A Mamdani-Type Fuzzy Inference Framework for UAV Threat Detection and Countermeasure Deployment in FANETs

Jingping Guo
China People's Police University, Guangzhou, Guangdong, 510663, China.
E-mail: 18680555590@163.com

Keywords: flying ad hoc networks (FANETs), mamdani-type fuzzy inference system (MFIS), threat assessment, unmanned aerial vehicles (UAVs), UAV misbehaviour

Recieved: May 16, 2025

The proliferation of Unmanned Aerial Vehicles (UAVs) in both civilian and military spheres has raised substantial security issues, especially within volatile communication environments such as Flying Ad Hoc Networks (FANETs). To challenge of the problem of real-time detection and response to UAV misbehaviour, the research proposed a Mamdani-type Fuzzy Inference System (MFIS) for real-time classification and detection of threats and subsequent actions. The MFIS is designed to take in information from UAV behaviours dataset (1000 samples) was obtained from Kaggle, consisting of four main features: energy consumption, mobility pattern, packet transmission, and link stability. After pre-processing the dataset through Min-Max normalization for standardization and amid Principal Component Analysis (PCA) for dimension reduction, the MFIS developed produces less computational load while retaining vital behavioural characteristics of the datasets. The results demonstrate the ability for the MFIS to enhance communication reliability while reducing key issues with routing and communication delays significantly over traditional FMIS methods like the Efficient Honesty-based Detection Scheme (EH-DS). The results show that the framework is an effective method for utilizing real-time context in making energy-efficient decisions for real-time UAV threat response. The simulation results show a significant improvement in performance parameters, including to-end delay, routing overhead (packets), and packet delivery ratio, by 15-55% compared to previous methodologies. While this framework has many advantages in terms of performance, these results confirm that the proposed fuzzy logic framework enables adaptive, accurate, and energy-efficient threat mitigation in real-time UAV operations.

Povzetek: Članek predstavi Mamdani-jevski fuzzy inferenčni sistem za sprotno zaznavanje groženj in odzivanje v FANET omrežjih. Ob uporabi normalizacije, PCA in štirih vedenjskih značilk UAV model učinkovito loči kooperativne in zlonamerne drone ter izboljša zakasnitev, nadzorni promet in dostavo paketov.

1 Introduction

UAVs, commonly referred to as drones, have proliferated rapidly in both civilian and military activities due to their wide range of functions, cheaper prices, and quick missions [1]. In contrast, the wider availability and advanced functions of UAVs promote an incremental increase in security fears, especially regarding monitoring, smuggling, or even attack missions. There is thus increasing pressure for effective UAV systems that can analyse threats dynamically and recommend appropriate responses accordingly in a real-time manner [2]. Traditional rule-based systems have difficulty representing uncertainty and adapting to dynamic environments. As depicted in Figure 1, the fuzzy logic-based system adapts the decision-making of UAV countermeasures by interpreting ambiguous information to identify threats and recommend actions.

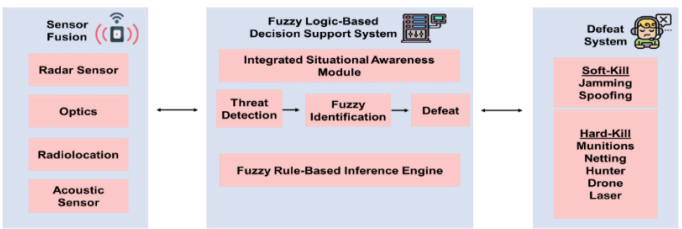

Figure 1: Decision support system using fuzzy logic

Figure 1 showed Decision Support System using Fuzzy Logic. A fuzzy logic-based decision support system (DSS) represents a responsive, flexible, and understandable manner of UAV threat evaluation and countermeasure selection [3]. The fuzzy DSS for UAV countermeasures takes in many input variables, including the key features [4]. The development of remote sensing and photogrammetry systems, especially in the use of UAVs, has provided efficient and high-resolution services for acquiring imagery of land. This research emphasizes how UAV data could be used to automatically detect and delineate land boundaries, which introduces improvement in the accuracy and reliability of cadastral updates [5].
Fuzzy logic-based decision-support systems have several benefits for the UAV countermeasures, but it has some limitations. The desire for expert guidance while developing rules and membership functions adds subjectivity and may limit the potential for the system to adjust to different threat circumstances [6]. The system is designed to enhance communication security in FANETs by identifying and mitigating potential threats. An MFIS classifies drones as cooperative or malicious based on their behavior. The performance of UAV target tracking was improved in [7]. To improve the accuracy of UAV trajectory prediction, Artificial Neural Networks (ANNs) characterize complex flight dynamics more effectively. The research creates a multi-layer ANN model to optimize UAV flight trajectories through uncertain and dynamic environments [8]. Additionally, fuzzy logic systems have no inherent learning functionality, and therefore cannot adjust to UAV technologies and tactics without constant updates [9].

1.1 Objective of the research

Existing UAV threat classification and detection systems struggle to operate effectively under uncertain and imprecise data conditions, limiting their real-time decision-making capabilities. The research aims to develop a robust fuzzy logic-based decision support system that classifies UAV behaviours and recommends adaptive countermeasures using sensor-derived behavioural indicators and optimized inference mechanisms.

1.2 Contribution of the research

- To propose a fuzzy logic-based decision support system using a multi-input fuzzy inference model that classifies UAV behaviour and supports real-time countermeasure selection.
- To utilize a UAV behavioural dataset comprising key threat-related features to simulate and evaluate UAV actions under normal and evasive conditions in security-sensitive zones.
- To implement Min-Max normalization for scaling sensor data and apply Principal Component Analysis (PCA) to extract dominant features, enhancing model accuracy and computational performance.
- To validate the proposed system against a benchmark model by conducting a comparative analysis using standard classification metrics to demonstrate improved decision quality under uncertain inputs.

1.3 System overview

The research's relevant work is outlined in Section 2, methodologies are covered in Section 3, findings are summarized in Section 4, and the work is concluded in Section 5.

2 Related works

To improve multicopper reliability under counter-UAV threats by proposing a modular autopilot system with backup control for trajectory tracking was proposed [10]. To introduce a fuzzy inference-based controller using image recognition from six map sectors. Results indicate enhanced autonomous navigation. However, the approach lacks practical deployment details, suggesting limitations in real-world testing and adaptability to diverse UAV environments. To predict energy consumption in low-cost UAVs using Artificial Intelligence (AI) algorithms to enhance efficiency was described [11]. To propose five models Random Forest (RF), Regression Tree (RT), Support Vector Machine (SVM), Artificial Neural Network (ANN), and Adaptive Neuro-Fuzzy Inference System (ANFIS) on an open quadcopter flight dataset. Results show RF performs best. Limitations include minimal consideration of weather impacts and diverse UAV configurations. To reduce computational demands in large-scale UAV swarm confrontations a fuzzy multi-agent reinforcement learning (FMARL) approach was described [12]. To model UAV interactions as a fuzzy game, assigning policies to abstract agents, not individuals. Results show reduced floating-point operations and storage needs. A key limitation is the potential loss of granularity during fuzzification and defuzzification processes.
A secure and adaptive AI control system for UAVs in dynamic environments was developed [13]. To propose a hybrid framework combining an enhanced Soft Actor-Critic (SAC) method with a Fuzzy Inference System (FIS), integrating expert knowledge for efficient learning. Results show effective real-time path planning and intruder tracking. Limitations include reliance on simulations and pending real-world validation. UAV performance in precision agriculture using fuzzy multi-

criteria decision-making (MCDM) approach was evaluated [14]. To suggest an integrated method combining Fuzzy-Weighted Zero-Inconsistency (FWZIC) and Fuzzy Decision by Opinion Score Method (FDOSM) to assess Unmanned Aerial Vehicles (UAVs) based on payload, endurance, and dimensions. Results show payload is most critical. Limitations include reliance on subjective expert input and scenario-specific criteria. Autonomous power monitoring in UAVs for power system stability was enhanced [15]. To recommend an onboard monitoring system using the Low Power Alarm and Battery (LPAB) status and forecasting method, with a fuzzy logic-based algorithm to estimate remaining flight time. Results show improved energy use and safe landings. Limitations include dependency on sensor accuracy and environmental variability.

