SvedbergOpen
DISSEMINATION OF KNOWLEDGE
International Journal of Artificial Intelligence and Machine Learning
Publisher's Home Page: https://www.svedbergopen.com/
Research Paper Open Access

A Heuristic Approach for Prevention Vampire Attack in Flying Ad-hoc Networks (HAPV)

Chhatrapani Gautam[1*], Ankur Pandey[2]

[1,2] Computer Science & Engineering, LNCT University Bhopal (M.P.).
E-mail: acpg.77@gmail.com

Abstract: Unnamed Aerial Vehicles (UAVs) can freely move in the limited area to capture the desired information and also forward that information to other UAVs or base stations in Flying Ad hoc Networks (FANETs). UAVs come in various heavy models, each designed to meet specific requirements. A single UAV is sufficient for the survey of a particular area, but multiple UAVs are required for the better handling of large amounts of data and data sharing. Routing plays an important role in establishing the connection and data forwarding between the sender and receiver. FANET networks are highly dynamic and UAVs have sufficient storage capacity. The role of the vampire attacker is to consume the UAV's capabilities, energy resources, and memory, which degrades the network's performance. This research presents a heuristic solution for the prevention of vampire attacks (HAPV), functioning as a distributed, energy-efficient security mechanism integrated into the routing process of flying ad hoc networks (FANET). The system constantly checks how UAVs are acting based on local observations and uses conditional heuristics to find and stop vampire attack activities without affecting routing protocol constraints. In the proposed HAPV mechanism calculate energy utilization, hop-count which uses to detect behaviour of attacker node. During the initialization phase, each UAV gives all of its neighbouring UAVs the highest trust rating, believing that they would behave well and that there is no blacklist. In the next step, focus on energy consumption, the requirements for route establishment, and the needs for connection establishment and data forwarding. The performance of the novel HAPV approach is compared with the vampire attacker, TAODV, and SAODV across various UAV density scenarios. Reliable communication reduces delay and overhead in the network and improves the PDR and throughput performance of HAPV.

Keywords: Energy, FANET, HAPV, Security, Routing, Vampire Attacker.

1. Introduction

Flying Ad hoc Networks (FANETs) have emerged as specialized from of mobile ad hoc networks (MANETs), where multiple unmanned aerial vehicles (UAVs) cooperate to accomplish mission-oriented task such as surveillance, disaster management, border monitoring, precision agriculture and military reconnaissance. Due to their characteristic such as high mobility, limited UAV onboard energy resources and dynamic topology, FANETs require efficient highly vulnerable to various security threats [20-23].

Among these threats, vampire attacks pose a particular insider form of resource exhaustion. Unlike conventional denial-of-service (DoS) attacks, they adhere to protocol standards and difficult to detection because it does not rely on malformed packets or obvious malicious behavior. Instead the attacker deliberately crafts packets or routing paths which maximize energy consumption across the network, forcing nodes to forward packets along unnecessarily long routes or repeatedly retransmit data. In flying ad hoc network UAVs operate with constraints battery capacity, such attacks can drastically exhaust utilized energy of UAVs and reduce network lifetime, degrade performance and compromise mission-critical operations [24-26].

In the existing security solution primary focus on routing and data dropping attacks such as blackhole, grayhole, wormhole, sybil and jamming etc. However, limited attention has been given to resource consumption or energy-drain attack like vampire attacks, especially in highly dynamic aerial vehicle environments. Traditional attack detection system of wireless sensor network is not directly applicable to FANET due to high mobility patterns, different radio range and topology changes. Therefore, there is a critical need for lightweight, adaptive and mobility

aware detection and prevention mechanism specifically design for FANET environments.
To address this research issue, this article proposes heuristic approach for prevention of vampire attack in flying ad hoc network (HAPV). The proposed model introduces a heuristic-based decision framework that monitors routing behavior, evaluates hop-count deviations and analyzes abnormal energy consumption patterns. It uses threshold-based heuristic rules and energy-aware metrics to identify suspicious behavior in routing activity and data transmission that indicate potential vampire behavior. Instead of relying solely on heavy encryption algorithm or complex machine learning models, the heuristic design ensures low computational overhead, making it suitable for real-time UAV deployment.
The core objective of HAPV is not only to detect vampire attack but also prevent energy-draining routing patterns before they significantly affect network stability. The proposed HAPV mechanism integrates energy monitoring, adaptive route validation and balanced traffic distribution to preserve residual UAV energy to extend overall network lifetime. Furthermore, it improve performance of packet delivery ratio, throughput and reduce end-to-end delay and overhead by blocking or eliminating malicious node and routes [27-29].
The article is organized into five sections. Section I presents an introduction to flying ad hoc networks (FANETs), outlining their key characteristics, applications and inherent limitation. It also discuss various security threats and attacks threats and attacks that effect network performance and reliability. Section II provide a detailed review of existing approaches designed to detect and mitigate different types of attacks in FANETs. This section critically examines current methodologies and highlights their strength and limitation. Section III explain the proposed heuristics approach for preventing vampire attacks in FANETs termed HAPV. It elaborates on the operational framework of proposed model. Section IV describes the simulation setup and parameters used to evaluated the proposed mechanism. It presents a comparative performance analysis based on key metrics such as packet delivery ratio, throughput, routing overhead, residual energy and end-to-end delay. Finally, Section V concludes the work and discuss future research directions. This section emphasizes the impact and advantages of the HAPV mechanism compared to traditional security approaches, highlight its effectiveness in enhancing network performance and energy efficiency.

