Abnormal Behavior State-of-the-Art for UAV Detection in Complex Environments

Pierre PATHE, Benjamin Pannetier, Bartheye Olivier, Daniel Lieutenant-Colonel Gigan

Abnormal Behavior State-of-the-Art for UAV Detection in Complex Environments

PATHE Pierre
CS GROUP LAB
3 Bd Thomas Gobert, 91120, Palaiseau, France

pierre.pathe@csgroup.eu

PANNETIER Benjamin
CS GROUP LAB
3 Bd Thomas Gobert, 91120, Palaiseau, France

benjamin.pannetier@csgroup.eu

BARTHEYE Olivier
CREA
Base aérienne 701, Chemin de Saint de Jean, 13661
SALON AIR, France

olivier.bartheye@ecole-air.fr,

Lieutenant-colonel GIGAN Daniel
Bureau du Numérique et des SIC
107 rue de Grenelle
75007 Paris, France

daniel-frederic.gigan@intradef.gouv.fr

ABSTRACT

The global drone market has surged, growing from $1.6 billion in 2015 to $5.6 billion in 2020. Despite their increasing prevalence, drones can pose challenges. For instance, drone sightings at Gatwick Airport in December 2018 disrupted around 1,000 flights, highlighting potential misuses and the need for effective regulation. Given such incidents, the effective detection, tracking, and identification of abnormal behaviors of small UAVs in complex environments become critical for ensuring security and mitigating potential threats. This paper presents a state-of-the-art review of abnormal behavior detection of small UAVs, focusing on the role of data fusion in enhancing detection performance, especially when dealing with heterogeneous data from multiple sensors.

Our research offers a structured overview of abnormal behavior detection methods and emphasizes the role of data fusion in addressing challenges, especially in environments with multiple operating drones like Amazon's delivery system. In addition, our research highlights the need to promote standardization of performances measures used to abnormal behavior detection algorithms. While metrics like precision, MOTA, and accuracy are standard for detection, tracking, and classification respectively, evaluating behavior detection in a data fusion system remains a challenge.

This paper is relevant to the SET-315 Research Symposium on "Detection, Tracking, ID and Defeat of Small UAVs in Complex Environments" as it provides a comprehensive review of current methods for detecting abnormal behaviors of small UAVs and the role of data fusion in enhancing detection performance. The findings and conclusions presented in this paper can contribute to a deeper understanding of the challenges and opportunities in employing data fusion techniques for counter-UAV applications and help guide future research efforts in this domain. The paper also suggests ways to enhance collaboration within NATO and promote the development of standardized performance measures to facilitate comparison and improvement of detection techniques.

1.0 INTRODUCTION

Detecting abnormal behaviors, which involves identifying significant deviations from expected actions or events, is a long-studied area with relevance in domains like education [35], health [9], and especially defense and security [36].

For defense and security, identifying abnormal behavior is vital due to potential threat implications [38], as highlighted by drone roles in situations like the Ukraine conflict. Drone detection systems utilize diverse sensors like radar, infrared cameras, and acoustic detectors. Data fusion techniques integrate this heterogeneous data, providing a holistic drone representation [37] and enabling prompt responses.

Given these dual aspects, understanding and monitoring UAV behavior becomes crucial to ensure security, safety, and adherence to regulations. This article delves into the current state of the art in abnormal behavior detection for small UAVs, emphasizing data fusion techniques.

Our primary aim is to dissect the current methodologies for abnormal UAV behavior detection, exploring their effectiveness and limitations. The central question driving this analysis is: "Is the current state of the art able to effectively detect abnormal behavior of a drone? And if not, what elements of existing methods should be changed, created, or improved?"

This paper begins with a comprehensive review of current techniques in small UAV abnormal behavior detection, evaluating their strengths and limitations. Addressing our central question, we assess whether the existing state of the art efficiently detects abnormal drone behavior and identify areas of improvement. The complexities inherent in multifaceted environments, diverse data sources, and the lack of standardized evaluation metrics further underscore the challenges in the abnormal behavior detection landscape.

We then explore data fusion's potential to bridge current methodological gaps, presenting our contributions and highlighting its role in enhancing abnormal behavior detection. Empirical experiments are showcased, comparing our approach with established techniques, and illuminating the efficacy of our methods.

Concluding, we provide a synthesis of our findings and their implications for the defense and security sectors. This culmination offers insights into the current challenges in UAV behavior detection and charts the path forward, exploring how advancements in data fusion can lead to more refined and reliable detection mechanisms.

2.0 STATE OF THE ART REVIEW WITH A SINGLE INFORMATION SOURCE

This section explores existing methodologies to evaluate their performance in detecting abnormal drone behavior. In the domain of drones for security and defense, abnormal behavior detection plays a crucial role [39] in identifying actions that deviate from the norm, such as unauthorized flights or the acquisition of sensitive data [40].

2.1 Existing Methods

Various techniques, each with distinct strengths [40], are employed for abnormal behavior detection. These approaches include Model-Based Methods, which utilize predefined models to define what's considered "normal", flagging deviations as anomalies. On the other hand, Statistical Methods, which include both Parametric and Non-parametric methods, harness the power of statistics to determine anomalies, with the former assuming a specific data distribution and the latter making no such assumptions [28].