Decision-making in UAV swarm confrontations using game theory was introduced [16]. To propose a dynamic non-zero-sum game model with concepts like relative advantage and advantage coefficient, solved using a multi-strategy fusion Particle Swarm Optimization (PSO) approach. Results confirm effectiveness via simulation. Limitations include reliance on simulation-based validation and possible challenges in real-time scalability. Modelling and evaluation methods for Cooperative Operation System-of-Systems (COSoS) involving manned aerial vehicles (MAVs) and UAVs were described [17]. To discuss standard framework-based and complex network-based modelling approaches, comparing their characteristics. Results summarize current effectiveness evaluation methods. Limitations include a lack of unified evaluation standards and challenges in real-world COSoS implementation. To improve UAV threat assessment in air defence using a dynamic fuzzy multi-attribute decision-making model [18]. To propose a 3D evaluation system—capability, opportunity, and intention combined with inverse Poisson-based time weighting and improved TOPSIS for threat prioritization. Results show enhanced accuracy and Limitations include complexity in real-time deployment and reliance on accurate intention estimation. Intrusion malware detection in UAVs by highlighting vulnerabilities in communication, software, and hardware systems are determined [19]. To present a taxonomy of detection methods using machine and deep learning algorithms, recent advances, and identify gaps. Results summarize current progress. Limitations include evolving threat complexity and limited real-time deployment evidence. Table 1 demonstrates the overall performance of previous work.

Table 1: Summary of the related work

References	Aim & Proposed Method	Results	Limitations
Mishra, and Palanisamy [10]	Improve multicopper reliability under counter-UAV threats via a modular autopilot system using a fuzzy inference-based controller with image recognition from six map sectors.	Enhanced autonomous navigation and trajectory tracking.	No practical deployment; limited real-world testing and adaptability.
Sarkar et al. [11]	Predict energy consumption in low-cost UAVs using AI models: Random Forest (RF), Regression Tree (RT), Support Vector Machine (SVM), Artificial Neural Network (ANN), and Adaptive Neuro-Fuzzy Inference System (ANFIS) on a quadcopter flight dataset.	RF achieved the best prediction accuracy.	Weather impacts and UAV variations are not fully addressed.
Hu et al. [12]	Reduce computational demands in UAV swarms using fuzzy multi-agent reinforcement learning (FMARL), modelling interactions via fuzzy game theory.	Lowered storage and floating-point operations while maintaining effective control.	Potential loss of detail due to fuzzification/defuzzification.
Xia et al. [13]	Develop a hybrid control system combining Soft Actor-Critic (SAC) and Fuzzy Inference System (FIS) for real-time path planning.	Effective path planning and intruder tracking.	Simulation-based; lacks real-world validation.
Jasim et al. [14]	Evaluate UAVs in precision agriculture using Fuzzy-Weighted Zero-Inconsistency (FWZIC) and Fuzzy Decision by Opinion Score Method (FDOSM).	Payload emerged as the most critical criterion.	Based on expert opinions; context-specific criteria.
Shcherban and Eremenko [15]	Enhance autonomous power monitoring for UAVs using LPAB and fuzzy logic to estimate remaining flight time.	Improved energy use and safer UAV landings.	Relies on sensor accuracy and environmental factors.
Wu et al. [16]	Use game theory and a non-zero-sum model with relative advantage coefficients and PSO for UAV swarm decision-making.	Model validated via simulation, showing effective outcomes.	Limited to simulation; scalability concerns.

Wang et al. [17]	MAV/UAV COSoS modelling using standard frameworks and complex networks and evaluate effectiveness.	Summarized modelling and evaluation strategies.	No unified standards; real-world implementation difficulties.
Niu et al. [18]	Improve UAV threat assessment using fuzzy multi-attribute decision-making with dynamic variable weights and enhanced TOPSIS.	Better threat prioritization in dynamic environments.	Complex real-time deployment; depends on accurate intention inputs.
Cai et al. [19]	Intrusion malware detection in UAVs; present taxonomy using ML and DL algorithms.	Comprehensive overview of current approaches and progress.	Rapidly evolving threats; limited real-world system integration.

2.1 Research gap

The existing methods on UAV threat detection based on the literature exist with multiple critical limitations that highlight the potential use of MFIS in regard to adaptivity, decision rules, and computation load. For example, the fuzzification methods in FMARL lead to removal of granularity, and even after significant validation, can still not be practically deployed; Image-based fuzzy controllers continue to exist without validation for deployment; AI energy prediction methods for MCDM assessment models that did not address environmental influences; and UFMS models such as SAC-FIS rely heavily on simulation-based development that do not address real-world applicability. Furthermore, multi-criteria decision making based fuzzy frameworks continue to be driven by expert judgment, which provides a level of subjectivity at multiple levels of application in the estimation of weights in fuzzy reasoning, and malware detection general methods for UAVs show silent integrations with real-time systems. All these demonstrate poor flexibility, static decision rules and high computation loads. Therefore, the proposed methods of designing MFIS as fuzzy MCDM suspect with data normalization in real-time, principles of PCA derived feature reduction, and scalable fuzzy rule base, provide a pathway for adaptive, scaling, and valid classifications of a UAV's behaviour in real-time and in different dynamic FANET environments, coupled with potential threat mitigation.

3 Methodology

The methodology involves monitoring the UAV behavioural dataset for threat classification and detection and countermeasure deployment using fuzzy logic-based decision systems to enhance communication security in FANETs by identifying and mitigating potential threats. UAV behavioural data was utilized in this research and Min-max normalization and PCA were applied for preprocessing and feature selection. An MFIS computes a dynamic honesty score based on key parameters. The system classifies UAVs and recommends countermeasures, enhancing threat classification and detection, network reliability, and energy efficiency. Figure 2 shows the general flow of the fuzzy logic decision-making process, from data capture through threat assessment and final response selection.

