the data, the adversary could easily discover the communication contents. When the traffic conveys the control information about the UAV network configuration, which contains potentially more detailed information than accessible through the location server, the eavesdropping can act effectively against the privacy protection.

2. Active Attacks

The unauthorized attackers' monitors, listens to and modifies the data stream in the communication channel are known as active attack. The following attacks are active in nature.

Routing Attacks in Networks

The attacks which act on the network layer are called routing attacks [5]. The following are the attacks that happen while routing the messages.

Vampire Attacker

Vampire Attacker is produced by the unintentional failure of nodes or malicious action. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of Vampire attacks in different layers might be performed. At physical layer the vampire attacks could be jamming and tampering, at link layer, collision, exhaustion and unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and de-synchronization. The mechanisms to prevent vampire attacks include payment for network resources, pushback, strong authentication and identification of traffic [6]. Our work is on to protect the network from that attack

Blackhole Attacker

A blackhole attacker is a malicious node that falsely advertises itself as having the shortest or best route to the destination. When surrounding nodes forward their data through this attacker, it absorbs or drops all incoming packets instead of relaying them, effectively creating a "blackhole" in the network. This type of attack can severely disrupt communication reliability, compromise data integrity, and degrade network performance in FANETs, which are already challenged by high mobility and dynamic topology.

III. LITERATURE SURVEY

Previous work gives knowledge about security from threats and improves vehicular communication. In this section discussing work in security by different authors:

V. Chandrasekar et al. [16]. Proposed a new method for creating a threat detection tool that can effectively identify and isolate illegal nodes in FANETs. The security and dependability of the network may be enhanced using this technique. The suggested secure AODV approach is crucial for this endeavour since it successfully identifies and isolates rogue nodes to eliminate false data from the network. By reducing packet loss and routing overhead while simultaneously increasing throughput, the proposed method enhances the security performance of FANET when compared to conventional techniques like TAODV and AODV. Integrating trust models that rely on either direct or indirect reliability offers an extra line of defense against potential attacks on susceptible transient nodes. Our proposed threat detection technique may significantly improve the timely detection and prevention of security breaches in real-time, strengthening the security and dependability of FANET operations. The paper's drawback is that the Sybil attacker's many IDs are not subtracted. Analysis of attacker infection is lacking.

A critical agreement procedure in FANET was proposed by Ashish et al. [17]. The protocol combines symmetric and asymmetric encryption with Elliptic Curve Cryptography (ECC) to ensure a secure key exchange between Unmanned Aerial Vehicles (UAVs). The protocol aims to minimize the computational and communication expenses associated with key exchange while preserving the security and reliability of sent keys. The proposed protocol consists of the following steps: shared key computation, decryption, key exchange, initialization key creation, and key verification. The actions we take are as follows: Unmanned Aerial Vehicles (UAVs) generate public and private keys and configure their parameters throughout the key exchange process. Each Unmanned Aerial Vehicle (UAV) generates a session key at random and encrypts it using the public key of the other UAV. Each Unmanned Aerial Vehicle (UAV) sends the encrypted session key to the other UAV. Each Unmanned Aerial Vehicle (UAV) receives the encrypted session key, which it decrypts using its private key. The decrypted session key is then used by both UAVs to calculate the shared secret key. Using a message authentication code, both unmanned aerial vehicles (UAVs) verify the shared secret key's integrity. Research's primary flaw is that it only compares methods that are currently in use. In order to quickly and accurately identify malicious nodes.

Shikha Gupta et al. [18] introduced a novel technique called SCSF that integrates fuzzy logic-based trust assessment for both cluster and individual nodes. Part of the research involves putting security

measures in place that increase the probability that each node will conclude their trust. SCSF is addressing the hitherto unknown topic of trust reconfiguration to enhance the network's legitimacy. This involves updating the trust of nodes who were unable to prove their trust because of network or runtime problems, as was covered in earlier trust analysis techniques. A new method and a trust reconfiguration model must be developed in order to increase the network's dependability. This approach will address the issue of nodes whose dependability cannot be verified due to network or other runtime issues. A likelihood is assigned based on their reliability history.