Bayesian Network Methods [9] stand out for their ability to capture complex relationships between variables in a probabilistic manner, offering a robust framework for reasoning under uncertainty. For temporal data analysis, Time Series Analysis proves invaluable [8], sifting through sequences to detect patterns, trends, and outliers.

In the area of data-driven approaches, methods like Proximity-Based, analyze the spatial relationships between data points. Clustering Methods [29], meanwhile, focus on grouping similar data points, flagging outliers.

The world of machine learning offers a trove of techniques, from Classification Methods like Support Vector Machines (SVM) [10] that divide data into classes, to the skill of Artificial Neural Networks which mimic biological neural structures. Rule and Decision-Based Methods offer a more deterministic approach, setting clear boundaries and rules. Emerging techniques, including Graph-Based Models [8] and Reinforcement Learning, join Ensemble and Subspace methods in enriching the toolkit for behavior detection.

Given the variety of methods outlined for detecting abnormal behavior, can these techniques be directly applied to small UAVs? Or does their application introduce a distinct set of challenges?

2.2 Abnormal Behavior Detection of Small UAVs

The rise in drone popularity and their potential for suspicious activities [46], has made abnormal behavior detection crucial [30]. Investigative approaches often use data from onboard sensors like radars and cameras, with machine learning algorithms pinpointing deviations from typical flight paths [31].

There's a shift towards advanced computer vision techniques that focus on real-time UAV motion tracking [32]. Deviations in flight trajectories or speeds often indicate anomalies. Alongside, radar and acoustic systems are integrated into UAV surveillance due to their sensitivity to UAV signatures [33]. Moreover, monitoring the predominant RF signals used by UAVs provides insights into abnormal behaviors or unauthorized access attempts.

Deep learning, with architectures like CNNs and RNNs, excels in analyzing diverse data streams, from imagery to RF signals, detecting intricate patterns [8]. Recognizing individual method limitations, hybrid systems are emerging, integrating various techniques to enhance UAV behavior detection reliability [32].

While these methods and techniques offer promising results in the field of UAV behavior detection, it is essential to critically assess their merits and potential drawbacks. This evaluation ensures the informed adoption of techniques tailored to specific operational needs and challenges.

2.3 Evaluation of Abnormal Behavior Detection Methods

Abnormal behavior and anomaly detection employ various metrics like accuracy and robustness. However, articles like "Survey on Anomaly Detection using Data Mining Techniques (2015)" [41] and "Anomaly Detection, Analysis and Prediction Techniques in IoT Environment: A Systematic Literature Review (2019)," [12] reveal diverse metric usage across studies, attributed to research focus or application context. This diversity, while underscoring the field's complexity, complicates direct algorithm comparisons.

Our approach to evaluating techniques for abnormal behavior detection is rooted in a thorough examination of existing research. The analysis and insights presented in our evaluation are not standalone; rather, they are built upon the foundation of several comprehensive studies. These studies have played an integral role in informing our methodology and conclusions. The key sources we have drawn upon include the research conducted by V. Chandola et al. [29], Dhiman [9], Xu et al. [42], M. U. Togbe et al. [43], Himeur et al. [8], and Agrawal et al. [41]. By incorporating the findings from these studies, we aim to provide a well-informed and comprehensive assessment of abnormal behavior detection techniques in the context of specific applications.

Nearest neighbor and clustering techniques excel when data forms clear clusters, making them beneficial for drone sensor data in controlled environments. S. Shaw et al. demonstrated that nearest neighbor method can detect anomalies in drones' data with high accuracies close to 100% [47]. Yet, in dynamic settings with complex drone data, their efficiency might decline.

Deep learning techniques show promising overall results, and as demonstrated by V. Bell et al [48]., employing LSTM and autoencoder methods for abnormal behavior detection achieved a precision of 0.793±0.08, a recall of 0.735 ± 0.13, and an accuracy of 0.821 ± 0. 11.

Classification-based techniques, such as Bayesian networks, are precise, but their performance is linked to the availability and quality of data labels, D. Pan et al. [49] modified a S3VM algorithm to achieve a true positive rate of 92.7% and a false positive rate of 8.2%. While Y. Ma et al. introduced a Bayesian network-based GNF for Small Unmanned Aerial Systems (sUAS). On the DLA dataset, GNF achieved a precision of 0.74, recall of 0.92, and F1 score of 0.82, outperforming models like LSTM-NDT (respectively: 0.53, 0.62 and 0.57). In the drone landscape, where real-time events might not always come with labeled data, especially for anomalies, the effectiveness of these techniques could be limited.

Statistical techniques, being unsupervised, work well with lower-dimensional data. But drone sensor data, which often captures a myriad of environmental variables, can be complex. E. d'Afflisio et al. [50] utilized a mean-reverting process (Ornstein-Ulhenbeck process) to simulate planned boat routes using AIS. Their method achieved commendable results in minimizing missed detections and false alarms. As this complexity grows, statistical techniques might struggle, especially if drone data deviates from expected statistical models. The erratic movement of drones complicates the use of these models.

Drawing from Dhiman et al [9], techniques like Trajectory Sparse Reconstruction Analysis, initially for human monitoring, can adapt to drones, focusing on real-time tracking, trajectory analysis, and abrupt changes.