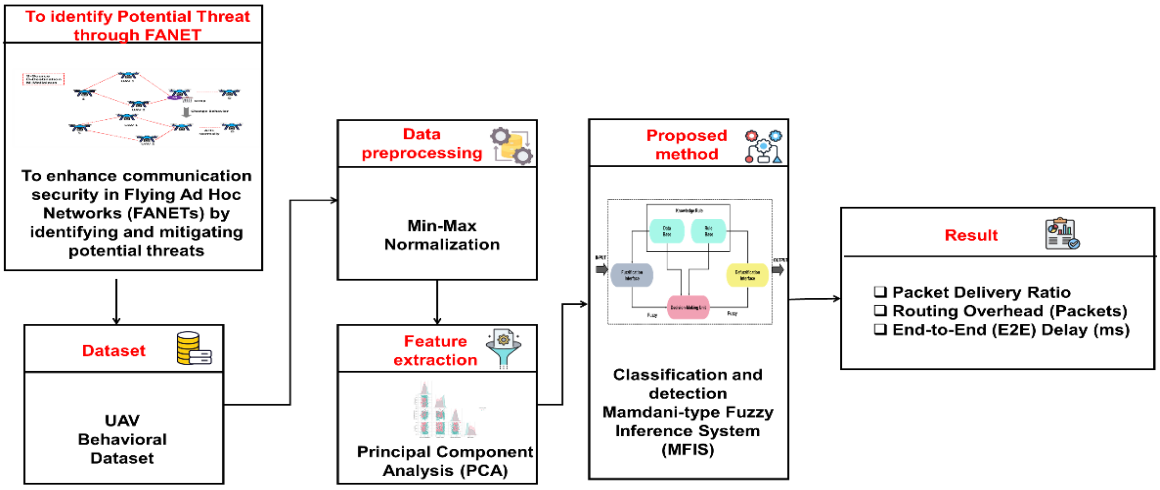

Figure 2: Overall flow of the proposed UAV countermeasure approach using fuzzy logic

3.1 FANETs

Using fuzzy logic for UAV countermeasures aims to reinforce communication safety in FANETs with accurate threat classification and detection and mitigation. The capacity of fuzzy logic systems to accommodate uncertain and vague data makes them suitable solutions for mobile environments such as FANETs that are characterized by

signal hops and unpredictable threats. Through monitoring key indicators, the fuzzy logic methodology can identify anomalies or threats to network security. For the security of communication in the network, it engages in such acts as the encryption of signals, isolation of drone, or modification of routing. Fuzzy logic increases communication assurance in FANETs by managing uncertainty in data and security by assessing signal quality, drone behaviour, and traffic patterns to determine possible security threats. It allows for responsiveness such as encryption, blocking a drone's messages, deploying an alternative drone, and modifying routing, as identified in Figure 3.

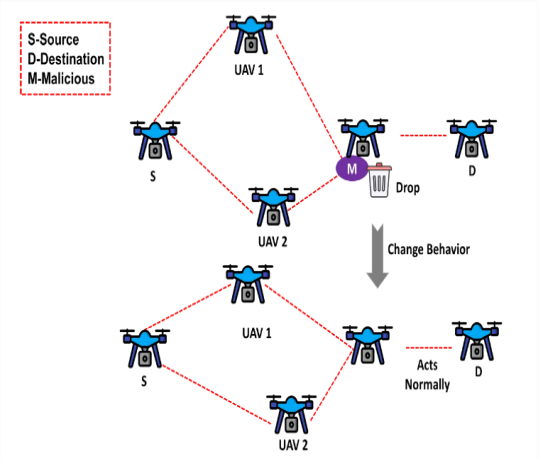

Figure 3: Resilient communication architecture in FANETs using Fuzzy Logic

3.2 Data collection

The data is a synthetic dataset with 1,000 instances to mimic the different behavioural characteristics of UAVs for use in research on fuzzy logic-based countermeasure systems, and intelligent threat classification and detection. Each instance can be characterized by four behavioural metrics: energy consumption, mobility pattern, packet transmission, and link stability. These metrics can be used to differentiate between cooperative UAV behaviour and malicious UAV behaviour.

The dataset can be used to develop intelligent decision-making models using labelled data with *behavior_label* indicating if the UAV behavior is cooperative (0), or malicious (1). The key features description is shown in Table 2.

Table 2: Feature description table

Feature Name	Description	Data Type / Range
energy_consumption	Power usage of the UAV in joules	Continuous (Joules)
mobility_pattern	Normalized movement variability (0 = stable, 1 = erratic)	Float (0–1)
packet_transmission	Successful packet transmission percentage	Percentage (0–100%)
link_stability	Communication links quality and consistency	Float (0–1)
behavior_label	UAV classification: 0 = Cooperative, 1 = Malicious	Categorical (0 or 1)

Source:https://www.kaggle.com/datasets/ziya07/uav-behavioral-dataset/data

Data Exploration: The data exploration shows pairwise relationships between key features, such as energy consumption, mobility pattern, packet transmission, and link stability, for two UAV behaviour types (labels 0 and 1), likely representing normal and indirect patterns. Kernel density plots reveal distribution differences; evasive UAVs (label 1) exhibit lower link stability and higher energy consumption.

These patterns support fuzzy logic-based classification by highlighting feature separability, enabling adaptive countermeasures through decision rules. Figure 4 shows the data exploration outcomes and data exploration highlights behavioural differences between normal and evasive UAVs. Evasive patterns show higher energy consumption and lower link stability, supporting fuzzy logic classification by emphasizing feature separation for adaptive threat classification and detection and countermeasure selection.

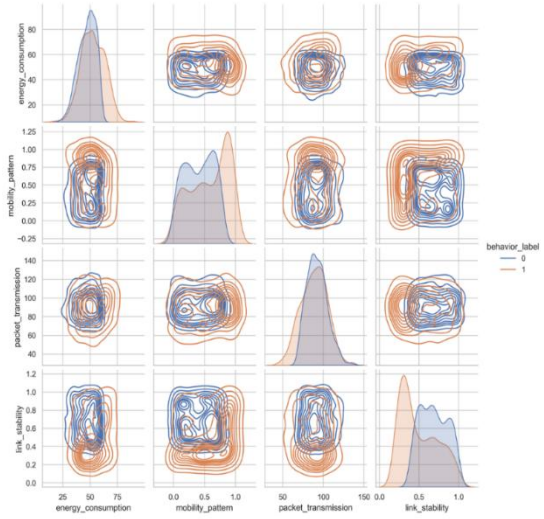

Figure 4: Feature distribution analysis for UAV behavioural classification

3.3 Data preprocessing

Data preprocessing for UAV countermeasures using fuzzy logic involves Min-Max normalization to scale sensor input data key parameters, between 0 and 1. Fuzzy logic is used in the research to enhance decision-making of aerial threats using UAVs through threat classification and detection, evasive manoeuvres, and adaptive control decisions.

Data preprocessing techniques to prepare sensor inputs to the fuzzy inference system are paramount in this process. The Min-Max normalization technique is applied to scale important UAV sensor characteristics, e.g., speed, altitude, and threat proximity, to a common range of [0,1]. This transformation improves the consistency of input values, allows for better computational efficiency, and improves understandability and responsiveness for the fuzzy logic system. as obtained in Equation (1).

$$X_{new} = \frac{X - \min(W)}{\max(X) - \min(X)} \quad (1)$$

W_{new}- The adjusted value derived from the normalized outcomes

W- Old value

$\max(x)$- The dataset's maximum value

$min(x)$- The dataset's minimum value

This preprocessing step guarantees a balanced assessment across data input variables while mitigating any bias from differential scales. By creating better consistency of data ranges, the system is better poised to accurately evaluate threats, and to adaptively respond to them in real-time in FANET scenarios.

3.4 Feature extraction using PCA

Feature extraction using PCA in UAV countermeasures based on fuzzy logic involves reducing the dimensionality of sensor data while preserving essential features. The efficiency and effectiveness of UAV countermeasure systems by integrating fuzzy logic and dimensionality reduction techniques that correctly identify and factor in the most important behavioural dimensions. PCA supports this through feature extraction as plan to minimize the dimensionality of UAV sensors and target data while still retaining critical features needed for quick classification and detection of threats, fast navigation, and making evasive decisions. PCA takes a set of variables that may be correlated and transforms them into a smaller number of uncorrelated variables called principal components, ordered by the amount of variance it explains from the original data. PCA allows the fuzzy inference system to reduce the input space, which benefits computational performance and understanding of the system. Assuming that $w_1, w_2, \ldots\ldots, w_l \in \Re^m$, security issues around energy data management are taken into consideration during PCA computation.

