ENSEMBLE MACHINE LEARNING FOR UAV NETWORK INTRUSION DETECTION:

Comprehensive Analysis Using the UAV- NIDD Dataset

Authors :

Mr. Anis CHARFI **Ms. Samiha Ayed** **Ms. Lamia Chaari Fourati** **Mr. Georgi Tsochev**

LIST3N, University of Technology of Troyes France **IMT Atlantique, Labsticc - Brest, France**

CRNS-SM@RTS Laboratory **Faculty of Computer Systems and Control - Technical University of Sofia**

Lisbon, Portugal
06/11/2025

Research Environment

Host institution:

utt
UNIVERSITÉ DE TECHNOLOGIE
TROYES

MEMBER OF

EUROPEAN UNIVERSITY
OF TECHNOLOGY

Research lab:

LIST3N
Computer Science
& Digital Society

PLAN

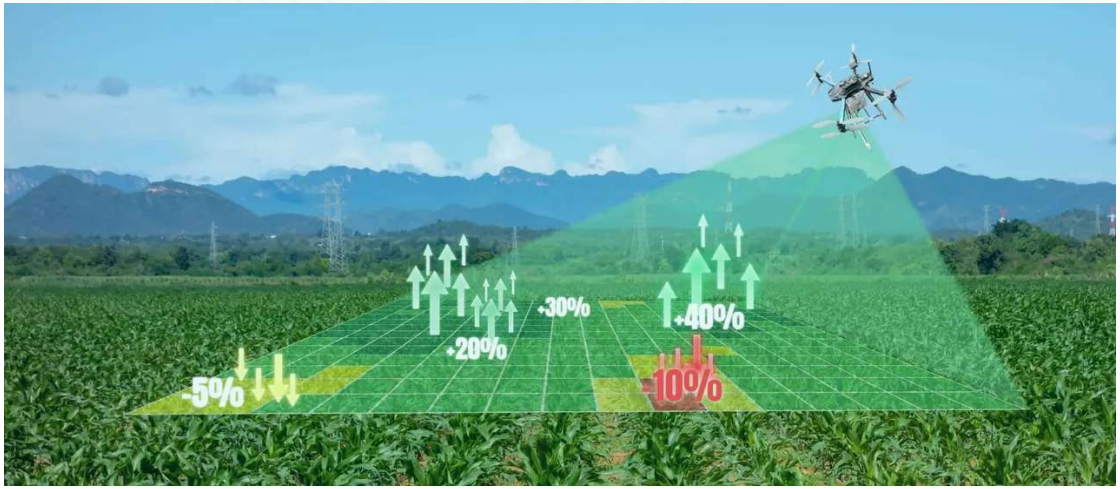
01

Introduction

Agricultural Drones in Modern Farming

Growing Role of Drones in Agriculture

- **Precision farming:** Target the application of fertilizers, pesticides, and water



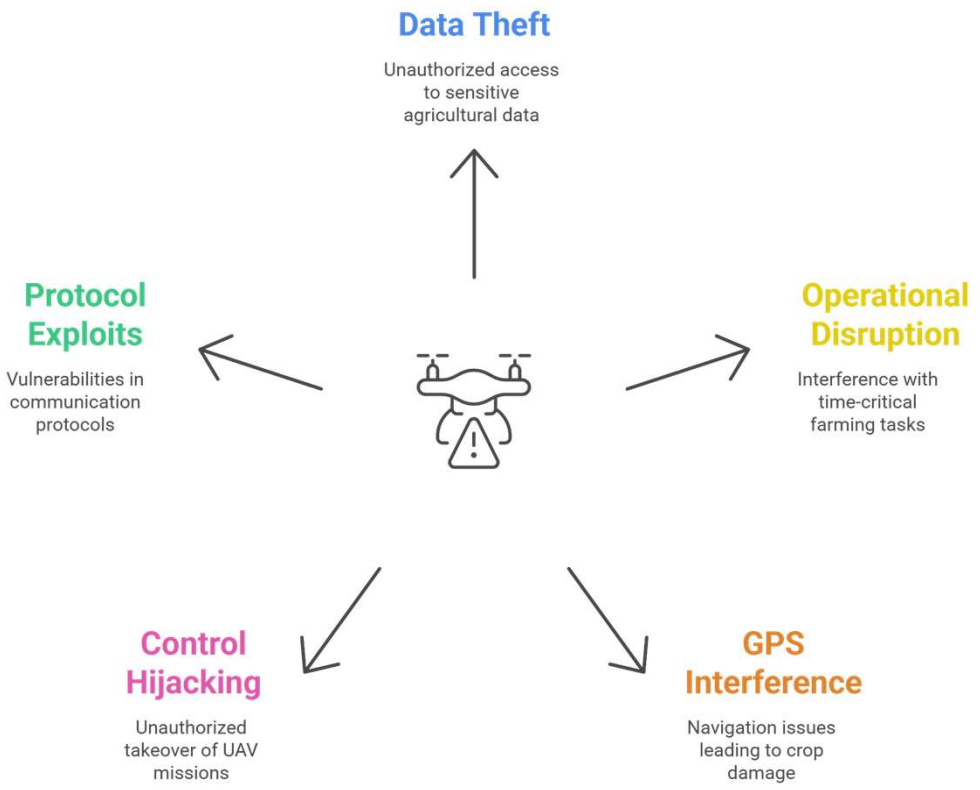
- **Crop monitoring:** Real-time assessment of plant health and growth (food security)