A lightweight anomaly detection system (LADS) that use behavioural analysis to identify rogue nodes was proposed by Ashraf Abdelhamid et al. [19]. These nodes are identified, eliminated from the network, and classified as malicious. The main objective of this work is to introduce an anomaly detection method for detecting black hole assaults, namely one based on a support vector machine (SVM). This detection method looks for anomalies in network data by examining node behaviour. A "black hole" attack targets nodes that exhibit particular behavioural characteristics that distinguish them from other nodes. Our lightweight detection method accurately detects these properties.

Nishant I. Mowla et al. [20] , focus on first jamming attack detection technique for FANETs was developed by They created a method to identify the UAV client groups that make the biggest contributions to the overall model because every UAV node trains its local model in a very varied environment. They establish the lower and upper bounds of the trust measure for any UAV user group using the Dempster-Shafer theory. In order to prioritize UAV client groups for the federated averaging computation, they developed a method. After that, they may determine which UAV client groups are most appropriate for the computation. FANET can identify on-device jamming attempts while keeping a minimal connection to the central system because to federated learning. The primary disadvantage of research is that data accuracy depends on successful data delivery. For jammer detection, disregard fuzzy rules. The effectiveness of the route was not assessed.

IV. SECURITY APPROACH FOR VAMPIRE ATTACKER DETECTION AND PREVENTION.

In a Flying Ad Hoc Network (FANET), a vampire attack is a security threat where malicious nodes drain the network's energy by generating or forwarding unnecessary packets. A heuristic-based security scheme can help detect and mitigate such attacks. Here are the typical steps involved:

Node Behavior Monitoring
Continuously monitor all nodes for packet forwarding and energy consumption patterns.

Suspicious Node Isolation
Temporarily isolate nodes identified as potential vampires from the network. Prevent them from forwarding or generating packets.

Figure 1 shows the procedure to capture information of routing misbehavior of vampire attacker through security scheme.

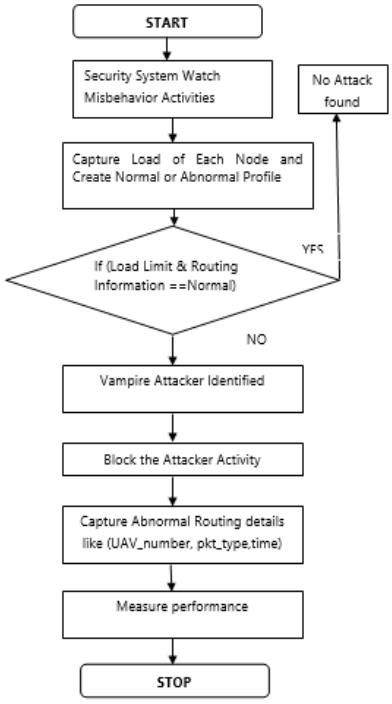

Figure 2 Procedure of Finding Attacker

Reputation Management
Assign and update reputation scores to each node based on their behavior. Lower scores for suspicious activity; restore scores for consistent normal behavior. Notify to UAVs when a potential vampire attacker is detected.

Recovery and Reintegration
Re-evaluate isolated nodes after a cool down period. Reinstate nodes if their behavior returns to normal, or permanently blacklist if malicious activity persists. Refine heuristics based on new attack patterns or network changes to adapt to evolving threats.

The attacker information is capture by security scheme and blocks the activities of attacker in network. The abnormal attacker behavior is identified by the node number, packet type and time. Infection is evaluated by the heavy flooding of messages in network.

Detecting and preventing vampire attackers in Flying Ad Hoc Networks (FANETs) is crucial due to the severe impact these attacks have on network longevity and reliability. Vampire attackers drain the network's energy by generating excessive, unnecessary data packets or by misrouting traffic, causing rapid depletion of node battery power. To detect such threats, heuristic-based schemes monitor key network parameters such as packet transmission rates, energy consumption, and routing patterns. Nodes exhibiting abnormal behaviors, like unusually high packet forwarding or accelerated energy usage, are flagged as suspicious. Preventive measures include isolating and blacklisting malicious nodes, employing reputation systems to track node reliability, and dynamically updating security rules to adapt to new attack strategies. Together, these proactive steps help maintain the energy efficiency and secure operation of FANETs.

To stop the attacker, UAV behaviour history is crucial. Before stopping a node, check its behaviour in network. If the past and present behaviour is normal, the UAV 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 heuristic based flooding security is reliable. By limiting data transmission to valid nodes, this technique improves network security and energy efficiency.