2. Literature Review

This section present a comprehensive study of traditional and recent-trend of security approaches used to detect and prevent FANETs from various attacks, along with an analysis of their performance and effectiveness.
V. Chandrasekar et al. [1] examine malicious node attacks in FANETs and propose a secure ad hoc on-demand distance vector (AODV) algorithm to enhance network security. It addresses the distributed denial –f service (DDoS) threat posed by sybil attack, in which a single adversary generates multiple fake identities to overwhelm a victim node with excessive data packets. Their study also highlights the need for development of standardized protocols, architecture and regulatory frameworks tailored specifically to FANET environments.
O. Ceviz et al. [2] was proposed a novel intrusion detection framework for FANETs, termed federated learning-based intrusion detection system (FL-IDS). Considering the inherently distributed nature of FANET data, a cooperative and decentralized architecture is more appropriate than centralized solutions, However, direct data sharing among UAV nodes can introduce significant privacy and security concerns, especially in mission-critical applications.

M. Nayfeh et al. [3] study presents a detection framework for GPS spoofing attacks which classify them into two categories static and dynamic. A dedicated datasets was generated for both attack scenarios by collecting GPS signal attributes-including, latitude, longitude and timestamp from authentic as well as spoofed experimental setup.
L.,M. Da Silva et al.[4] in this article they introduce the intrusion detection system (IDS) to identify both flight anomalies and network-based attack within UAV swarms. The network attack detection module adopts a supervised learning approach, leveraging conventional machine learning algorithm which includes decision tree (DT), random forest (RF), Gaussian naïve bayes (NB) and multi-layer perceptron (MLP) to detect attacks such as blackhole, grayhole and vampire attack.
Zhang et al. [5] proposed a many-to-one certificate-less authentication protocol for the Internet of Drone (IoD), asserting that it provides resistance against forgery attacks while operating efficiently under constrained bandwidth conditions. The protocol use the computational Diffie-Hellman problem (CDHP) for secure public–private key exchange among participating entities. The scheme exhibits certain limitations including vulnerability to denial-of-service (DoS) and insider attack.
Tian et al. [6] and Viet et al. [7] Presented a certificate-less public key cryptography-based aggregate signature authentication protocol. Their work focuses on enabling secure communication among small-scale drones operating at low altitude to deliver various services. To strength the security of the certificate-less aggregates signature scheme, they incorporated mathematical lemmas along with the RSA cryptographic algorithm, However, the proposed approach demonstrates limited efficiency during message broadcasting among multiple participants.
Pu and Li [8] Proposed a physical unclonable function (PUF) to authenticate and validate communications between drones and ground stations. Their study argues that conventional cryptographic technique alone may be inadequate for safeguarding sensitive data transmission, whereas PUF based mechanism can enhance

communication security.

Saeed U. et al. [9] proposed elliptic curve cryptography based authentication scheme for securing IoD-FANET. The security analysis and performance evaluation of the proposed scheme have been thoroughly addressed. The demonstrated of proposed scheme achieves superior security, efficiency and overall effectiveness. It is well suited for deployment in Internet of Drones (IoD) applications, particular for infrastructure surveillance in post-disaster scenarios such as floods or earthquake.

G. Soni et al. [10] was proposed a delay estimated rate-based control mechanism to enhance UAV-to-UAV communication in FANET. They use efficient load balancing AOMDV scheme monitor which adjust dynamically rate and minimize network delay. This adaptive strategy mitigates congestion risks and ensures balanced traffic distribution across network links. Leveraging the ultra-fast communication capabilities of FANET network, the proposed approach significantly improves reliability and overall network performance.

Martin Andreoni Lopez, et al. [11] Provides a comprehensive survey of security challenges in UAV swarm communication over wireless mesh networks, emphasizing that highly dynamic and infrastructure-less nature of flying ad hoc networks (FANETs) makes them vulnerable to multi-layer attacks such as jamming, spoofing and routing manipulation. In this article they systematically classify these threats across network layers and highlights key limitation including energy constraints, high mobility and unreliable connectivity.