Determine the mean vector μ in m-dimensions by Equation (2).

$$\mu = \frac{1}{l}\sum_{j=1}^{l} w_j \quad (2)$$

The mean of all input vectors is computed across each dimension to center the data. This equation calculates the overall average (mean) across all UAV sensor observations for each dimension (speed, altitude, threat offset, etc.). Centring the data by simply subtracting this average ensures that PCA will ultimately detect not the absolute location of the UAV in feature space, but the variability of the UAV behaviour in feature space. This makes the fuzzy system more responsive to the real behaviour patterns in the data, as opposed to noise.

$$T = \frac{1}{l}\sum_{j=1}^{l}(w_j - \mu)(w_j - \mu)^s \quad (3)$$

Determine the observed data's estimated matrix of covariance T by Equation (3). $(w_j - \mu)^s$ is the transpose of the centered vector. This equation quantifies how much each pair of sensor features covaries across all UAV observations. When fully understood, these relationships are leveraged through PCA to determine what combinations of features are most salient for differentiating normal UAV behaviour from threatening ones. This improves the quality of input into the fuzzy system to facilitate better decision-making in response to threats. Determine the associated eigenvectors and eigenvalues of T, whereby $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_l \geq 0$. Determine the primary components from the l original variables by Equation (4).

$$z_1 = b_{11}w_1 + b_{12}w_2 + \cdots + b_{1l}w_l$$
$$z_2 = b_{21}w_1 + b_{22}w_2 + \cdots + b_{2l}w_l \quad (4)$$
$$\cdots$$
$$z_l = b_{l1}w_1 + b_{l2}w_2 + \cdots + b_{ll}w_l$$

These equations convert the initial sensor data into new, uncorrelated features (principal components) that better capture the variation present in UAV behaviour. These features reduce redundancy and improve the clarity of the fuzzy logic system inputs thus directing its attention towards truly meaningful patterns in the data that can be used for the classification and detection and control of threat responses. It is orthogonal that z_l are uncorrelated. As much of the initial variation in the data set can be explained by z_1, as much of the residual variance can be explained by z_2, etc. In the most useful data sets, a small number of bigger eigenvalues often outnumber the others, as follows in Equation (5). b_{11} describes the coefficients (elements of eigenvectors) used for projecting original vectors into the new space. These components z_l are orthogonal and uncorrelated, forming a new feature basis. Where the proportion maintained in the data format is denoted by z_l. PCA was used for feature extraction with the requirement to retain the extracted main components that explain at least 80% of the total variation. Figure 5 presents the feature importance of the dataset.

$$\gamma_l = \frac{\lambda_1+\lambda_2+\cdots+\lambda_n}{\lambda_1+\lambda_2+\cdots+\lambda_n+\cdots+\lambda_l} \geq 80\% \quad (5)$$

γ_l is defined as the total variance captured by the first n components. It ensures that the reduced space still reflects the majority of the original data information content. Utilizing PCA in this approach allows the UAV countermeasure system to only process the more relevant features of behaviour, allowing the computational load to be dramatically reduced and increasing the overall decision accuracy) of the system. Moreover, privacy limitations have been addressed by removing class labels from the behavioural features presented; the UAV countermeasure system is therefore solely focusing on the de-identified numerical data and statistical features of behaviour, specifically in energy-sensitive applications. This equation guarantees that the chosen principal components retain at least 80% of the original data's total variance. It ensures that most of the useful information about UAV behaviour is preserved after the dimensionality reduction; therefore, the fuzzy system can work properly without sacrificing accuracy. The pair plot visualizes feature distributions and relationships between UAV behaviours (label 0 = cooperative, 1 = malicious). Malicious UAVs tend to show higher energy consumption, erratic mobility, lower packet transmission, and reduced link stability, enabling fuzzy logic to distinguish patterns and support adaptive threat classification and detection shown in Figure 5. To conduct 20 experimental runs to capture performance variability.

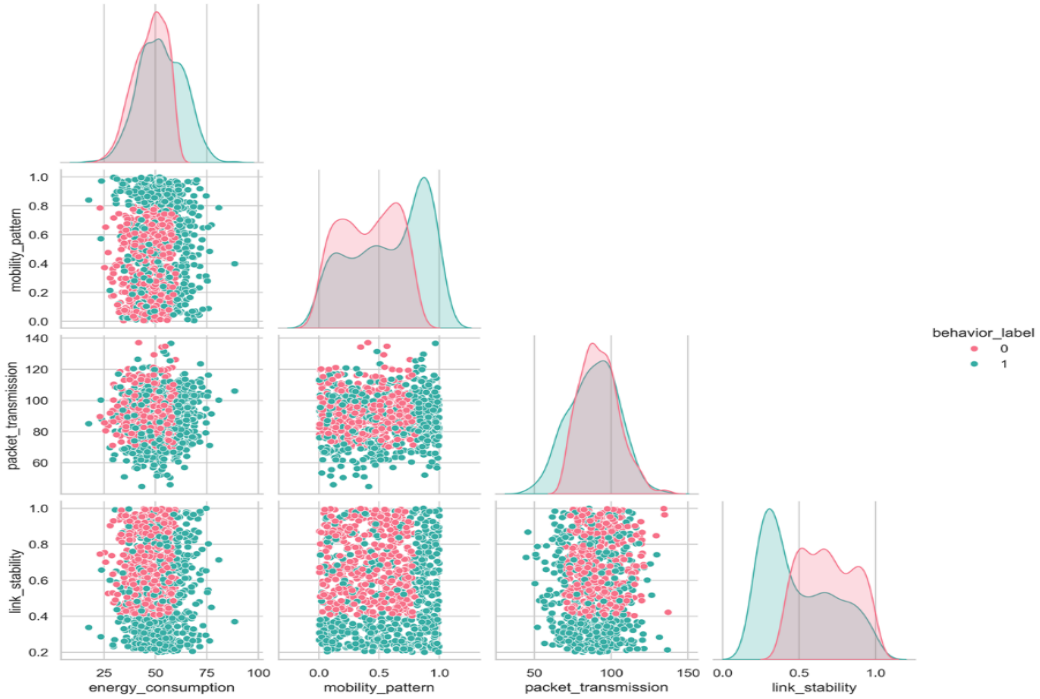

Figure 5: Feature Importance of the proposed dataset

The Table 3 summarizes the percentages of variance explained by the principal components. The first component accounts for 52%, the second accounts for 22%, and third component accounts for 11% and the last

four components together account for 15%. This indicates that there is some concentration in the distribution of variance.

Table 3: The distribution of variance

Component	Variance Explained (%)
1	52
2	22
3	11
Others	15

To settled on 3 retained components, totaling 85% of the variance (Component 1 = 52% (12826/31940), Component 2 = 22% (7081/31940), Component 3 = 11% (3582/31940)). This is consistent with the generally accepted 80% threshold for cumulative variance retention, which is commonly noted in UAV threat classification and detection studies. A scree plot of the eigenvalues used, is provided in Figure 6.