Information theoretic techniques shine when anomalies alter the data's information content. S. Wu et al. [52] introduced two abnormal behavior detection algorithms, ITB-SS and ITB-SP, based on information theoretic principles. When tested on multiple real datasets, mostly sourced from UCI, their performance was measured using the Area Under the Curve (AUC) metric. The algorithms demonstrated superior performance, achieving the highest AUC scores in over half of the real datasets, with many exceeding 0.90. On synthetic datasets, both algorithms consistently delivered perfect AUC scores of 1.0. This notable performance underscores their efficiency and adaptability across varying data scales and dimensions. Given their impressive performance on both real and synthetic datasets, it suggests that these methods might be well-suited for analyzing complex datasets like those generated by drones.

Agrawal et al. [41] highlighted the potential of hybrid methodologies in anomaly detection. The hybrid combination of SVM with k-Medoids consistently outperformed the Naïve Bayes combined with k-Means or k-Medoids. Specifically, for small datasets, SVM achieved an average accuracy of 99.43% compared to NB's 93.87% (k-Means) and 94.25% (k-Medoids). This superiority persisted in larger datasets with SVM's 99.21% accuracy surpassing NB's 84.82% and 88.30%. Furthermore, SVM consistently registered higher detection rates and a false alarm rate under 1%, showcasing its enhanced performance and reliability. In the context of drones, combining techniques could provide a more holistic view of the drone's operations, ensuring that no anomaly, whether it's a rapid descent or a sudden battery drain, goes undetected.

In conclusion, detecting abnormal drone behaviors necessitates diverse techniques given the intricacies of drone operations. A fusion approach may offer comprehensive detection. Yet, a gap exists in literature addressing multi-sensor abnormal behavior detection, possibly due to challenges in integrating data from diverse sensors.

Considering these challenges, how does the literature address data heterogeneity in abnormal behavior detection from multi-sensor UAV systems?

3.0 ADDRESSING HETEROGENEITY IN UAV BEHAVIOR DETECTION

3.1 Data Fusion Levels

In the realm of heterogeneous data, data fusion stands out as a well-developed area of research. It amalgamates information from diverse sources, thereby enhancing the accuracy and reliability of sensors. The foundational principle of data fusion is encapsulated by the Joint Directors of Laboratories (JDL). They define data fusion as a process that refines identity estimates and situational assessments by leveraging information from both individual and multiple sources [1].

Data fusion emerges as an effective tool, combining these diverse data streams and enhancing the decision-making capabilities of systems. However, the indiscriminate or ill-conceived application of fusion can backfire, leading to diminished accuracy [3]. Hence, the data's credibility and the sensors' reliability are essential.

The JDL data fusion model systematically breaks down the fusion process into distinct levels, each tailored for a specific phase of data handling and interpretation. At the foundational Level 0, raw data is collected from various sources and then assigned to appropriate subsequent levels for further use. Level 1 transforms this raw data into individual object representations, akin to prepping ingredients for a meal, ensuring data undergoes necessary calibration, corrections, or filtering. In Level 2, data from diverse sources comes together, reminiscent of assembling a puzzle, to provide a more coherent and detailed depiction of the object or situation at hand. Level 3 interprets the assembled data, deriving conclusions and basing critical decisions on the insights obtained. Lastly, Level 4 operates as the guardian of the process, monitoring the efficiency of the fusion and ensuring optimal operation.

Before delving into the potential of data fusion techniques, it's imperative to first ascertain the current landscape: "Has heterogeneous data been employed for abnormal UAV behavior detection? If so, how?" Furthermore, "Have data fusion methods been previously adopted to enhance abnormal behavior detection capabilities in UAVs?"

Answering these questions will provide a foundation upon which we can further explore the nuances of data fusion in this context and subsequently, how these techniques can be refined to meet the specific challenges associated with detecting abnormal UAV behavior in diverse environments.

To navigate the complexities of abnormal behavior detection, a deep dive into the JDL's data fusion levels is instrumental. For UAV abnormal behavior detection, Level 2 fusion, which focuses on the relationships between objects and their environment, becomes particularly relevant.

The fusion of data is emerging as a key aspect for the effective detection abnormal behaviors. Our survey revealed a major tendency towards fusion techniques. When faced with heterogeneous data, the absence of fusion often stemmed from its perceived complexity or lack of expertise [6, 25].

However, the majority recognized the strength of fusion. Methods such as Dempster-Shafer's evidence theory [15, 16, 17], fuzzy logic [18], and deep learning [19] have been central in combining data from diverse sensors. The fusion process, as seen in articles [17, 20, 21], often combines pre-existing abnormal behavior detection algorithms, magnifying their detection capabilities.

Interestingly, the field's novelty is clear. For instance, the 2018 article titled 'Anomalous behaviour detection based on heterogeneous data and data fusion' [11] stands as a testament to the early stage of fusion in abnormal behavior detection, indicating its innovative nature.

Several authors have shied away from fusion, citing challenges. For example, one article mentioned, "The heterogeneous and dynamic nature of data presents significant challenges to DAD (Deep Anomaly Detection) techniques" [13]. Fahim and Sillitti in 2019 observed, "Our analysis could not find any work based on fusion techniques. Such techniques can provide a robust platform to fuse the sensory data streams and assist the analysis of anomalous behavior." [12]. Furthermore, Erhan et al. [6] highlighted that the convergence of fusion and detection heralds an uncharted research domain, describing it as an "opening avenue of new research issues."