Hutchins, et al. [12] Introduces a novel dataset (FAN-GHETS24) specifically designed for early detection of grayhole attacks in flying ad hoc networks (FANETs), where UAVs communicate via multi-hop routing and are vulnerable to packet dropping attacks that degrade network performance the dataset is generated through simulation of UAV interactions and processed using anonymization and feature engineering techniques to support machine learning models. The proposed mechanism provides an important benchmark resource for future research on secure and energy efficient UAV network defense mechanism.

Priya S. Gosavi and B. M. Patil [13] was provides an introductory analysis of vampire attacks in wireless ad hoc sensor networks, highlighting that these attacks are a form of energy draining denial-of-service where malicious nodes exploit routing protocols to consume excessive battery power without disrupting communication, which making them difficult to detect and highly damaging over time. In this article authors discuss how such attacks can be easily launched using protocol-complaint message and propose a mitigation approach compared against existing routing protocols like Beacon vector routing, showing improved detection and prevention performance.

Sudha, et al. [14] Present a deep learning based method to detect vampire attacks in wireless sensor networks, where attackers drain node energy, the model combines multiple techniques like LSTM, RNN and GRU with fuzzy logic to improve attack detection accuracy and achieve over 95% accuracy in simulation and although it is effective, the approach may be computationally complex and mainly tested in simulated environment.

Kirik, et al. [15] Present an ISAC (integrated sensing and communication) based beam alignment method for HAP-based 6G flying ad-hoc networks, addressing the challenge of maintaining reliable communication links between highly mobile high altitude platforms. It proposes a two-step beam alignment approach. The physical layer optimization and may require advanced hardware support, it offers an effective solution for improving connectivity and reliability in next generation FANET systems.

Tang, et al. [16] was proposed an adaptive virtual tunnel routing (AVTR) protocol for flying ad hoc networks to address challenges like dynamic topology, sparse connectivity and boundary effects, where nodes at network edges suffer from poor routing decisions. In this method reduce unnecessary transmissions and routing overhead, while incorporating factors such as link quality, residual energy and hop count for optimal next-hop selection and simulation result show improved performance in terms of delay, packet delivery ratio and efficiency compared to existing protocols.

Sen, et al. [17] was proposed a lightweight authentication scheme for UAV-based FANETs using physical unclonable functions (PUFs) to generate secure, unique devices identities. The approach protects against attacks like impersonation and reply while keeping communication overhead low. Result show improved security and efficiency, though scalability and real-world deployment areas for future work.

Prabhakar, et al. [18] Present as AI-enabled routing and MAC protocol for flying ad hoc networks (FANETs) that combines fully Echoed Q-routing with adaptive directional MAC to improve communication efficiency in highly dynamic UAV environments. The approach uses reinforcement learning to optimize routing decisions and directional transmission to reduce interface and collisions. Results show enhanced packet delivery, lowr delay and better network stability compared to traditional methods.

Srinivasan [19] Proposes an innovative cross-layer defense mechanism to detect and mitigate blackhole and wormhole attacks in wireless ad hoc networks. The existing approach integrate routing, MAC and trust-based parameters to improve attack detection accuracy and network resilience.

3. Proposed HAPV

The propose Heuristic Approach is use for Prevention of Vampire Attack (HAPV), a lightweight energy-aware and mobility-aware safe routing framework for preventing routing-layer vampire attacks in Flying Ad-Hoc Networks (FANETs). A FANET is a network of Unmanned Aerial Vehicles (UAVs) that interact with each other without the need for permanent infrastructure. The constant movement of UAVs causes frequent changes in the topology, the

quality of the connection, the interactions with neighbors, and quick energy consumption. These characteristics make the traditional routing systems susceptible to malicious nodes which intentionally modify the packet forwarding or route selection to force the legitimate UAVs to make unnecessary transmissions and receptions. Relevance of vampire attacks is specifically in the sense that the objective is to drain node resources gradually, not necessarily to cause sudden packet interruption. Thus, HAPV incorporates mobility awareness, analysis of forwarding behavior, monitoring of energy consumption, estimation of route quality and heuristic path selection in one preventive mechanism.

First, each UAV periodically collects information about its neighboring UAVs, such as residual energy, hop count, link lifetime, received signal strength, packet forwarding rate, transmission distance, route progress and the observed energy consumption. So instead of only having a shortest path routing, HAPV has a dynamic neighbor and route information table. The data is refreshed whenever there are substantial changes in mobility or link quality. The purpose is to distinguish between a suspect route whose excessive energy consumption is caused by abnormal forwarding behavior and a normal high-cost route due to FANET mobility. This distinction is important as in a highly dynamic aerial network, large energy consumption itself should not be treated as a vampire attack.