Explosive Market Growth and results

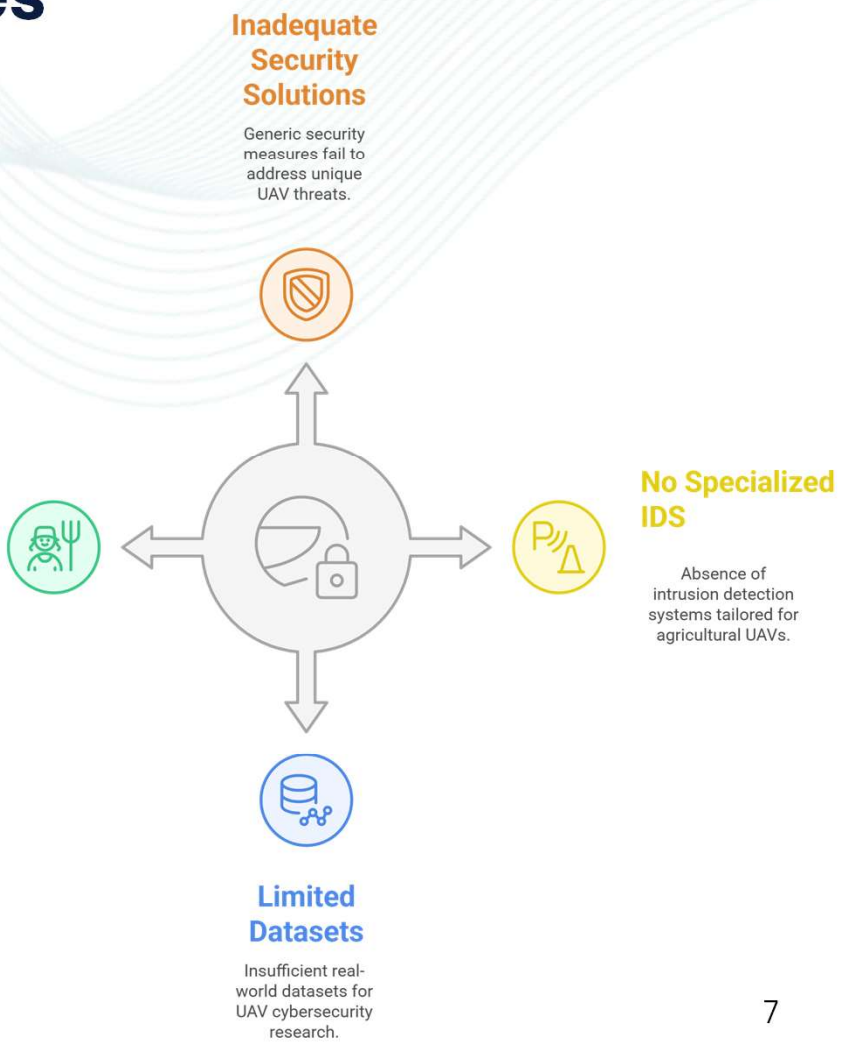
Challenge : Mitigate vulnerabilities in connected agricultural systems