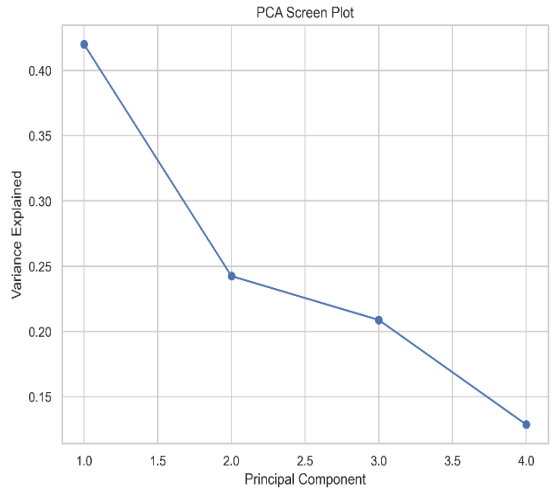

Figure 6: Scatter plot for PCA

3.5 Classification and detection using mamdani-type fuzzy inference system (MFIS)

An MFIS is employed in UAV countermeasures to classify drones as cooperative or malicious based on behavioural inputs. The system uses a rule-based approach with fuzzy logic to handle uncertainty and imprecision, evaluating input variables through membership functions and inference rules. By translating ambiguous behaviour into actionable classifications, MFIS enhances threat classification and detection, supporting real-time decision-making in autonomous aerial defence systems against potential malicious UAVs. The proposed MFIS employs triangular and trapezoidal membership functions for fuzzification, followed by minimum (min) T-norm for handling logical AND operations during rule evaluation, and maximum (max) S-norm for aggregating outputs from multiple rules. Finally, the Mean of Maximum (MoM) method is used in the defuzzification phase to obtain a crisp control output from the fuzzy set. To elaborate on the fuzzy logic system components. The MFIS employs triangular and trapezoidal membership functions for the four input variables—energy consumption, mobility pattern, packet transmission, and link stability—each with three linguistic terms (low, medium, high). These combinations form a total of 45 fuzzy rules, which are expert-defined to capture UAV behaviour patterns.

➢ ***Fuzzification using a knowledge rule***

Using the normalized scale $[0,1]$, it identifies data and rules based on the values of the observations $w, z, x, ..$, for the value of w determined at the time s, also defines $w(s) \in [0,1]$. Each of these observables $(w, z, x, ..)$ corresponds to a limited number of atomic sentences, as shown in Equation (6).

$$W_1, W_2, .., Z_1, Z_2, .., X_1, X_2 \ldots. \quad (6)$$

W_j is the linguistic term for input variables w (eg., high deviation), Z_j is the linguistic term for input variables z (eg., Medium delay), X_j is the linguistic term for input variables x (eg., High threat), These are atomic sentences that represent the linguistic terms (e.g. "High altitudes", "Low battery") corresponding to the input and output variables of fuzzy logic thermal context. The atomic sentences define the vocabulary in which fuzzy rules can be expressed such as "IF flight deviation is high THEN threat level is high, which connects to the purpose of assessing UAVs' ambiguous behaviours. Defines the linguistic variables (e.g. "high speed", "low energy") that characterize input and output behaviours.

The union of the atomic phrases thus forms the language V that is linked to the system. It considers the $FORM_V$ over the V set of formulas. It refers to a function $e: [0,1] \rightarrow [0,1]$ as a fuzzy set concerning observations. The selection of an infinite number of sets of fuzzy values over each observable is known as fuzzification of the observations $w, z, x,...$, and results in functions, as follows in Equation (7).

$$e_1, e_2, .., h_1, h_2, .., g_1, g_2 \ldots \quad (7)$$

e_1 membership function for W_j, applied to input w, h_1 membership function for Z_j, applied to input z, g_1 membership function for x_j, defining fuzzy output values. These functions assign degrees of truth for the atomic sentences, where inputs (for example, deviation, delay) are mapped and assigned to values between 0 and 1. These

fuzzy sets allow the system to classify UAV behaviours "softly," thereby acknowledging the uncertainty that is important for detecting potential threats in real time. Defines fuzzy membership functions to evaluate the degree of truth of every linguistic term.

The function of e_1, for example, in logic, is to give the associated atomic sentence W_1 a way to be assigned a level of truth. Specifically, at the time s, w is $w(s) \in [0,1]$. Then $e_1(w(s))$ is the level of truth of W_1. Immediately, it follows that the fuzzification of the observations w, z, z,... uniquely determines an atomic assignment at each instant s, as obtained in Equation (8).

$$\bar{\mu}_s(W_j) = e_j(w(s)), \bar{\mu}_s(Z_j) = h_j(z(s)), \ldots \quad (8)$$

$w(s)$ and $z(s)$ are the real-time input values at time s, $\bar{\mu}_s(W_j)$ is degrees to which $w(s)$ satisfies fuzzy set W_j, and $\bar{\mu}_s(Z_j)$ is described as degrees to which $z(s)$ satisfies fuzzy set Z_j. Assign a truth value for each observation (e.g. how true is "speed is high" at time ss) using the corresponding fuzzy membership function. This creates the fuzzy input vector at any given time step, allowing raw UAV behaviour to be transformed into a fuzzy logic-capable format. Evaluate the truth value of each atomic sentence at time s using membership functions.

It is particularly, to choose a model; the system is irrelevant. It fixes a many-valued logic $\mathcal{L}$ by selecting a t-norm *: [0, 1]2 → [0, 1]. The atomic assignment then uniquely extends to an assignment since $\mathcal{L}$is is truth-functional, as shown in Equation (9).

$$\mu_s: FORM_V \rightarrow [0,1] \quad (9)$$

Given the logic $\mathcal{L}$ and the fuzzification applied to fuzzy logic, each formula $\phi \in FORM_V$ of $\mathcal{L}$ might be provided with a distinct truth value at each instant s. Extends the atomic truth assignments to whole fuzzy logic rules using many-valued logic (with some t-norm operation such as MIN). This allows logical reasoning about fuzzy rules, which is the fundamental mechanism for discerning whether a UAV is malicious or safe. Extends atomic assignments (from Eq. 8) to whole fuzzy logic rules using many-valued logic.

➢ ***FIS***

The fuzzy inference, specifically fuzzy control systems. The Mamdani-type inference follows in logical recasting. Instead, it will strive to be in line with accepted practices. It may be interpreted as Mamdani-type reasoning. Fuzzy inference may be summed up as follows.

Phase 1: The observables $w, z, x, .,$ should be divided into two non-empty, disjoint subsets: the input observables $\{w, z \ldots\}$ and the output observables $\{x, \ldots\}$. Should the language V be divided into the following sets: input variables $\{W_1, W_2, \ldots, Z_1, Z_2, \ldots\}$ and output variables $\{X_1, X_2, \ldots,\}$ Additionally, divide the fuzzy sets into the following collections: input fuzzy sets $\{e_1, e_2, \ldots, h_1, h_2, \ldots\}$ and output fuzzy sets $\{g_1, g_2, ..\}$.

Phase 2: Establish a limited set of rules of the following type: X is (NOT) W_j if w is (NOT) W_j AND z is (NOT) Z_i THEN x is NOT X_i... It maintains that W_j is negated when the NOT is contained in "w is (NOT) W_j," and the same is true for $Z_i, X_l, ..,$

Phase 3: For each rule Q as in (M2), given the resulting input values $w(z), z(s), \ldots$ at time s, set, as follows in Equation (10).

$$Q_s = \min\left\{e_j'(w(s))\right), h_i'\left(z(s)\right), \ldots,\} \in [0,1] \text{ were,}$$
$$e_j'(\dot{w}(s)) =$$
$$\begin{cases} 1 - e_j(w(s)) if\ W_j is\ negated\ in\ Q \\ e_j(w(s))\ Otherwise \end{cases} \quad (10)$$

Calculates the firing strength of a fuzzy rule at time ss using the minimum T-norm for logical ANDs. When computing firing strength, to determine the impact of UAV behaviour on rules. As an example, if a UAV has a high deviation behaviour and has bad communication, the corresponding rule for "malicious UAV" would fire strongly. Computes the firing strength of a rule at time ss, using MIN t-norm for logical AND.