Then each forwarding UAV is assigned a Vampire suspicion score. The score includes normalized energy-depletion rate, forwarding-path stretch, routing behavior, packet forwarding frequency, route-progress ratio, and link stability. A general formulation is as follows:

$$VS_i = w_e\widehat{E_{d,\iota}} + w_s\widehat{S_\iota} + w_f\widehat{F_\iota} + w_r\left(1-\hat{R}_\iota\right) + w_l\left(1-\hat{L}_\iota\right) \quad \text{.....(1)}$$

where VS_i is the Vampire suspicion score of UAV i, $\widehat{E_{d,\iota}}$, is its normalized energy-depletion rate, $\widehat{S_\iota}$ is route-stretch behavior, $\widehat{F_\iota}$ is abnormal forwarding frequency, $\widehat{R_\iota}$ is normalized route-progress efficiency, and $\widehat{L_\iota}$ is link stability. The coefficients w_e, w_s, w_f, w_r and w_l specify the relative importance of the related features and fulfill:

$$w_e + w_s + w_f + w_r + w_l = 1$$

A UAV is not considered malevolent only because it has a high score in one parameter. In contrast, HAPV adopts a heuristic judgment method based on a threshold:

$$VS_i \geq \tau v \Rightarrow U_i = Suspicious \quad \text{.....(2)}$$

where τv is the dynamically set threshold for Vampire detection. This decreases the probability of false detection of genuine UAVs as attackers due to temporary high mobility, bad wireless circumstances, or typical changes in energy consumption.

HAPV is built around a heuristic secure route-selection function. When the UAVs are detected as suspicious, the routes passing through them are punished or excluded according to the level of suspicion. HAPV creates a composite route cost for each candidate route P_k based on energy consumption, hop count, link stability, residual energy, mobility stability, route progress and Vampire-risk score:

$$HC(P_k) = w_1(1-\widehat{E_k}) + w_2\widehat{H_k} + w_3(1-\widehat{L_k}) + w_4\widehat{M_k} + w_5\widehat{V_k} + w_6(1-\widehat{R_k} \quad \text{.....(3)}$$

where $HC(P_k)$ is the heuristic cost of route P_k, $\widehat{E_k}$ is the normalized residual energy, $\widehat{H_k}$ is the normalized hop count, $\widehat{L_k}$ is the link stability, $\widehat{M_k}$ is the mobility instability, $\widehat{V_k}$ is the aggregated Vampire-risk score, and $\widehat{R_k}$ is the route-progress efficiency. Choose the path with the smallest heuristic value:

$$P^* = arg \min_{P_k \epsilon P_{safe}} HC(P_k) \quad \text{.....(4)}$$

where P_{safe} is the set of paths that satisfy the security and energy restrictions.

A main characteristic of HAPV is the detection of route-stretch. A Vampire node can try to influence the forwarding so that packets take longer than necessary paths, increasing the amount of transmissions and receptions conducted by genuine UAVs. Prior Vampire-attack research has identified path-length manipulation and packet forwarding behavior as important attack techniques. HAPV compares the actual forwarding distance or hop count with the projected route cost. The route-stretch factor can be expressed as:

$$RS(P) = \frac{H_{actual}(P)}{H_{optimal}(P)} \quad \text{.....(5)}$$

where $H_{actual}(P)$ is the hop count of the observed path and $H_{optimal}(P)$ is the projected minimal viable hop count. An increase in $RS(P)$, in particular when coupled with excessive energy consumption and poor route progress, increases the Vampire suspicion score.

HAPV also provides a tool to detect energy depletion. Each UAV estimates its energy usage in the coming observation intervals:

$$EDR_i = \frac{E_i(t) - E_i(t+\Delta t)}{\Delta t} \quad \text{.....(6)}$$

where EDR_i is the energy-depletion rate of UAV $i, E_i(t)$ is the residual energy of UAV i at time t, and Δt is the monitoring period. An abnormally high energy depletion in abrupt or constant manner in comparison to other forwarding nodes may be a sign of malicious routing behavior. However, the value is assessed in conjunction with route stretch, packet forwarding frequency, route progress and link circumstances to not confuse real high

workload with an attack.

HAPV also includes mobility-aware prevention to better fit FANETs. High speed of UAVs may result in natural short link lifespan and frequent route reconstruction. Thus, the framework analyzes connection stability and projected link lifetime before penalizing a route. The heuristic cost is larger for a candidate path with a highly mobile UAV with a very short anticipated lifetime of the link. This enables HAPV to prevent two problems simultaneously, namely selecting routes sensitive to regular mobility driven failures and selecting routes influenced by Vampire nodes.