Problem Statement & Security Challenges

Threats to Agricultural UAVs

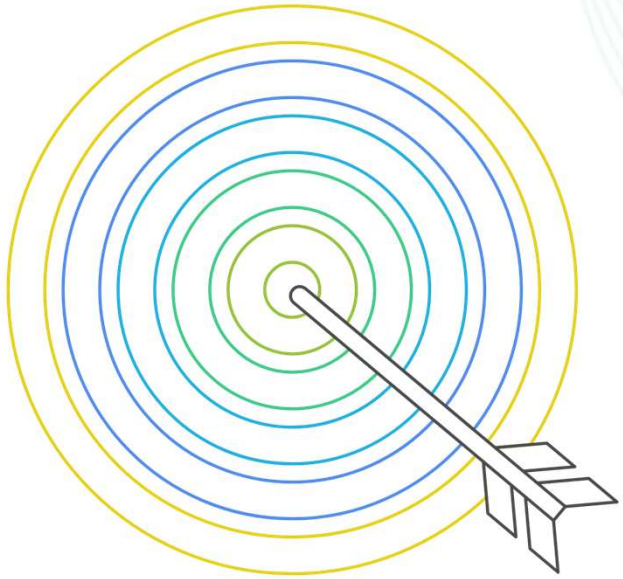


Current Limitations



02

Objectives



Quality Standards

Ensures validity and repeatability

Easy to Use

Farmers can operate the system

Real-time Detection

Protects drones during flight

Stable Performance

Maintains consistency across tests

Detect 90% of attacks correctly

Ensures comprehensive attack detection

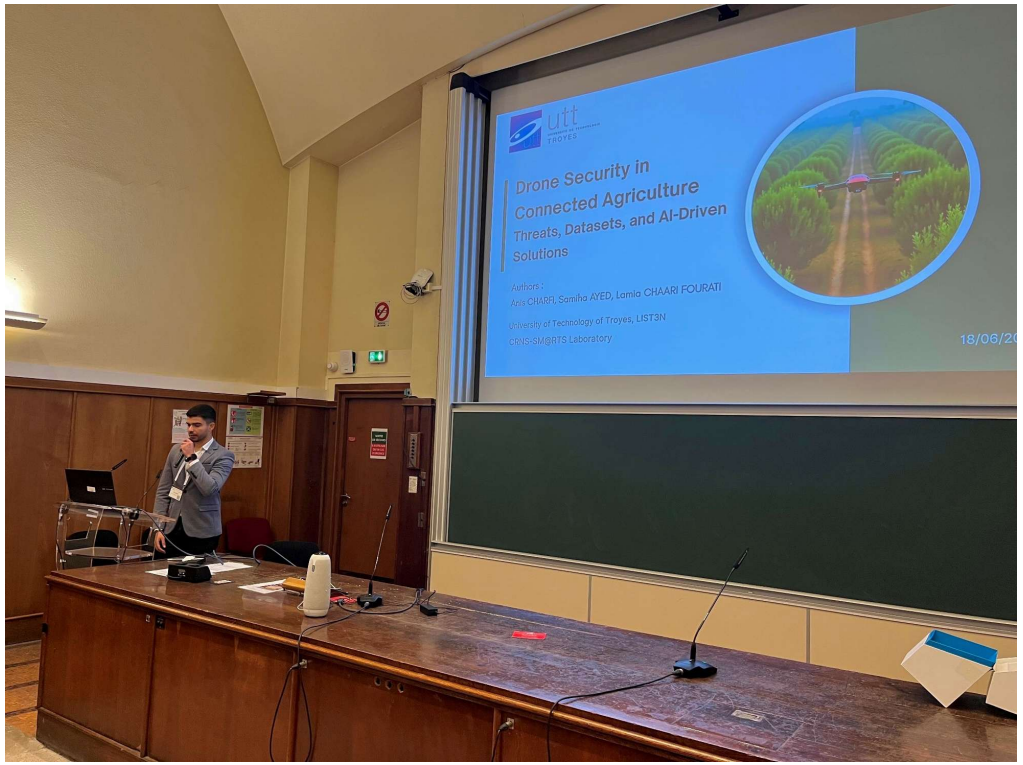
03

State of Art

Research Paper (State Of Art)

IFIP NTMS, Paris, France, June 2025

Research paper title : Drone Security in Connected Agriculture: Threats, Datasets, and AI-Driven Solutions



State of the Art - AI Techniques for UAV Security

Existing Research Categories

AI Technique	Representative Studies	Methods Used	Key Findings	Limitations
ML-Based Approaches	ML approaches for UAVs widely studied (AL-Syouf et al., 2024)	SVM, Random Forest, Neural Networks	Good for known attack pattern, 70-85% typical accuracy	❌Limited to general datasets ❌Single algorithm focus
Deep Learning	ConvLSTM for drone attacks widely adopted (Alzahrani, 2024)	CNN-LSTM, ConvLSTM, RNN-based approaches	Up to 99% accuracy, Excellent pattern recognition	❌High computational requirements ❌Limited UAV-specific datasets
Federated Learning	FELIDS framework for Agri-IoT (Ferrag et al., 2022)	DNN, CNN, RNN, Distributed training	• 93.29% DNN, 94.09% CNN, 94.15% RNN, Privacy-preserving collaboration	❌Communication overhead ❌Limited UAV-specific applications
Reinforcement Learning	UAV-assisted applications with RL (Adil et al., 2023)	Q-learning, Deep Q-networks	Dynamic adaptation capability, Good for resource allocation	❌Training complexity ❌Limited security-focused applications