V. RESULT ANALYSIS

In this section measure the performance of Vampire attacker, TAODV, SAODV and novel HAPV are compared with previous approaches for attacker detection and prevention.

1. Routing Overhead Analysis
The table 1 presents a comparative routing analysis of Vampire, TAODV, SAODV, and HAPV using mean and median values. Among the protocols, Vampire shows the highest mean (38.82) and median (39.57), indicating the lowest performance. TAODV demonstrates moderate performance, while SAODV shows improved efficiency with lower values. HAPV achieves the lowest mean (15.42) and median (16.32), highlighting its superior and more consistent routing performance. The close proximity between mean and median values for all protocols indicates stable and low-skew data distribution, confirming the reliability of the results.

Table-1: Routing Overhead Analysis

Protocol Type	Routing Analysis	
	Mean	Median
Vampire	38.82	39.57
TAODV	22.34	22.02
SAODV	17.58	17
HAPV	15.42	16.32

2. Throughput Analysis
The table 2presents a comparative throughput analysis of the four routing protocols—Vampire, TAODV, SAODV, and HAPV—based on mean and median values. Vampire exhibits significantly lower throughput, with a mean of 10.8 and a median of 12, indicating poor performance. TAODV shows a considerable improvement, achieving a mean of 98 and a median of 97. SAODV further enhances throughput performance with higher values of 124 (mean) and 125 (median). Among all protocols, HAPV demonstrates the best performance, recording the highest mean (142.2) and median

(142), which indicates superior efficiency and reliability in data transmission. The close alignment between mean and median values across all protocols suggests stable and consistent throughput behavior.

Table 2: Throughput (Mbps) Vs Protocol

Protocol Type	Throughput Analysis	
	Mean	Median
Vampire	10.8	12
TAODV	98	97
SAODV	124	125
HAPV	142.2	142

3. End to End Delay Analysis

The table presents a comparative delay analysis of the routing protocols—Vampire, TAODV, SAODV, and HAPV—using mean and median values. Vampire records the highest delay, with a mean of 0.372 and a median of 0.38, indicating the least efficient performance. TAODV shows improved performance with reduced delay values, while SAODV further minimizes delay, reflecting better optimization. Among all protocols, HAPV achieves the lowest mean (0.196) and median (0.20), demonstrating the most efficient and reliable performance in terms of delay reduction. The close proximity between mean and median values across all protocols indicates stable and consistent delay characteristics with minimal variation.

Table-3: Network Delay (ms) Vs Protocol

Protocol Type	Delay Analysis	
	Mean	Median
Vampire	0.372	0.38
TAODV	0.274	0.26
SAODV	0.226	0.23
HAPV	0.196	0.2

VI. Conclusion

The novel security approach enhances routing in FANET and network security. UAVs share data to other UAVs or base stations. Malicious UAVs only release data packets. This dynamic approach enables for data collecting and real time analysis and decision making. UAVs enhance response speeds and situational awareness in such networks under critical scenarios. The performance of the network is affected by malicious UAVs. Vampire attackers are the worst as they affect the battery power of UAVs and dropped data. In this study we present a heuristic security strategy for the vampire attacker. Flooding based heuristic technique is mostly used to detect the attacker. This form of identity verification is key to network integrity and fleet communication. The proposed approach employs advanced behaviour analysis to improve the robustness of FANETs against deceptive strategies. The second attacker target not only the routing performance but also try to target the. Comparison of novel HAPV with Vampire attack, TAODV, and SAODV and innovative security approach perform better. Proposed increase in throughput. It reduces delay in network as well as reduces overhead. This achievement establishes trust in the network and makes it safer for all UAVs to operate.