If a suspicious UAV surpasses the predefined risk threshold, HAPV does not immediately terminate the entire communication session. Instead it does local route isolation and alternative-path selection. " The suspicious node is assigned with a high routing penalty and the nearby UAVs try to create a path that bypasses the suspicious node. This method reduces control overhead and ensures that a single rogue UAV does not frequently force full network-wide route discovery. If numerous neighboring UAVs report similar suspicious behavior, the risk level of the node is increased and the node can be temporarily ignored in the further decisions of route selection.

The framework also keeps a table of Vampire-risk history. HAPV does not make a routing choice on a single observation, but keeps the recent behavior of UAVs and produces a time-weighted suspicion value. This prevents false positives due to transient congestion, rapid movement and ephemeral communication deterioration. A simple historical score is defined as:

$$V_i(t) = \gamma V_i(t-1) + (1-\gamma) VS_i(t) \ldots\ldots\ldots (7)$$

where $V_i(t)$ is the current accumulated Vampire-risk value, $VS_i(t)$ is the freshly observed suspicion score, and $0 \leq \gamma \leq 1$ regulates the contribution of the history behavior.

Hence, the whole HAPV operation consists of neighbor discovery, network state monitoring, energy depletion measurement, route stretch analysis, mobility and link stability estimation, vampire suspicion calculation, heuristic route evaluation, suspicious node isolation, secure route selection and continuous route monitoring. Under typical conditions, HAPV chooses energy efficient and stable routes. When anomalous forwarding behavior is detected, the heuristic process raises the risk score of the related node. If the score is higher than the adaptive threshold, the node is avoided and an alternative route is generated. In this way, the network can continue to communicate without the suspect node continually consuming the energy of the surrounding UAVs.

4. Result Discussion

In this section represent outcome of proposed HAPV and existing FANET security system. The network is deploy using the network simulator-2 and uses the processing tool to analyze performance on the bases of throughput, packet delivery ratio, delay and energy utilization to validate the HAPV system adoptability for FANET communication.

4.1 Simulation Parameters & Results

Simulation parameters are considered for research is mentioned in table 2. Here the area of simulation, number of UAV nodes and rest of all the parameters are mentioned. For this research Cygwin software is used to install NS-2 simulator and run the simulation of proposed approach on windows. Performance of different approaches is evaluated in different UAVs density scenario in FANET. The simulation area is 1000m*1000m is considered, the number of BS is 4 used for the data collection and UAVS can also exchange data with each other. Rest of tall parameters is mentioned in table 1.

Table 1: Simulation Parameters

Simulation Tool	Network Simulator-2.31
Simulation Area	1000m X 1000m
Number of Nodes	20, 40, 60, 80, 100
Network Type	FANET
Base Stations (BS)	Four
Number of attacker	Varied from two
Node Movement	Random Uniform Distribution
Node Speed	0-20 m/n
Traffic Type	CBR, UDP
Packet Size	512 Byte
Network Protocol	AODV
Attack Type	Vampire
Security Technique	TAODV, SAODV, HAPV
Energy -(initial) -discharge rate	 100 (j) 0.01 to 1.5 (j)/ per seconds

Channel Type	Wireless Phy
Media Control	IEEE 802.11b
Radio Range	550m^2
Simulation Time	100s

4.2 Energy Consumption Analysis

Energy is the primary source of communication, and all UAVs in the network require a sufficient amount of battery capacity. In this figure 1, measure the performance of the Vampire attacker, TAODV, SAODV, and the proposed HAPV in FANET. A vampire attacker is always harmful for the network because the work of the attacker is to consume resources intentionally and drop the data packets. The main target of a vampire attacker is battery power and tries to deplete the battery power of all the connected UAVs quickly and that will affect the routing performance. The energy consumption in the HAPV approach is lowest and the rest of the approaches consume high energy during routing. In 100 UAVs, the energy consumption in novel HAPV is only 16J and it is nearly 4.5J less as compared to SAODV. The energy consumption means low battery life and degrades network lifetime. The proposed HAPV approach is able to enhance network lifetime.

The Vampire assault, TAODV, SAODV, and new HAPV are all mentioned in Table 2, which contains a study of their respective energy usage. The higher energy usage indicates that the connectivity between the UAVs is not strong, which, in turn, indicates that the power or energy that is needed for retransmission is completely wasted.