Employing data fusion techniques in abnormal behavior detection offers several compelling advantages. For one, it significantly enhances detection performance by harnessing information from multiple data sources, offering a more complete view of the environment. This approach not only facilitates the integration of diverse modalities like audio, visual, and motion data, enriching the overall detection process, but it also skillfully addresses various data-related challenges [44]. Whether it is handling missing data or navigating the complexities of data uncertainty, data fusion presents a robust solution, ensuring a more comprehensive and accurate detection mechanism.

The journey towards harnessing the full potential of data fusion in UAV abnormal behavior detection is still beginning. It calls for a complex interaction of research, exploration, and innovation.

3.1 Exploring Abnormal Behavior Detection Through Data Fusion Levels

Research into abnormal behavior detection enhanced by data fusion algorithms has been a focal area for years. As early as 2010, Wolfgang Koch mentioned in his article "Selected Tracking and Fusion Applications for the Defense and Security Domain" published in SET-157 NATO-OTAN [44] , that fusion-based anomaly detection improves situational awareness. He also suggested that understanding whether an abnormal behavior is a threat can be done at more advanced stages of data fusion.

S. Wu et al. [3] pioneered an approach leveraging the Piecewise Aggregate Approximation (PAA) algorithm for compressing time series data in wireless sensor networks (WSNs). By fusing this with an advanced unsupervised *K*-Means method and the Artificial Immune System (AIS), the method adeptly discerned between typical and anomalous data points. Impressively, their algorithm boasted a detection rate of 97.23% and a false alarm rate of 3.58%.

In a distinct vein, the paper "Towards Multisensor Data Fusion for DoS detection" [15] harnessed the Dempster-Shafer's Theory of Evidence (D-S) to fuse evidence from a multitude of sensors, ultimately detecting flooding attacks. Their chosen performance metrics, Basic Probability Assignments (bpa's) and the false alarm rate, shed light on the system's efficacy, although a comprehensive comparison with existing methods remained elusive.

The investigation presented in [17] delved deep into large-scale network anomaly detection, spotlighting both the Dempster-Shafer Theory of Evidence and the Principal Component Analysis (PCA) techniques. Their performance metrics diverged from typical standards, emphasizing the sector's need for standardized fused-based detection metrics. Their results demonstrated the strengths of Dempster-Shafer in detecting nuances in UDP packet compositions, while PCA was particularly potent in pinpointing SYN attacks.

Carlos Fernando Crispim Junior and his team [18] embarked on a mission to detect early indicators of dementia in older individuals by fusing video and accelerometer data. Their multi-sensor system astoundingly achieved an average sensitivity of 93.51% and a precision of 63.61%. In contrast, the video-only approach lagged with a sensitivity of 77.23% and a precision of 57.65%.

Dong-Lan LIU et al. [19] integrated deep learning into the fusion framework, focusing on anomaly detection in power big data. Their Multilevel Deep Learning (MDL) method outshone rivals, with metrics such as a

mutual information score of 0.12 and an accuracy surpassing 95%. Furthermore, their false positive and negative rates further accentuated their technique's superiority.

Lastly, the innovative "HMM Based Falling Person Detection Using Both Audio and Video" [26] study underscored the value of multi-sensor fusion. By combining audio and video data, their method not only retained a 100% correct detection rate but also eradicated false detections, recording a 0% false detection rate.

A dedicated table has been constructed to illustrate the relationships between the selected data fusion methods and abnormal behavior detection techniques, providing a quick reference for these associations.

Table 1: Associations of methods in references articles.

Paper No.	Data Fusion	Abnormal Behavior detection
[3]	PAA algorithm + Hybridization of existing methods	K-Means and Artificial Immune System (AIS)
[15]	Dempster-Shafer's Theory of Evidence	Sensors' detection
[17]	Dempster-Shafer's Theory of Evidence	Principal Component Analysis (PCA)
[18]	Decision-Level Fusion Camera + Accelerometer	Recognition and Classification of IADLs using Ontology-Based Modeling
[19]	Deep restricted Boltzmann	Recurrent Neural Networks (RNN)
[20]	Hybridization of 2 existing algorithms	Naive Bayesian classifier and ID3 algorithm
[26]	"AND" operation-based fusion	Hidden Markov Models (HMM)
[27]	Bayesian Network Fusion	Multi-SVM Based Learning

While the above studies have made significant strides in fused-based abnormal behavior detection, a glaring observation is the absence of standardized methods for performance evaluation. Each research work leans on its bespoke metrics, underscoring the need for universally accepted benchmarks in the domain. This absence suggests that the domain would significantly benefit from universally accepted benchmarks in fusion-based abnormal behavior detection. The dilemma is whether to use separate metrics for abnormal behavior detection and data fusion or a combined one. Without standard metrics, comparing algorithms becomes challenging. A potential solution might be using data fusion on the performance metrics, as suggested by Chatzigiannakis et al. [45] in 2006, providing a comprehensive measure of algorithm performance.