State of the Art - Dataset Landscape

Dataset Landscape

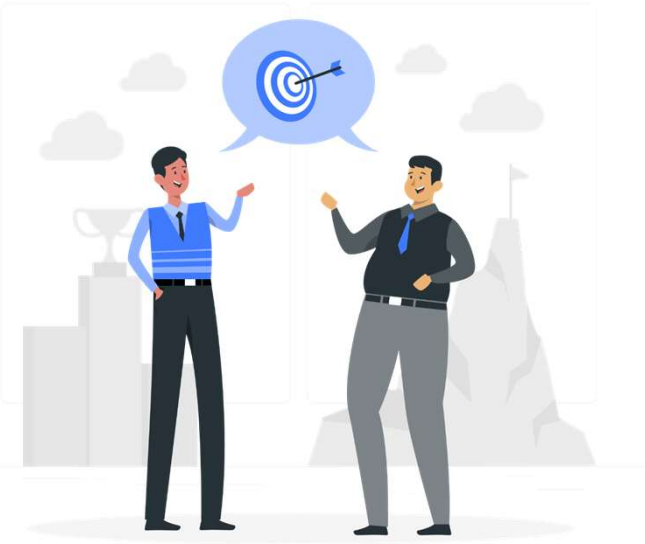
Dataset	Focus	Attack Types	UAV-Specific?	Reference
CICIDS2018	General network intrusion	Multiple network attacks	❌No	Sharafaldin et al., (2018)
X-IIoTID	Industrial IoT security	IoT-specific attacks	⚠ Partial	Al-Hawawreh et al., (2018)
ToN_IoT	IoT/IIoT networks	IoT network attacks	⚠ Partial	Moustafa, N. (2021)
Bot-IoT	IoT botnet detection	Botnet activities	⚠ Partial	Koroniotis et al., (2019)
WSN-DS	Wireless sensor networks	WSN-specific attacks	❌No	Almomani et al., (2016)
UAV-NIDD	UAV network intrusion	UAV-specific attacks	✅ Yes	Hadi, H. J. et al., (2025)