Phase 4: Using the function Q_s, create the resulting fuzzy set of rule Q, at the time s for each Q_s calculated in phase 3: Given by $g_l^s: [0,1] \rightarrow$, as follows in Equation (11).

$$e_j'(\omega) = \begin{cases} \min\{Q_s, 1 - g_l^s(\omega)\}\ if\ X_l\ is\ negated\ in\ Q; \\ \min\{Q_{s,} g_l^s(\omega)\}\ Otherwsie \end{cases} \quad (11)$$

Produces a fuzzy output set given the input firing strength $Q_{s,}$ and the output fuzzy set g_l^s of the rule. Creates the output response (e.g., a threat level), still not crisp, but fuzzy indicating something along the lines of "likely malicious". Creates the fuzzy output set from a rule, and modifies it for output negation.

Phase 5: The function $E_s: [0,1] \rightarrow [0,1]$ is defined as the aggregate output fuzzy set at time $s$in Equation (12).

$$E_s = \max\{g_l^s\} \quad (12)$$

E_s is described as the agreed fuzzy output at time s for output value (w), max is the logical OR to combine multiple rule consequences. It takes all individual rule outputs and combines them into a single fuzzy output set using the maximum (S-norm) operation. This considers the collective decision of the system at time ss based on all individual rules and provides a joint fuzzy evaluation of the UAV behaviour.

It takes all rule outputs and combines them into a single fuzzy output set using the MAX S-norm.

Consequently, as in phase 4, the maximum of all rules ranges throughout the output fuzzy sets. Consequently, Mamdani-type inference yields the fuzzy set E_s at each instant s, as shown in (phase 5).

➢ ***Defuzzification***

The fuzzy set E_s: $[0,1] \rightarrow [0,1]$ is the result of a Mamdani-type inference at time s. The range of normalized values for the physical observation x that has to be controlled is known as the domain of E_s. To have real control, x needs to be set to a certain value $\omega_s \in [0,1]$. This is accomplished by defuzzifying E_s.

It assumes decision support that the well-known mean of the maximum defuzzification method is used to calculate ω_s from E_s. It shows how ω_s is calculated when utilizing discrete approximations to E_s. Assume the set of sample points $T = \left\{\frac{1}{m} \middle| m = 0,1,\ldots,M\right\} \subseteq [0,1]$ after selecting an integer $M > 1$. Set $N_s = \{t \in T | E_s(s) = \max_{w \epsilon T} E_s(\omega)\}$ to extract those that maximize E_s over T, as obtained in Equation (13). Figure 6 presents the MFIS structure.

$$\omega_s = \frac{\sum_{t \in N_s} T}{|N_s|} \quad (13)$$

Converts the fuzzy output $E_s(s)$ into a crisp control value $\omega_s \in [0,1]$ $omega\_s$ in $[0,1]$ by averaging the values where $E_s(s)$is highest. This crisp output is essential for taking decisive control actions like activating countermeasures or issuing alerts perfectly aligning with the objective of actionable, real-time UAV threat classification. The proposed MFIS uses fuzzy logic to classify UAVs as cooperative or malicious by evaluating behavioural inputs. It applies fuzzy rules, membership functions, and defuzzification to support real-time decision-making for adaptive UAV countermeasures in uncertain environments as shown in Figure 7.

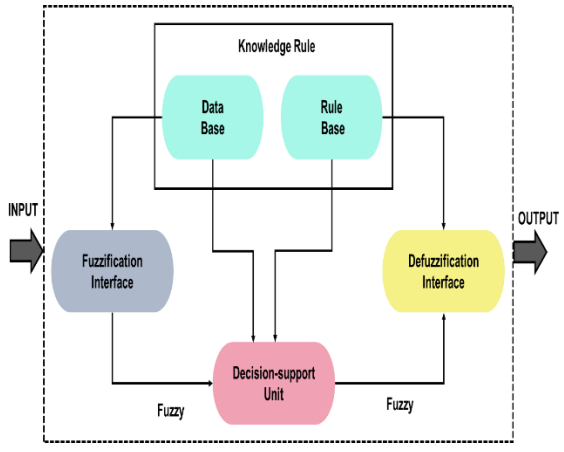

Figure 7: Architecture of the Proposed MFIS for UAV threat classification

4 Result

This section deliberates on the results produced by the implementation of the model, including parameter setup, evaluation criteria, and comparative phase.

4.1 Experimental setup

Python 3.8 made multitasking and development duties demanding performance evaluations much easier due to this modern laptop design as shown in Table 4.

Table 4: Experimental setup

Aspect	Details
Hardware	Intel Core i7 CPU, 16 GB RAM, NVIDIA GTX 1660 GPU
Software Stack	Python 3.8, scikit-fuzzy, NumPy, Pandas
Training-Validation Split	80% training, 20% validation

4.2 Hyperparameters

MFIS parameters as described in Table 5.

Table 5: Parameter's setup

Parameter	Value/Setting
Number of Input Variables	4 (Energy, Mobility, Transmission, Link Stability)
Membership Function Type	Triangular, Trapezoidal
Number of Membership Functions	3 (Low, Medium, High)
Rule Base Size	45 rules
Inference Method	Mamdani-type inference
Fuzzy T-norm Operator	Minimum (min)
Fuzzy S-norm Operator	Maximum (max)
Defuzzification Method	Mean of Maximum (MoM)
Normalization Technique	Min-Max Normalization
Number of Principal Components	3 components
Variance Retained (PCA)	≥ 80%

4.3 Evaluation criteria

The proposed MFIS approach showed good performances on all evaluation metrics. The ROC and PR curve evaluations have provided evidence of accurate threat classification and detection, and the energy & mobility pattern analysis has demonstrated the energy-efficient UAV countermeasures.

4.3.1 ROC Curve

The performance of a fuzzy logic-based UAV countermeasure system was evaluated. The curve shows a high true positive rate across almost all false positive rates, indicating strong classification performance. The AUC is 0.98, suggesting the model is highly effective at distinguishing threats from non-threats in fuzzification strategy for mitigating fuzzy logic. The steep rise near the y-axis reflects excellent sensitivity with minimal false alarms, making the system suitable for real-time UAV threat classification and detection and response. Figure 8 demonstrates the impressive classification performance of the fuzzy logic-based UAV countermeasure system by having very high sensitivity with low false alarm rates, making it suitable for real-time threat identification and response.

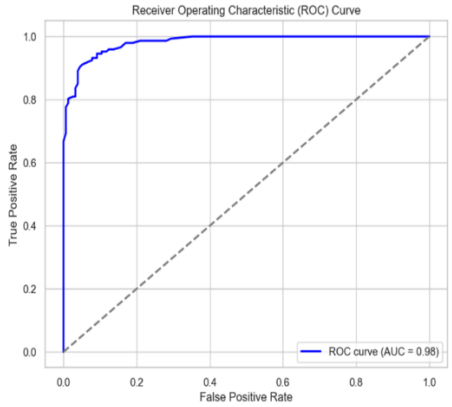

Figure 8: ROC Curve illustrating classification performance of the proposed MFIS-Based UAV countermeasure system

4.3.2 Precision-Recall (PR) curve

The PR curve evaluates the performance of a fuzzy logic-based UAV countermeasure model. The high area under the curve (AUC = 0.98) indicates outstanding classification performance which sustained high precision despite increased recall. It suggests that the model effectively detects threats (true positives) with minimal false alarms, making it highly suitable for real-time UAV threat mitigation. Figure 9 displays the PR curve outcomes.