Given the identified shortcomings in the literature about heterogeneous-based abnormal behavior detection of UAVs, the discussion naturally gravitates towards data fusion techniques as a promising avenue for enhancing abnormal behavior detection capabilities. This perspective prompts several crucial questions, "Why is there a shortage of articles in the literature that utilize data fusion to enhance abnormal UAV behavior detection?", "Are there inherent challenges specific to UAVs that complicate, or even preclude, the effective application of data fusion techniques?", "How can data fusion techniques be optimized to address the unique challenges of abnormal UAV behavior detection in diverse environments?". By addressing these questions, we aim to uncover any underlying issues and offer insights into how data fusion can be effectively integrated into the process of UAV abnormal behavior detection.

4.0 CHALLENGES AND ISSUES

4.1 Complex Environments and Heterogeneous Data

The environments in which small UAVs operate can be complex and data from different sensors can be heterogeneous. Therefore, data fusion for the detection of abnormal UAV behaviors presents significant challenges, such as managing uncertainty, accounting for sensor variability, and the difficulty of modelling nonlinear relationships. Finally, the limitations of current methods, in particular their ability to manage complex behaviors, may constitute an obstacle to the effective detection of abnormal behavior of UAVs.

Given the intricacies of UAV environments and the diverse nature of sensor data, there is a pressing need to address the challenge of data fusion in this context. How can we develop methods that account for this complexity and variability? Is there a way to bridge the gap between the challenges posed by these environments and the current capabilities of abnormal behavior detection algorithms?

4.2 Non-standardized Performance Measures

Performance measures used in abnormal behavior detection studies vary widely, making it difficult to compare results between different methods. Performance metrics used for anomaly detection include precision, recall, F1 metric and area under the ROC curve (AUC), false alarm rate, time to detection, and more. The lack of standardized performance measures makes it difficult to evaluate and compare the performance of abnormal behavior detection methods and limits the reliability of the results. In fact, it exists well known metrics for detection, tracking and classification algorithm, but how evaluate behavior detection processing for a data fusion system? It is therefore important to develop standardized performance measures to evaluate the performance of abnormal behavior detection methods.

The variability in performance measures across studies calls into question the comparability of results and conclusions drawn from different research papers. What steps can be taken to arrive at a consensus regarding performance metrics in UAV abnormal behavior detection? Is it feasible to establish a comprehensive metric that encapsulates all facets of detection performance?

4.3 Limitations of Current Methods

Despite advances in detecting abnormal behavior of UAVs, there are still significant limitations in current methods. One of the main limitations is the difficulty of managing complex environments and heterogeneous data, which can make anomaly detection difficult or even impossible. Additionally, like said previously, current performance metrics are not standardized, making it difficult to compare the performance of different detection methods. Finally, some current methods may still have limitations in terms of accuracy, processing speed, or cost, which limit their practical use in real-world scenarios. It is therefore necessary to continue research in this field to overcome these limitations and improve the performance of methods for detecting abnormal behavior of UAVs.

The limitations inherent in current methods highlight areas of opportunity for researchers in the field. Are there innovative approaches yet to be explored that can bridge these gaps? How can we build upon current methodologies to enhance their accuracy, efficiency, and applicability in diverse UAV scenarios?

5.0 EXPERIMENTATION

5.1 Simulation

In this study, five distinct abnormal behavior detection algorithms were selected for testing: Logistic Regression, Isolation Forest, One-Class SVM, Random Forest Classifier, and Gradient Boosting Classifier. Among these, Logistic Regression is a statistical method traditionally used for binary classification problems, while Isolation Forest, an unsupervised algorithm, focuses on isolating anomalies. The selection of these algorithms was based on their efficacy in classification tasks and their ability to offer a comprehensive preliminary evaluation of the impact of data fusion on abnormal behavior detection.

The data used for this study was harvested from the CARLA [34] simulator, a renowned open-source platform tailored for autonomous driving research. CARLA meticulously mimics real-world scenarios, with real-world behavior, offering data from various sensors such as radar, lidar, cameras, and GPS. In our experiment, radar and lidar sensors, stationed at identical locations with a range of 100m, collected the data. During the data acquisition phase, the sensors remained stationary.

The experiments aimed to identify the proficiency of the selected abnormal behavior detection algorithms on radar, lidar, and data fused from both sensors. Standard metrics like accuracy, precision, recall, and F1-score gauged the performance. The core objective was to deduce if fused data improves the efficacy of the abnormal behavior detection algorithms compared to singular sensor data.

Our dataset comprised lidar and radar data from 100 simulated vehicles and pedestrians in CARLA, including 10 instances of abnormal behavior. This data encompassed both positions and velocities of the subjects. We employed the Joint Probabilistic Data Association Filter (JPDAF) for data fusion, enabling us to generate object tracks and fused data to enhance the performances of our abnormal behavior detection algorithms.

The system was carefully designed to detect unusual behaviors, highlighting specific features. While the radar data was clear, the lidar data showed typical real-world sensor noise. Using CARLA, the simulation depicted a roadway where vehicles and pedestrians acted normally, following traffic rules. We added abnormal behaviors to the dataset, like erratic speeds, sudden lane changes, ignoring signals, or causing collisions.

The anomalies were intentionally obvious, ensuring algorithms could identify between standard and abnormal behaviors. This methodological choice was central to establish a clear benchmark for algorithmic efficiency. Any failure to identify these pronounced anomalies would spotlight the algorithm's weaknesses.