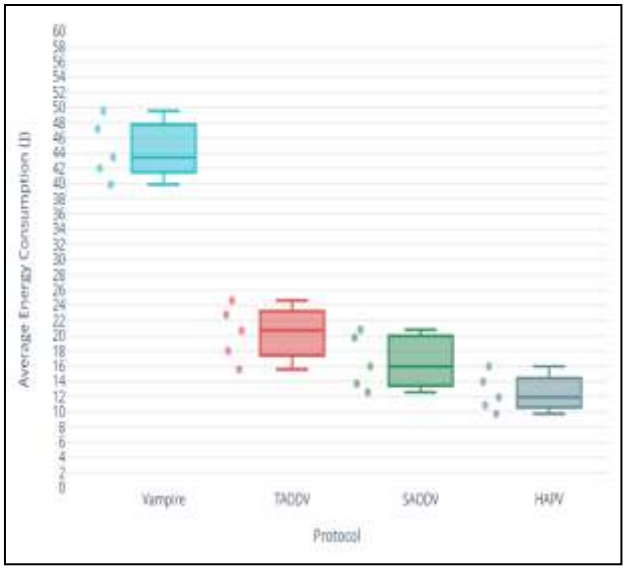

Fig 1: Energy Consumption Analysis

The UAVs in the network are powered mostly by battery power, which is the primary source of power. While the performance of each of the ways is examined in a variety of UAV densities, the proposed approach is the only one that was found to waste less energy throughout the routing process.

Table 2: Energy Consumption in joule(J)

Protocol Type	Number of Flying Nodes				
	20	40	60	80	100
Vampire	39.87	41.99	43.43	47.17	49.52
TAODV	15.57	18.03	20.7	22.76	24.63
SAODV	12.57	13.7	15.96	19.73	20.79
HAPV	9.73	10.87	11.92	13.94	15.97

4.3 Remaining Energy Analysis

The basic means of communication is energy, and all unmanned aerial vehicles (UAVs) that are part of the network

need to have a significant level of battery capacity. If their battery life is insufficient, it significantly reduces the efficiency of their operations.

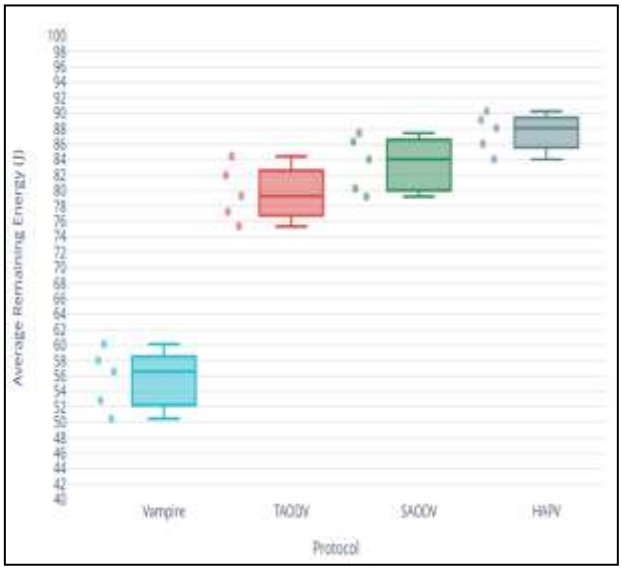

Fig 2: Residual Energy Analysis

To keep communication and operating efficiency consistent throughout the fleet, it is essential to ensure that energy management is optimized whenever possible. Determine the residual energy performance of the vampire attacker, TAODV, SAODV, and the suggested HAPV in FANET. Figure 2 represents the results of this measurement. To have a detrimental impact on the performance of routing, the primary objective of a vampire attacker is to rapidly deplete the battery power of all connected unmanned aerial vehicles (UAVs). As a result of less flooding of routing packets and less data loss, the HAPV technique is able to keep the greatest amount of remaining energy, whereas the other alternatives have a lower amount of remaining energy. Regarding the scenario involving twenty unmanned aerial vehicles (UAVs), the innovative HAPV has just 90 J of residual energy, which is roughly 3.9 J higher than the SAODV version. The high remaining energy extends both the battery's power and the network's lifetime.
The remaining energy analysis of Vampire attack, TAODV, SAODV and novel HAPV is mentioned in table 3. Higher remaining energy consumption shows the strong connectivity between the UAVs and that means fruitful utilization of power or energy used in routing of data in FANET. Battery power is the primary source for operates the UAVs in network. The performance of all the approaches is evaluated in different UAVs density but only proposed approach utilizes higher energy in packet sending and receiving.