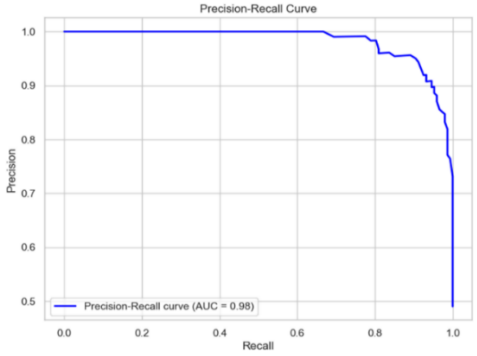

Figure 9: High-performance classification and detection accuracy is shown by the PR Curve for MFIS

4.3.3 Energy consumption vs mobility pattern

The relationship between energy consumption and mobility patterns in UAVs, segmented by behavior labels (0 and 1), is analyzed. The x-axis represents energy consumption, while the y-axis indicates normalized mobility patterns.

Two distinct clusters emerge: behaviour label 0 (in blue) generally reflects lower to moderate energy consumption and varied mobility, whereas behaviour label 1 shows broader energy usage and more consistent high mobility. In the context of UAV countermeasures based on fuzzy logic, this visualization helps identify behaviour patterns that can trigger adaptive responses for efficient energy management and mobility control under uncertain operational conditions. Figure 10 presents the outcomes of mobility pattern vs energy consumption.

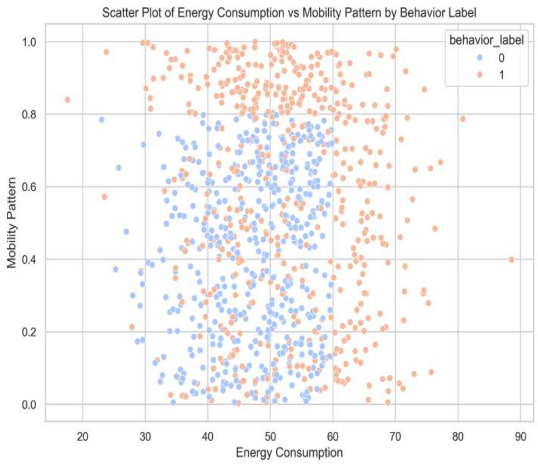

Figure 10: Energy consumption and mobility pattern using the proposed MFIS Method

4.4 Comparison phase

Python 3.12 made multitasking and development duties demanding performance evaluations much easier due to this modern laptop design. The result comparison parameters, such as packet delivery ratio, routing overhead, and end-to-end delay, are used to demonstrate the comparison of the proposed model, MFIS, with the traditional model, efficient honesty-based classification and detection scheme (EH-DS) [20].

4.4.1 Packet delivery ratio

The packet delivery ratio for the proposed MFIS method was compared with the existing EH-DS approach, showing significant improvement as the number of drones increases. The MFIS method consistently shows higher packet delivery ratio values across all drone counts compared to EH-DS. While EH-DS increases steadily, MFIS achieve significantly better performance, indicating more reliable and efficient data delivery. Figure 11 display the packet delivery ratio outcomes.

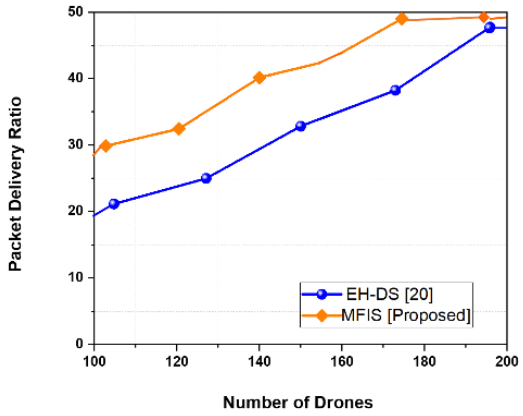

Figure 11: Comparison of packet delivery ratio

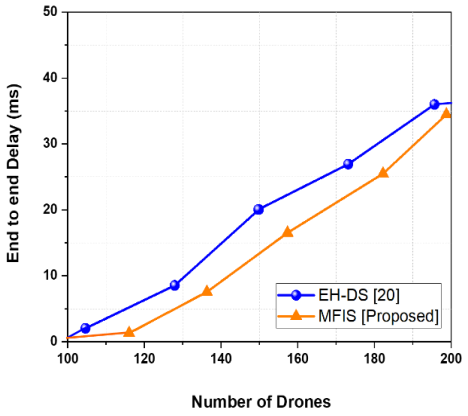

Figure 13: Result of the E2E delay

4.4.2 Routing overhead (packets)

The additional communication and processing burden placed on a network because of the transfer or routing of control or routing packets. MFIS demonstrates lower routing overhead throughout the range, with values remaining minimal even as the number of drone increases. In contrast, EH-DS shows relatively higher overhead, suggesting more control traffic and less efficient routing management. Figure 12 depict energy consumption with the growing number of drones.

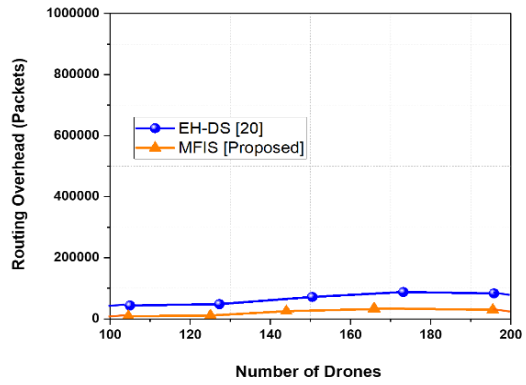

Figure 12: Representation of routing Overhead (Packets)

4.4.3 End-to-End (E2E) Delay (ms)

The E2E delay for UAV systems with different numbers of drones is compared, evaluating the proposed MFIS method with the existing method, EH-DS. The end-to-end delay for MFIS remains lower across all drone densities compared to EH-DS. As the number of drones increases, EH-DS experiences higher delays, whereas MFIS maintains better responsiveness and faster communication flow. Figure 13 demonstrate MFIS's superior scalability and efficiency in reducing communication latency, making it a more effective solution for real-time UAV operations under increased network loads.

4.5 Discussion

The research is primarily aimed at producing an intelligent fuzzy logic-based UAV countermeasure system (MFIS) that improves accuracy, energy efficiency, and communication reliability in constantly changing and different environments. EH-DS method [20], while functional, is limited in significant areas: static thresholds, low adaptability to noise, difficulty dealing with cooperative or spoofing attacks, and inattention to dealing properly with situations of very fast drone movements or complicated environments. Alternatively, the proposed MFIS method performs real-time fuzzification to obtain effectively adaptive decision-making mechanisms, resulting in improved packet delivery ratio and reduced time taken in acquisitions. Consequently, these advancements demonstrate that MFIS has superior performance across important metrics, and more importantly, better scalability and operational efficiency with increasing sizes of UAV networks. The proposed MFIS has many potentials to adapt fuzzy logic limits by providing real-time input normalization and dynamic rule evaluation to generate context-aware decisions. Conventional fuzzy logic systems tend to use non-adaptive sets of rules, but MFIS employs PCA-optimized feature refinement and use of input variability to contextualize retrospectively to improve the adaptation of UAVs to perceptions. In part, this will relax their reliance on fixed thresholds and their adaptability when dealing with UAVs as unique environmental system factors.