5.2 Results

The performance metrics for Logistic Regression, Isolation Forest, One-Class SVM, Random Forest Classifier, and Gradient Boosting Classifier were comprehensively evaluated using standard metrics such as accuracy, precision, recall, and F1-score.

Table 2: Performance comparison of abnormal behavior detection algorithms.

Data Source	Algorithm	Accuracy	Precision	Recall	F1-score
Radar	Logistic Regression	0.90	0.94	0.76	0.81
Lidar		0.90	0.86	0.51	0.49
Fused		0.90	0.94	0.78	0.83
Radar	Isolation Forest	0.83	0.78	0.64	0.67
Lidar		0.43	0.52	0.55	0.37
Fused		0.85	0.82	0.67	0.71
Radar	One-Class SVM	0.78	0.70	0.76	0.72
Lidar		0.23	0.51	0.52	0.23
Fused		0.88	0.81	0.84	0.82
Radar	Random Forest	0.93	0.90	0.91	0.90
Lidar		0.73	0.55	0.60	0.54
Fused		1.00	1.00	1.00	1.00
Radar	Gradient Boosting	0.96	0.93	0.94	0.93
Lidar		0.75	0.57	0.65	0.57
Fused		0.99	0.99	0.97	0.98

The comparative analysis reveals several significant trends. Firstly, data fused from both radar and lidar consistently outperforms using either radar or lidar alone across all algorithms. The Gradient Boosting algorithm, when applied to fused data, achieves near-perfect scores across all metrics, indicating its strong compatibility with fused datasets for this task. Additionally, a graphical representation of these performances is provided in the appendix.

6.0 CONCLUSION

The domain of abnormal behavior detection in Unmanned Aerial Vehicles (UAVs) has seen significant advancements and transformations. Our exploration began with a thorough understanding of the current state-of-the-art methodologies in Section 2. We uncovered a myriad of techniques, each with its unique strengths, challenges, and applications. From model-based methods to data-driven approaches, the landscape of abnormal behavior detection is both diverse and intricate. Yet, the application of these methods to small UAVs presents its set of challenges, underscoring the need for further research and evaluation.

As we ventured into Section 3, the concept of data fusion emerged as a beacon of hope for addressing the heterogeneity inherent in UAV behavior detection. Through a meticulous examination of data fusion techniques and levels, we discerned its potential in enhancing decision-making capabilities and navigating the complexities of diverse data streams. The literature clearly hinted at a trend towards fusion techniques, yet the field's novelty and the challenges associated with fusing heterogeneous data were evident.

Our journey into Section 4 unveiled the multifaceted challenges that plague the domain. From grappling with complex environments and heterogeneous data to the lack of standardized performance metrics, each challenge presents a barrier to the effective detection of abnormal UAV behavior. Yet, within these challenges lie opportunities for innovation, exploration, and refinement of methodologies.

In Section 5, our empirical analysis brought forth illuminating insights. The experiments conducted underscored the transformative potential of data fusion in the realm of abnormal behavior detection. The efficacy of fused data in elevating the performance of detection algorithms was undeniable. Yet, it is crucial to remember that these findings, though promising, are based on simulated environments. The real world, with its unpredictability and chaos, might present scenarios that are starkly different.

Reflecting on our research, the implications for the defense and security sectors are profound. The capability to enhance abnormal behavior detection transcends academic interest; it resonates with real-world applications that can potentially fortify security paradigms. As we forge ahead, the focus should be on grounding these experiments in real-world scenarios, optimizing methodologies to adapt to unforeseen challenges, and continually refining our understanding of UAV behavior in diverse contexts.

7.0 REFERENCE

[1] Joint Directors of Laboratories, "Data Fusion Lexicon.", 1991.

[2] B. Khaleghi et al., "Multisensor data fusion: A review of the state-of-the-art", Information Fusion, 2013.

[3] X. Guo et al., "An Anomaly Detection Based on Data Fusion Algorithm in Wireless Sensor Networks", International Journal of Distributed Sensor Networks, 2015.

[4] D. L. Hall et al., "An Introduction to Multisensor Data Fusion", PROCEEDINGS OF THE IEEE, 1997.

[5] F. Castanedo, "A Review of Data Fusion Techniques," The Scientific World Journal, 2013.

[6] L. Erhan et al., "Smart Anomaly Detection in Sensor Systems: A Multi-Perspective Review," Information Fusion, 2021.

[7] N. C. Tay et al., "A Review of Abnormal Behavior Detection in Activities of Daily Living," IEEE Access, 2023.

[8] Y. Himeur et al., "Artificial intelligence-based anomaly detection of energy consumption in buildings: A review, current trends and new perspectives," Applied Energy, 2021.

[9] C. Dhiman et al., "A review of state-of-the-art techniques for abnormal human activity recognition," Engineering Applications of Artificial Intelligence, 2019.

[10] A. Sidibé et al., "Study of Automatic Anomalous Behaviour Detection Techniques for Maritime Vessels," Journal of Navigation, 2017.

[11] A. M. Ali et al., "Anomalous behaviour detection based on heterogeneous data and data fusion, " Soft Computing, 2018.

[12] M. Fahim et al., "Anomaly Detection, Analysis and Prediction Techniques in IoT Environment: A Systematic Literature Review," IEEE Access, 2019.

[13] R. Chalapathy et al., "Deep Learning for Anomaly Detection: A Survey", arXiv:1901.03407, 2019.