04

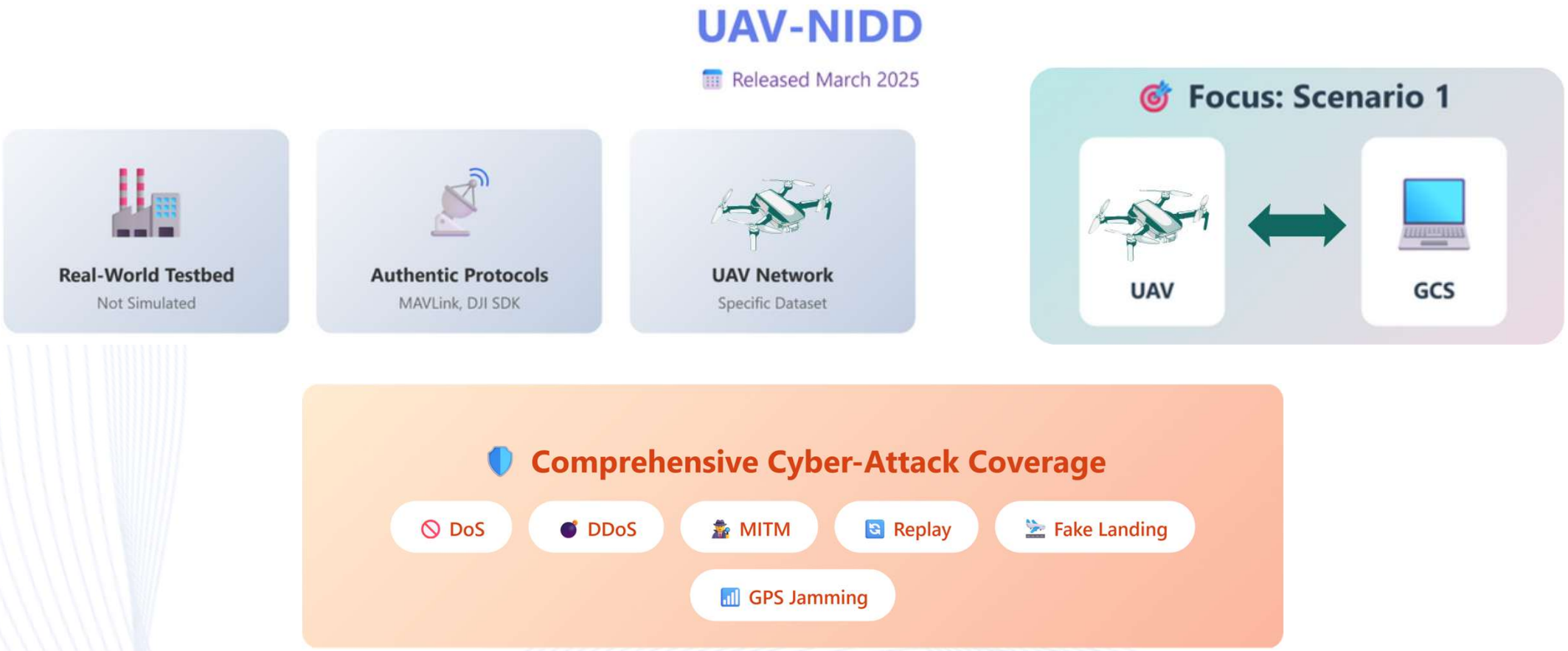
Proposed Approach

Goal: Define project objectives and success criteria

- **Literature review and gap analysis :** identified lack of UAV-specific IDS and datasets
- **Dataset selection:** UAV-NIDD chosen as most relevant and realistic
- **Success criteria:** focus on macro-averaged F1-score, especially for critical attacks



UAV-NIDD Dataset – Basis for Our Research



Materials & Collection Setup

- Real UAVs: PX4 Vision Dev Kit, DJI Mini 3 Pro, DJI Mavic Air Ground
- Control Stations: 2 laptops Tools:
- Wireshark, Aircrack-ng, Tcpdump, Nmap, LOIC, HOIC, Recon-ng

(a) DJI Mavic Air

(b) DJI Mini 3 Pro

(b) PX4 Vision Dev Kit v1.5

Exploration of the Dataset

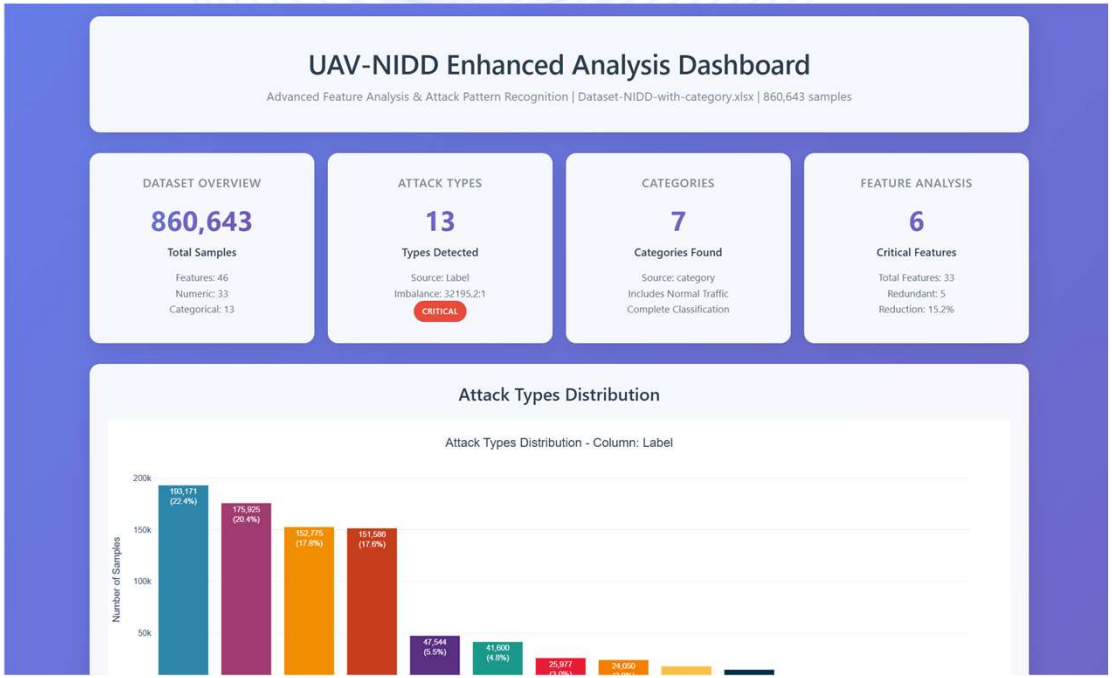
Implementation of dashboard for visual statistics

Purpose of the Dashboard:

- Provide a visual and interactive overview of UAV-NIDD data. Help quickly detect anomalies,
- imbalances, and feature correlations.