Table 3: Remaining Energy in Joule

Protocol Type	Number of Flying Nodes				
	20	40	60	80	100
Vampire	60.13	58.01	56.57	52.83	50.48
TAODV	84.43	81.97	79.3	77.24	75.37
SAODV	87.43	86.3	84.04	80.27	79.21
HAPV	90.27	89.13	88.08	86.06	84.03

Conclusion and Future Work

In a dynamic network like FANET, connection establishment and data forwarding are not very easy, as in wireless networks. All the UAVs are very fast devices and continuously moving in the particular area to store the information in the form of images and videos. In the FANET, UAVs are the multipurpose devices and they can carry a limited amount of weight for transfer or any other purpose. UAVs need the support of routing for transfer between the sender and the receiver. Routing protocol selection is very important because UAVs are very fast-moving devices as compared to other mobile devices. The vampire attacker role is to consume the limited bandwidth and attack the battery power to disrupt the routing performance. In this research, we propose a novel HAPV scheme to improve

the energy utilization and packet receiving. HAPV incorporates a heuristic-driven energy monitoring system and secure routing decision-making. The framework functions in a decentralized fashion; it does not necessitate comprehensive network awareness. The rapid movement of UAVs heightens the likelihood of mutual untrustworthiness, as UAVs regularly alter their routes and no entity is accountable for overseeing the UAVs to ascertain the trustworthiness of UAVs for dependable communication. In the communication process, vampire attackers deplete network resources and alter routing by exhausting the capacity of other UAV devices. The HAPV approach incorporates the heuristic trust value (HTV), calculated from each neighbouring node based on energy depletion, route length, and packet forwarding behaviour. The performance of HAPV is compared with the Vampire attacker, TAODV, and SAODV in 20, 40, 60, 80, and 100 UAV density scenarios. In all the scenarios the performance of HAPV is better. The average remaining energy is 4 joules more as compared to all approaches in FANET. It means UAVs can utilize this energy for further communication. The HAPV scheme is able to utilize the energy consumption and block the vampire attacker's malicious activities in different node density scenarios. The novel approach improves routing performance and provides secure communication among the UAVs.

This research proposed the security scheme for a vampire attacker in FANET. This type of attacker is the active attacker and is very harmful for the network. In the future, try to propose the approach for multiple different attackers to secure routing performance and control flooding and data dropping in dynamic networks. The attackers will be detected by the machine learning (ML) model and the record of multiple attackers will be maintained separately. The prevention scheme role is to block the attacker infection in the network and provide the secure routing.

References

1. Chandrasekar, V., Shanmugavalli, V., Mahesh, T.R. et al. (2024), Secure malicious node detection in flying ad-hoc networks using enhanced AODV algorithm. Sci Rep 14, 7818.
2. Ozlem Ceviz, Pinar Sadioglu, Sevil Sen, Vassilios G. Vassilakis, (2025) “A Novel Federated Learning-Based IDS for Enhancing UAVs Privacy and Security, arXiv:2312.04135.
3. M. Nayfeh, Y. Li, K. Al Shamaileh, V. Devabhaktuni, N. Kaabouch, (2023) Machine learning modeling of gps features with applications to UAV location spoofing detection and classification, Computers & Security 126, 103085.
4. L. M. Da Silva, I. G. Ferr˜ao, C. Dezan, D. Espes, K. R. Branco, (2023) Anomaly-based intrusion detection system for in-flight and network security in UAV swarm, in: International Conference on Unmanned Aircraft Systems (ICUAS), IEEE, pp. 812–819.
5. L. Zhang, B. Qin, Q. Wu, and F. Zhang, (2010), Efcient many-to-one authentication with certificate-less aggregate signatures, Comput. Netw., vol. 54, no. 14, pp. 24822491.
6. Y. Tian, J. Yuan, and H. Song, (2019) Efcient privacy-preserving authentication framework for edge-assisted Internet of Drones,'' J. Inf. Secur. Appl., vol. 48, Art. no. 102354. 1799.
7. N. O. Viet, N. Quoc, and W. Ogata, (2015), Certificate-less aggregate signature protocols with improved security,'' IEICE Trans. Fundamentals Electron., Commun. Comput. Sci., vol. 98, no. 1, pp. 92-99.
8. C. Pu and Y. Li, (2020), Lightweight authentication protocol for unmanned aerial vehicles using physical unclonable function and chaotic system,'' in Proc. IEEE Int. Symp. Local Metrop. Area Netw. (LANMAN, Orlando, FL, USA, pp. 1-6.
9. S. U. Jan, I. A. Abbasi, F. Algarni and A. S. Khan, (2022), A Verifiably Secure ECC Based Authentication Scheme for Securing IoD Using FANET, in IEEE Access, vol. 10, pp. 95321-95343.
10. G. Soni, K. Chandravanshi, D. Deoskar, S. Parashar and R. Thakur, (2024), Design and Develop an Efficient Load Balancing Approach with AOMDV Routing in 7G-FANET, IEEE 4th International Conference on ICT in Business Industry & Government (ICTBIG), Indore, India, pp. 1-7
11. Martin Andreoni Lopez, Michael Baddeley, Willian T. Lunardi, Anshul Pandey, Jean-Pierre Giacalone,(2021), Towards Secure Wireless Mesh Networks for UAV Swarm Connectivity: Current Threats, Research, and Opportunities, IEEE, arXiv:2108.13154
12. Hutchins, C., Aniello, L., Gerding, E. et al., (2025), A flying ad-hoc network dataset for early time series classification of grey hole attacks. Sci https://doi.org/10.1038/s41597-025-05560-1
13. Priya S. Gosavi, B. M. Patil, (2016), Vampire Attack: Draining Life from Wireless Ad –hoc Sensor Networks. International Journal of Computer Applications. 144, 9, 1-4. DOI=10.5120/ijca2016910424
14. Sudha, M., Arunachalam, R., Karthikayen, A. (2026), Fuzzy computation on ensemble deep network for the performance of vampire attack detection model in WSN. J. Wirel. Commun. Netw. https://doi.org/10.1186/s13638-025-02540-2
15. M. Kirik, L. Afeef and H. Arslan, (2025), An ISAC-Assisted Beam Alignment Design for HAP-Based 6G Flying Ad-Hoc Networks," in IEEE Open Journal of the Communications Society, vol. 6, pp. 5923-5939, doi: 10.1109/OJCOMS.2025.3586964.
16. H. Tang, P. Wang, D. Li, Y. Zhang and X. Chen, (2025), An Adaptive Virtual Tunnel Routing Protocol With Eliminating Boundary Effects for Flying Ad-Hoc Networks, in IEEE Internet of Things Journal, vol. 12, no. 16, pp. 34068-34085, doi: 10.1109/JIOT.2025.3577510.