[14] K. Wolsing et al., "Anomaly Detection in Maritime AIS Tracks: A Review of Recent Approaches," Journal of Marine Science and Engineering, 2022.

[15] C. Siaterlis et al., "Towards multisensor data fusion for DoS detection", Proceedings of the 2004 ACM symposium on Applied computing, 2004.

[16] C. Thanh et al., "Data Fusion-Based Network Anomaly Detection towards Evidence Theory," 2019 6th NAFOSTED Conference on Information and Computer Science, 2019.

[17] V. Chatzigiannakis et al., "Data fusion algorithms for network anomaly detection: classification and evaluation," 2007.

[18] C. F. Crispim-Junior et al., "A Multi-Sensor Approach for Activity Recognition in Older Patients," 2012.

[19] D.-L. Liu et al., "A Multilevel Deep Learning Method for Data Fusion and Anomaly Detection of Power Big Data," EEEIS, 2017.

[20] D. M. Singh et al., "Combining Naive Bayes and Decision Tree for Adaptive Intrusion Detection," International journal of Network Security & Its Applications, 2010.

[21] C. OReilly et al., "Anomaly Detection in Wireless Sensor Networks in a Non-Stationary Environment," IEEE Communications Surveys & Tutorials, 2014.

[22] J. Zhang et al., "An Abnormal Behavior Detection Based on Deep Learning," 2018 IEEE SmartWorld, 2018.

[23] M. Hervas et al., "Abnormal Behavior Detection: A Comparative Study of Machine Learning Algorithms Using Feature Extraction and a Fully Labeled Dataset," IEEE, 2019.

[24] J. Audibert et al., "USAD: UnSupervised Anomaly Detection on Multivariate Time Series," ACM, 2020.

[25] D. Arifoglu et al., "Detection of abnormal behaviour for dementia sufferers using Convolutional Neural Networks," Artificial Intelligence in Medicine, 2019.

[26] B. U. Töreyin et al., "HMM Based Falling Person Detection Using Both Audio and Video," Computer Vision in Human-Computer Interaction, 2005.

[27] Y. Chen et al., "Abnormal Behavior Detection by Multi-SVM-Based Bayesian Network," 2007 International Conference on Information Acquisition, 2007.

[28] F. J. Anscombe, "Rejection of Outliers," Technometrics, 1960.

[29] V. Chandola et al., "Anomaly detection: A survey", ACM Computing Surveys, 2009.

[30] J. Liang et al., "Detection of Malicious Intent in Non-cooperative Drone Surveillance," 2021 Sensor Signal Processing for Defence Conference (SSPD), 2021.

[31] Y. Shi et al., "Abnormal Ship Behavior Detection Based on AIS Data," Applied Sciences, 2022.

[32] Pannetier et al., "A comparative study of joint video tracking and classification for countering unmanned aerial vehicles," Automatic Target Recognition XXXIII, 2023.

[33] H. Cai et al., "CUDM: A Combined UAV Detection Model Based on Video Abnormal Behavior," Sensors, 2022.

[34] A.Dosovitskiy et al., "CARLA: An Open Urban Driving Simulator," Proceedings of the 1st Annual Conference on Robot Learning, 2017.

[35] X. Tian et al., "An Abnormal Behavior Detection Method Leveraging Multi-modal Data Fusion and Deep Mining," 2021.

[36] D. Zhang et al., "Research on abnormal behavior target tracking algorithm in airport intelligent video surveillance", 2017 International Conference on Progress in Informatics and Computing (PIC), 2017.

[37] S. Jovanoska et al., "Passive Sensor Processing and Data Fusion for Drone Detection," Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE, 2021.

[38] P. K. Vaddi et al., "Dynamic Bayesian Networks based abnormal event classifier for nuclear power plants in case of cyber security threats," Progress in Nuclear Energy, 2020.

[39] R. R. Guillén et al., "A Review of Deep Learning Methods for Detection of Gatherings and Abnormal Events for Public Security," UCAmI 2022.

[40] H. Ahn et al., "Learning-Based Anomaly Detection and Monitoring for Swarm Drone Flights," Sciences, 2019.

[41] S. Agrawal et al., "Survey on Anomaly Detection using Data Mining Techniques," Procedia Computer Science, 2015.

[42] Xiaodan Xu et al., "Recent Progress of Anomaly Detection", Complexity, 2019.

[43] Togbe et al., "Etude comparative des méthodes de détection d'anomalies," Revue des Nouvelles Technologies de l'Information, 2020.

[44] W. Koch, “Selected Tracking and Fusion Applications for the Defence and Security Domain,” 2010.

[45] V. Chatzigiannakis et al., “On the realization of a generalized data fusion and network anomaly detection framework,” Fifth International Symposium on Communication Systems, Networks and Digital Signal Processing, 2006.

[46] J.P. Yaacoub et al. “Security analysis of drone systems: Attacks, limitations, and recommendations,” Internet of Things, vol. 11, 2020.

[47] S. Shaw et al., “Anomaly Detection in Drones with Machine Learning Algorithms,” in Futuristic Communication and Network Technologies, Electrical Engineering, vol. 792, Springer, 2022.

[48] V. Bell et al., “Anomaly detection for unmanned aerial vehicle sensor data using a stacked recurrent autoencoder method with dynamic thresholding”, arXiv preprint, 2022.