Dashboard Features:

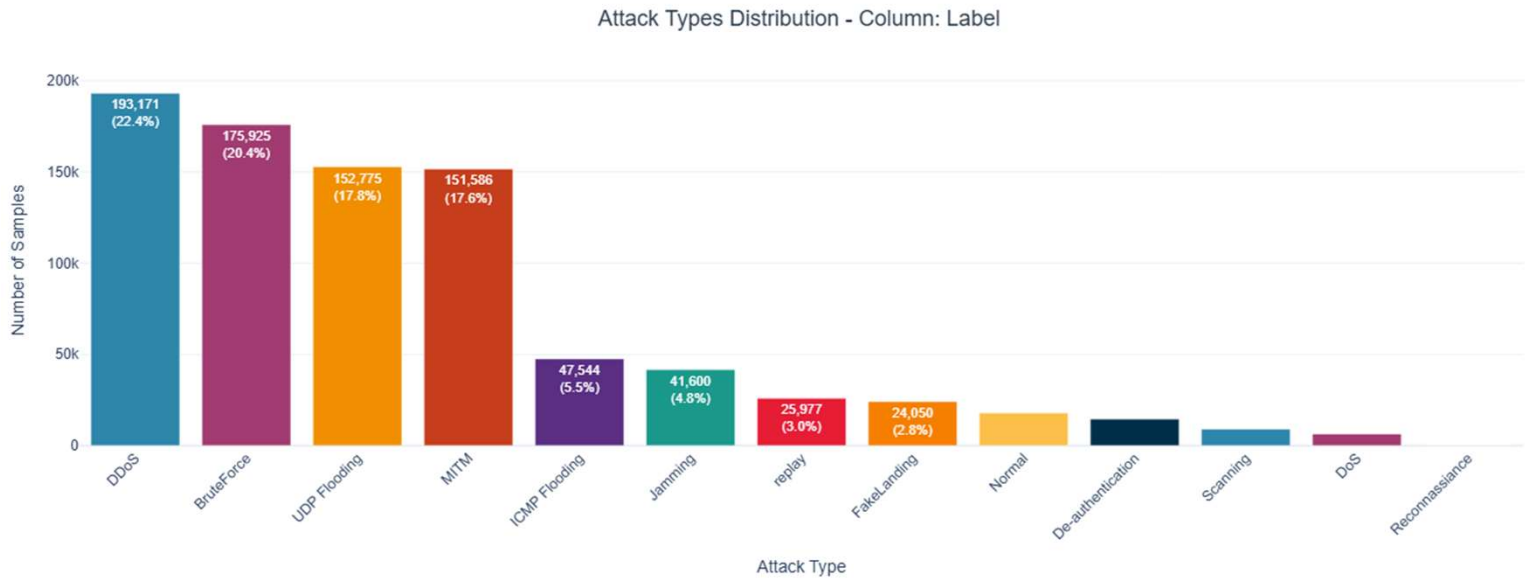
- Class distribution visualization. Correlation
- heatmap for feature relationships. Imbalance
- ratio detection between classes.