REFERENCES

1. Ali, A. 2001.Macroeconomic variables as common pervasive risk factors and the empirical content of the Arbitrage Pricing Theory. Journal of Empirical finance, 5(3): 221–240.
2. O.K Sahingoz, "Routing Protocols in flying Ad-hoc Networks (FANETs): Concepts and Challenges," Journal of Intelligent Robot System, Vol. (74), pp.513–527, 2014.
3. G. Soni, M. K. Jhariya, K. Chandravanshi and D. Tomar, "A Multipath Location based Hybrid DMR Protocol in MANET," 2020 3rd International Conference on Emerging Technologies in Computer Engineering: Machine Learning and Internet of Things (ICETCE), pp. 191-196, 2020.
4. D. Anwekar and S. Phulre, "Analysis of Congestion Control Techniques to Improve QoS and Frequent Communication in FANET," 2023 World Conference on Communication & Computing (WCONF), RAIPUR, India, 2023, pp. 1-7.
5. K. Chandravanshi, G. Soni, D.K. Mishra, "Design and Analysis of an Energy-Efficient Load Balancing and Bandwidth Aware Adaptive

Multipath N-Channel Routing Approach in MANET," IEEE Access, Vol. 10, pp. 110003 – 110025, 2022.
6. J. Jiang, G. Han, "Routing Protocols for Unmanned Aerial Vehicles. IEEE Communication Magine, Vol. 56, pp. 58–63, 2018.
7. M.F Khan, Kok-Lim Alvi Yau, Rafidah Md Noor, Muhammad Ali Imran, "Routing Schemes in FANETs: A Survey," Sensors, MDPI, pp. 1-33, 2019.
8. Ceviz, O., Sadioglu, P., Sen, S.. "Analysis of Routing Attacks in FANETs," Ad Hoc Networks and Tools for IT. ADHOCNETS TridentCom 2021. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 428. Springer, 2022.
9. S. Ren, D. Li, Q. Hu, Y. Liu and J. Liu, "An Improved Security OLSR Protocol against Black Hole Attack based on FANET," 2022 13th Asian Control Conference (ASCC), Jeju, Korea, Republic of, 2022, pp. 383-388.
10. Altaweel, H. Mukkath and I. Kamel, "GPS Spoofing Attacks in FANETs: A Systematic Literature Review," in IEEE Access, vol. 11, pp. 55233-55280, 2023.
11. G. Soni, K. Chandravanshi, D. Deoskar, S. Parashar and R. Thakur, "Design and Develop an Efficient Load Balancing Approach with AOMDV Routing in 7G-FANET," 2024 IEEE 4th International Conference on ICT in Business Industry & Government (ICTBIG), Indore, India, , pp. 1-7, 2024.
12. Kai-Yun Tsao, Thomas Girdler, Vassilios G. Vassilakis , "A Survey of Cyber Security Threats and Solutions for UAV Communications and Flying Ad-Hoc Networks," Ad Hoc Networks, Vol. 133, pp. 1-36, 1 August 2022.
13. A.S Kaurav, S. R Dutt, "Detection and prevention from different attacks in VANET: A Survey," Journal of Physics: Conference Series, Volume 2040, International Conference on Physics and Energy 2021 (ICPAE 2021), Kancheepuram, India, 2021.
14. Sayani Sarkar, Sima Shafaei, Trishtanya S. Jones, Michael W. Totaro, "Secure Communication in Drone Networks: A Comprehensive Survey of Lightweight Encryption and Key Management Techniques", Drones, vol.9, no.8, pp.583, 2025.
15. 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, 2024.
16. V. Chandrasekar, V. Shanmugavalli, T. R. Mahesh, R. Shashikumar, Naiwrita Borah, V.Vinoth Kumar, Suresh Guluwadi, "Secure Malicious Node Detection in Fying Ad Hoc Networks using Enhanced AODV Algorithm," Journal of scientific reports, 03 April 2024.
17. Ashish Singh Parihar, Amitesh Pandey, "Proposing A Novel Key Agreement Protocol for Flying Ad-Hoc," 2023 Fifteenth International Conference on Contemporary Computing (IC3 2023), pp. 711-715, 2023.
18. Shikha Gupta, Neetu Sharma, "SCFS-Securing Flying Ad hoc Network using Cluster-based Trusted Fuzzy Scheme," Complex & Intelligent System, Springer, 7 January 2024.
19. Ashraf Abdelhamid, Mahmoud Said Elsayed, Anca D. Jurcut, Marianne A. Azer, "A Lightweight Anomaly Detection System for Black Hole Attack," Electronics, MDPI, pp. 1-18, 2023.
20. Nishat I Mowla, Nguyen H. Tran, Inshil Doh, Kijoon Chae, "Federated Learning-Based Cognitive Detection of Jamming Attack in Flying Ad-Hoc Network, IEEE Access, 201.