[49] D. Pan et al., “UAV Anomaly Detection Using Active Learning and Improved S3VM Model,” International Conference on Sensing Measurement & Data Analytics in the era of Artificial Intelligence, 2020.

[50] E. d’Afflisio et al., “Detecting anomalous deviations from standard maritime routes using the Ornstein–Uhlenbeck process,” IEEE Transactions on Signal Processing, 2018.

[51] R. Chitrakar et al., “Anomaly detection using Support Vector Machine classification with k-Medoids clustering,” Third Asian Himalayas International Conference on Internet, 2012.

[52] S. Wu and S. Wang, “Information-Theoretic Outlier Detection for Large-Scale Categorical Data,” IEEE Transactions on Knowledge and Data Engineering, 2013.

Appendix 1 : PERFORMANCE GRAPHS

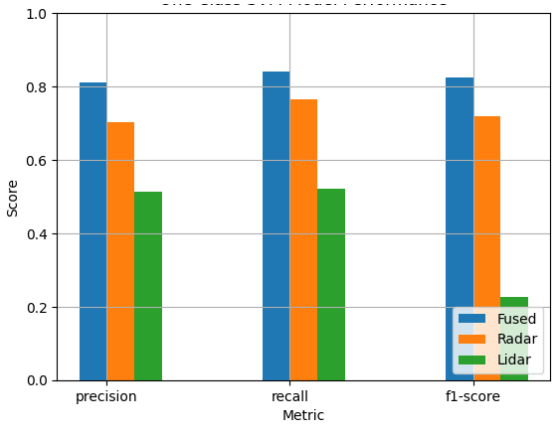

Figure 1: One Class SVM

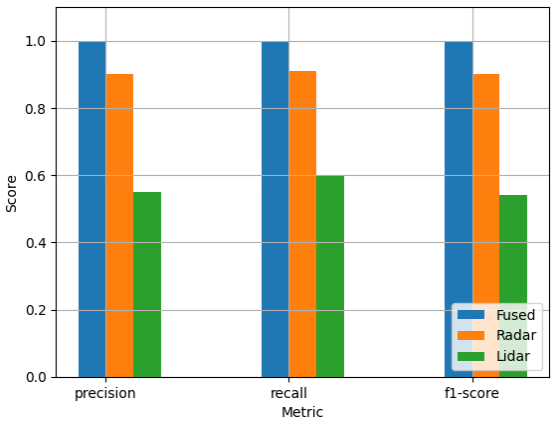

Figure 2: Random Forest Classifier

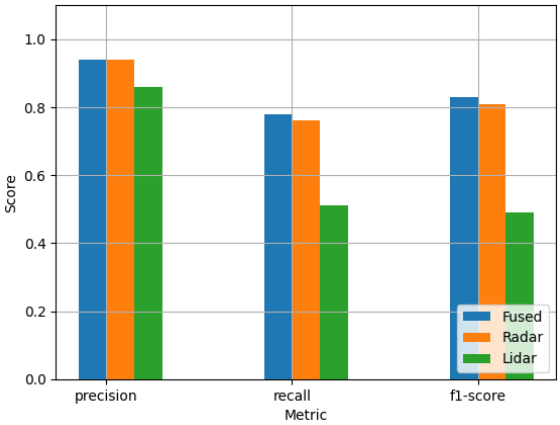

Figure 3: Logistic Regression

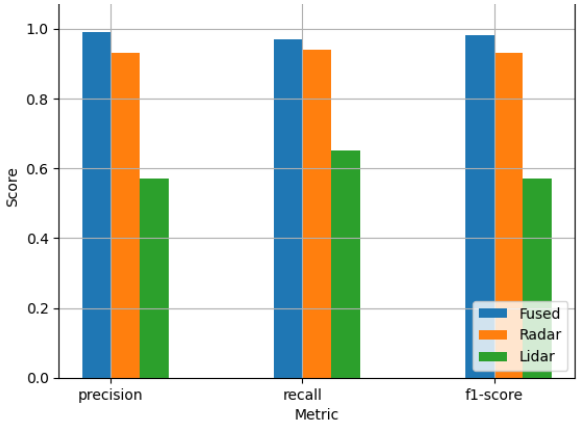

Figure 4: Gradient Boosting Classifier

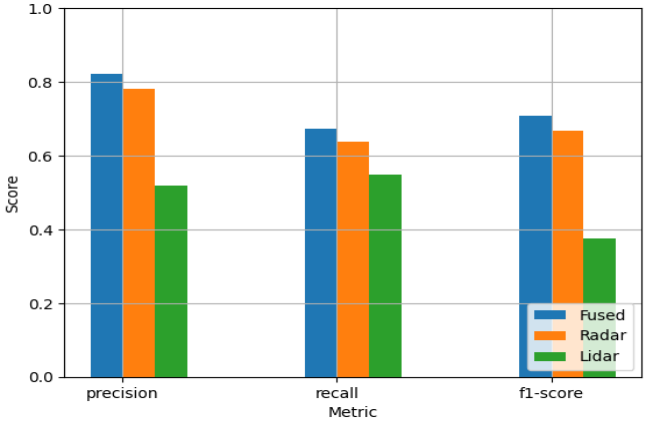

Figure 5: Isolation Forest Model Performance.