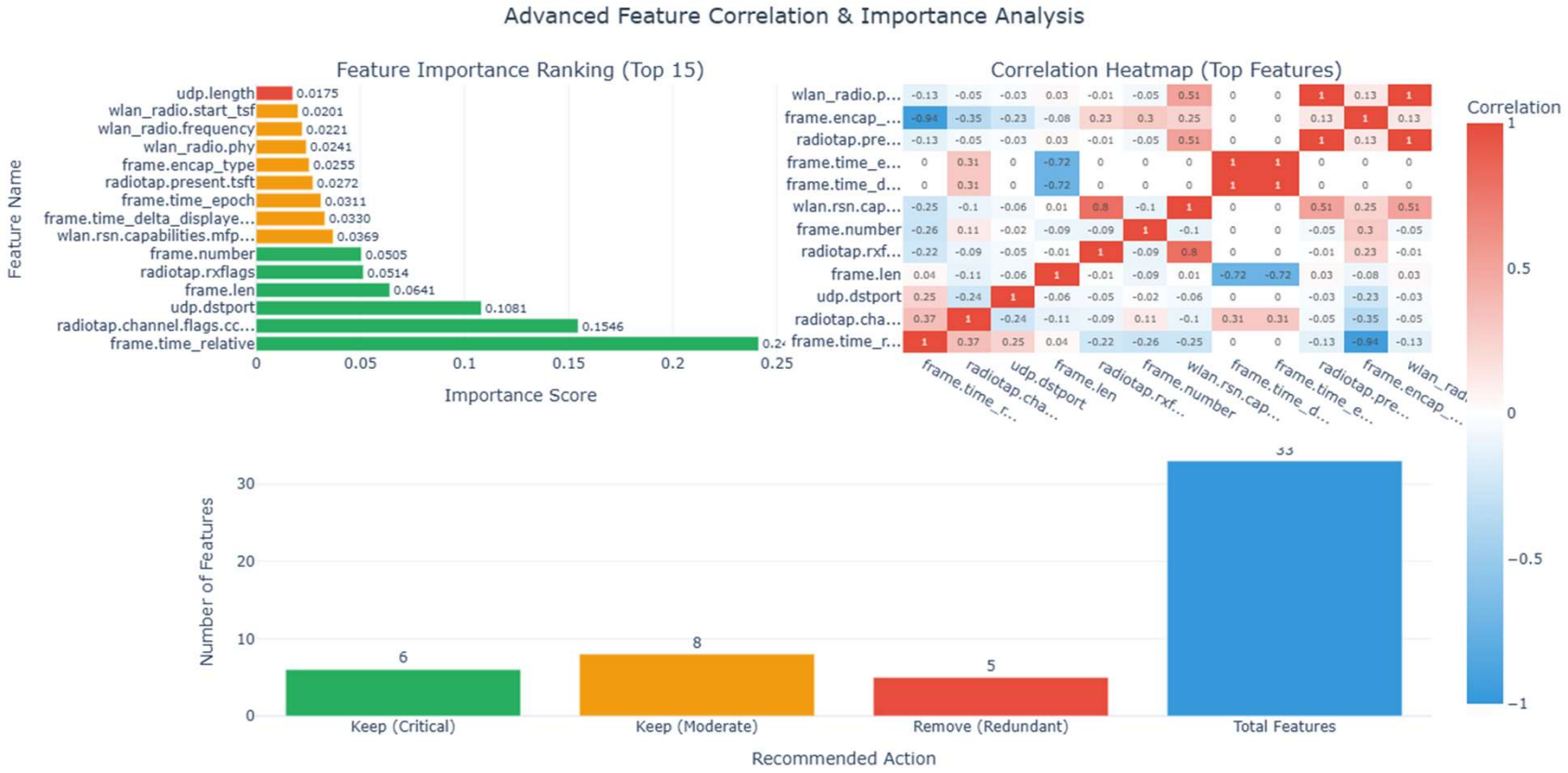
Findings from Data Understanding

Main Observations:

- **Severe Class Imbalance:**
  - Ratio is high compared to rarest class.
- **Reconnaissance Attack Issue:**
  - Only 6 samples, statistically irrelevant so it will be removed from modeling.