5 Conclusion

This decision-support approach for UAV threat identification and mitigation, based on fuzzy logic, uses a well-developed dataset that collects UAV behavioural information, including key parameters. Preprocessing strategies, including min-max normalization, ensure uniform data and reduce the effects of scaling issues, which strengthens the eventual analysis. Using PCA in feature extraction, critical attributes relevant to UAV

behaviour were emphasized. The system is designed to increase the safety of the messages in FANETs by detecting threats and countermeasures. The MFIS was used as the main tool, constantly computing a dynamic honesty score based on the features it received. This enabled dynamic labelling of UAVs as cooperative or malicious to facilitate the effective implementation of countermeasures. The simulation results show a significant improvement in performance parameters, including to-end delay, routing overhead (packets), and packet delivery ratio, by 15-55% compared to previous methodologies. The findings confirm the merits of the system to generate reliable and timely threat analysis and relevant advice without compromising operational effectiveness. Real-time processing speed and scalability remain a challenge, especially in cases of large networks of UAVs. The future improvements will focus on speed optimization and hybridization of the most modern hybrid methods, suitable for larger-scale usage. In future research, integrate realistic UAV mobility models such as Gauss-Markov or Random Waypoint (RWP) to simulate dynamic flight behaviours over time. It will apply statistical significance tests to compare MFIS and EH-DS, ensuring reliable performance validation across all metrics. It will address this by incorporating time-based UAV mobility datasets and real-time testing environments to comprehensively evaluate latency and computational overhead. It plans to enhance the system by integrating hybrid fuzzy systems, specifically a neuro-fuzzy inference mechanism, to allow adaptive tuning of membership functions and rule bases through learning. It also aims to incorporate reinforcement learning techniques to enable online rule adjustment based on real-time UAV behavioural feedback, allowing the system to continuously evolve and improve its threat classification and detection and response strategies. To incorporate statistical significance testing such as t-tests or ANOVA to validate performance gains by computing confidence intervals and p-values for reported metrics. Future work will incorporate statistical measures for both methods to strengthen performance comparison

Acknowledgements

2021-2022 Hebei province higher education teaching reform research and
practice project : Research on the construction of innovative talent
training system of police unmanned aerial vehicle application under the new
engineering traction. （NO：2021GJJG455）

References

[1] Rukaiya R and Khan SA (2024). Communication architecture and operations for the SDR-enabled UAVs network in disaster-stressed areas. *Ad Hoc Networks*, 160, p.103506.https://doi.org/10.1016/j.adhoc.2024.103506.

[2] Narmeen R, Almadhor A, Alkhayyat A, and Ho PH (2024). Secure Beamforming for Unmanned Aerial Vehicles Equipped Reconfigurable Intelligent Surfaces. *IEEE Internet of Things Magazine*, 7(2), pp.30–37.https://doi.org/10.1109/IOTM.001.2300238

[3] Tuncer O and Cirpan HA (2023). Adaptive fuzzy based threat evaluation method for air and missile defense systems. *Information Sciences*, 643, p.119191.https://doi.org/10.1016/j.ins.2023.119191

[4] Ahmad A, Amjad R, Basharat A, Farhan AA, and Abbas AE (2024). Fuzzy knowledge based intelligent decision support system for ground-based air defence. *Journal of Ambient Intelligence and Humanized Computing*, 15(4), pp.2317–2340.https://doi.org/10.1007/s12652-024-04757-3

[5] Fetai B (2024). Advancing Cadastral Mapping with UAVs and Automated Boundary Delineation. *Informatica*, 48(2).https://doi.org/10.31449/inf.v46i2.6800

[6] Anagnostis I, Kotzanikolaou P, and Douligeris C (2025). Understanding and Securing the Risks of Unmanned Aerial Vehicle Services. *IEEE Access*. https://doi.org/10.1109/ACCESS.2025.3549861

[7] Li C, Zhao W, Zhao L, Ju L, and Zhang H (2024). Application of fuzzy logic control theory combined with target tracking algorithm in unmanned aerial vehicle target tracking. *Scientific Reports*, 14(1), p.18506.https://doi.org/10.1038/s41598-024-58140-5

[8] Almseidein TA and Alzidaneen A (2025). Optimizing UAV Trajectories with Multi-Layer Artificial Neural Networks. *Informatica*, 49(2).https://doi.org/10.31449/inf.v49i2.7178

[9] Huang G, Hu M, Yang X, Lin P, and Wang Y (2024). Addressing Constraint Coupling and Autonomous Decision-Making Challenges: An Analysis of Large-Scale UAV Trajectory-Planning Techniques. *Drones*, 8(10), p.530.https://doi.org/10.3390/drones9030206

[10] Mishra S and Palanisamy P (2023). Autonomous advanced aerial mobility: An end-to-end autonomy framework for UAVs and beyond. *IEEE Access*, 11, pp.136318–136349.https://doi.org/10.1109/ACCESS.2023.3339631.

[11] Sarkar A, Santoso F, Shen J, Du B, Telikani A, and Yan J (2024). Evaluating Energy Consumption Prediction Models of a Quadcopter Unmanned Aerial Vehicle. *IEEE VTC2024-Fall*, pp.1–7.https://doi.org/10.1109/VTC2024-Fall63153.2024.10757699

[12] Hu C, Li J, Yang Y, Gu Q, Wu Z, and Ning B (2025). A Large-Scale UAV Swarm Confrontation Method Based on Fuzzy Reinforcement Learning.

International Journal of Fuzzy Systems, pp.1–12.https://doi.org/10.1007/s40815-024-01903-z

[13] Xia B, Mantegh I, and Xie W (2024). UAV Multi-Dynamic Target Interception: A Hybrid Intelligent Method Using Deep Reinforcement Learning and Fuzzy Logic. *Drones*, 8(6), p.226.https://doi.org/10.3390/drones8060226

[14] Jasim AN, Fourati LC, and Albahri OS (2023). Evaluation of unmanned aerial vehicles for precision agriculture based on integrated fuzzy decision-making approach. *IEEE Access*, 11, pp.75037–75062. https://doi.org/10.1109/ACCESS.2023.3294094

[15] Shcherban A and Eremenko V (2023). UAV battery charge monitoring system using fuzzy logic. In *Systems, Decision and Control in Energy V*, pp.195–221. Springer, Cham. https://doi.org/10.1007/978-3-031-35088-7_12

[16] Wu P, Wang H, Liang G, and Zhang P (2023). Research on unmanned aerial vehicle cluster collaborative countermeasures based on dynamic non-zero-sum game under asymmetric and uncertain information. *Aerospace*, 10(8), p.711. https://doi.org/10.3390/aerospace10080711

[17] Wang X, Cao Y, Ding M, Wang X, Yu W, and Guo B (2023). Research Progress in Modeling and Evaluation of Cooperative Operation System-of-Systems for Manned–Unmanned Aerial Vehicles. *IEEE Aerospace and Electronic Systems Magazine*, 39(4), pp.6–31. https://doi.org/10.1109/MAES.2023.3347504

[18] Niu Q, Ren S, Gao W, and Wang C (2025). A Dynamic Threat Assessment Method for Multi-Target Unmanned Aerial Vehicles at Multiple Time Points Based on Fuzzy Multi-Attribute Decision Making and Fuse Intention. *Mathematics*, 13(10), p.1663. https://doi.org/10.3390/math13101663

[19] Cai C, Yang J, Wu S, Zhang H, and Chai W (2025). Landing Position Detection and Array Coil Matching of Multi-UAVs Wireless Power Transfer System. *IEEE Transactions on Transportation Electrification*. https://doi.org/10.1109/TTE.2025.3570684

[20] Kundu J, Alam S, and Dey A (2024). Fuzzy based trusted malicious unmanned aerial vehicle detection using in flying ad-hoc network. *Alexandria Engineering Journal*, 99, pp.232–241. https://doi.org/10.1016/j.aej.2024.04.066