17. Sen, M.A.; Al-Rubaye, S.; Tsourdos, A. (2025), Securing UAV Flying Ad Hoc Wireless Networks: Authentication Development for Robust Communications. Sensors, 25, 1194. https://doi.org/10.3390/s25041194
18. Prabhakar, P., Yokesh, V., Aruchamy, P. and Nanthakumar, S. (2025), Artificial Intelligence-Enabled Fully Echoed Q-Routing and Adaptive Directional Medium Access Control Protocol for Flying Ad-Hoc Networks. Int J Commun Syst, 38: e6138. https://doi.org/10.1002/dac.6138
19. Srinivasan, J. (2025), Innovative cross-layer defense mechanisms for blackhole and wormhole attacks in wireless ad-hoc networks. Sci Rep 15, 14747, https://doi.org/10.1038/s41598-025-97094-0
20. Bada, M. et al., (2021), A policy-based solution for the detection of colluding GPS-Spoofing attacks in FANETs. Transp. Res. Part A Policy Pract. 149, 300–318.
21. Gupta, P., Singh, B., & Shrivastava, Y. (2023). Theoretical and Experimental Prediction of Optimal Process Variables for Enhanced Metal Removal Rate during Turning on CNC Lathe. EVERGREEN – Joint Journal of Novel Carbon Resource Sciences & Green Asia Strategy, 10(2).
22. Namdev, M., Goyal, S. & Agarwal, R. (2021), An optimized communication scheme for energy efficient and secure flying ad-hoc network (FANET). Wirel. Pers. Commun. 120(2), 1291–1312.
23. Ravi Verma, Gaurav Soni, Sandeep Sahu, Kamlesh Chandrawanshi, (2023), Security Requirements, Issues, and Challenges in IoE" 1st Edition, CRC Press,
24. Gupta, P., Singh, B., & Shrivastava, Y. (2022). Robust Techniques for Signal Processing: A Comparative Study. EVERGREEN – Joint Journal of Novel Carbon Resource Sciences & Green Asia Strategy, 9(2), 404–411.
25. Usman, Q. et al., (2021), A reliable link-adaptive position-based routing protocol for flying ad hoc network. Mob. Netw. Appl. 26(4), 1801–1820.
26. A. K. Khare, A. Saxena, S. Suman, A. Shrivastava and K. Chandravanshi, (2025), Sybil Attack Detection and Prevention Using Dynamic Trust Mechanism in VANETs, *2025 IEEE 5th International Conference on ICT in Business Industry & Government (ICTBIG)*, Indore, Madhya Pradesh, India, India, 2025, pp. 1-8.
27. Sudha, M., Arunachalam, R., Karthikayen, A. (2026), Fuzzy computation on ensemble deep network for the performance of vampire attack detection model in WSN. *J Wireless Com Network*.
28. Rajesh Arunachalam, Erode Dhanapal Ruby Kanmani, (2024), Detection and mitigation of vampire attacks with secure routing in WSN using weighted RNN and optimal path selection, Computers & Security, Volume 145.
29. G. Soni, D. Saraswat, A. Jain, A. Manhar, K. Chandravanshi and L. K. Khanday, (2025), Cityscape: Blockchain - Based Real Estate Platform for Transparency and Fraud Minimization," *2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS)*, Indore, India, pp. 1-5