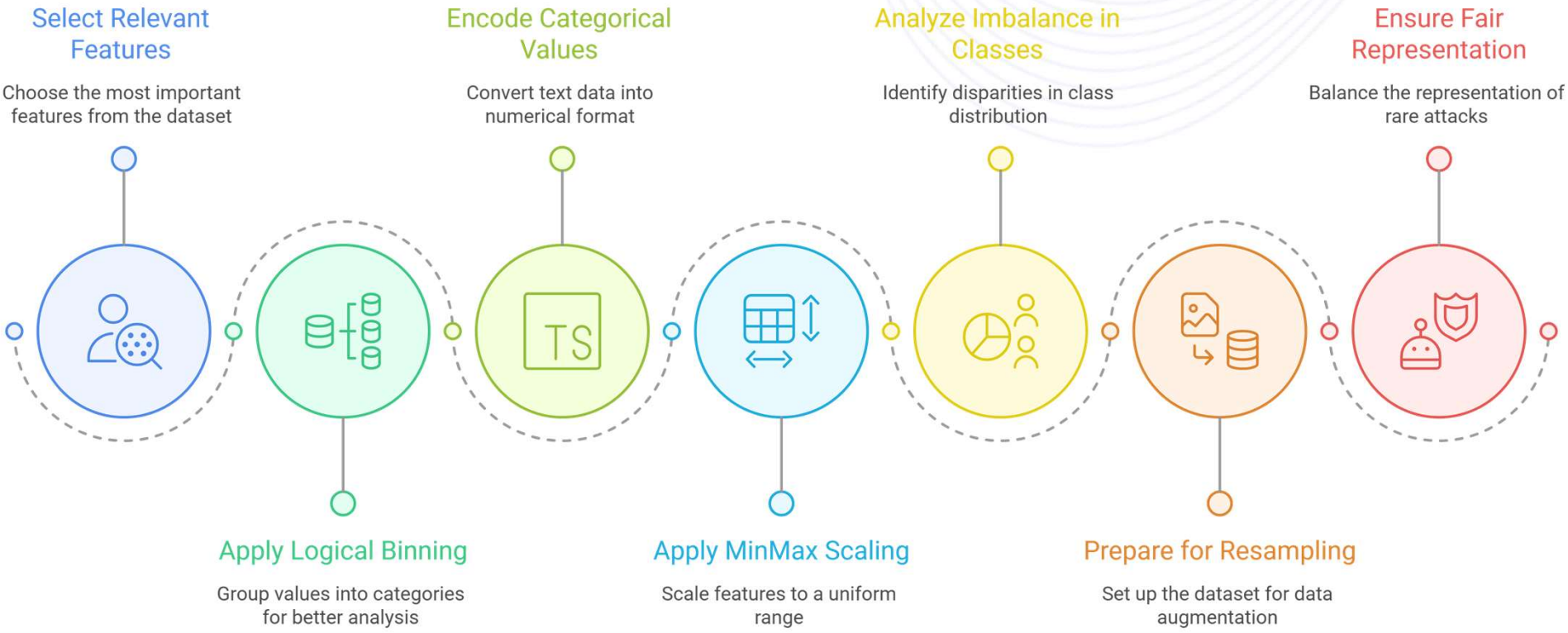


- **Feature Correlations:**
  - Some features highly correlated so there is a potential of redundancy.



Data Preparation (Process & Strategy)

Goal : TransformrawUAVnetworkdataintofeaturessuitable forMLmodeling with our Dual-Path Strategy:



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	frame.len	otap.channel.flags	wlan.seq	radiotap.dbm_antsignal	radiotap.rxflags	n.rsn.capabilities.n	radiotap.length	an.fcs.bad_checksu	wlan.tag	wlan_radio.frequency	wlan_radio.phy	udp.srcport	Label	category
2	Small_Data	No_Modulation	0	No_Signal_Data	Low_Range	Low_Range	Low_Range	No_Errors	0	Low_Range	Low_Range	No_UDP_Traffic	Normal	Normal
3	Medium_D	Normal_Timing	0	No_Signal_Data	Low_Range	Low_Range	Low_Range	No_Errors	0	Low_Range	Low_Range	DHCP_Service	Normal	Normal
4	Medium_D	Normal_Timing	0	No_Signal_Data	Low_Range	Low_Range	Low_Range	No_Errors	0	Low_Range	Low_Range	DHCP_Service	Normal	Normal
5	Control_Fra	Normal_Timing	0	No_Signal_Data	Low_Range	Low_Range	Low_Range	No_Errors	0	Low_Range	Low_Range	No_UDP_Traffic	Normal	Normal
6	Control_Fra	Normal_Timing	0	No_Signal_Data	Low_Range	Low_Range	Low_Range	No_Errors	0	Low_Range	Low_Range	No_UDP_Traffic	Normal	Normal
7	Control_Fra	Normal_Timing	0	No_Signal_Data	Low_Range	Low_Range	Low_Range	No_Errors	0	Low_Range	Low_Range	No_UDP_Traffic	Normal	Normal
8	Small_Data	Normal_Timing	0	No_Signal_Data	Low_Range	Low_Range	Low_Range	No_Errors	0	Low_Range	Low_Range	MAVLink_UAV	Normal	Normal
9	Small_Data	Normal_Timing	0	No_Signal_Data	Low_Range	Low_Range	Low_Range	No_Errors	0	Low_Range	Low_Range	MAVLink_UAV	Normal	Normal
10	Small_Data	Normal_Timing	0	No_Signal_Data	Low_Range	Low_Range	Low_Range	No_Errors	0	Low_Range	Low_Range	MAVLink_UAV	Normal	Normal
11	Control_Fra	Normal_Timing	0	No_Signal_Data	Low_Range	Low_Range	Low_Range	No_Errors	0	Low_Range	Low_Range	No_UDP_Traffic	Normal	Normal
12	Control_Fra	Normal_Timing	0	No_Signal_Data	Low_Range	Low_Range	Low_Range	No_Errors	0	Low_Range	Low_Range	Application_Port	Normal	Normal
13	Small_Data	Normal_Timing	0	No_Signal_Data	Low_Range	Low_Range	Low_Range	No_Errors	0	Low_Range	Low_Range	No_UDP_Traffic	Normal	Normal
14	Small_Data	Normal_Timing	0	No_Signal_Data	Low_Range	Low_Range	Low_Range	No_Errors	0	Low_Range	Low_Range	Application_Port	Normal	Normal
15	Small_Data	Normal_Timing	0	No_Signal_Data	Low_Range	Low_Range	Low_Range	No_Errors	0	Low_Range	Low_Range	No_UDP_Traffic	Normal	Normal
16	Small_Data	Normal_Timing	0	No_Signal_Data	Low_Range	Low_Range	Low_Range	No_Errors	0	Low_Range	Low_Range	No_UDP_Traffic	Normal	Normal
17	Small_Data	Normal_Timing	0	No_Signal_Data	Low_Range	Low_Range	Low_Range	No_Errors	0	Low_Range	Low_Range	MAVLink_UAV	Normal	Normal

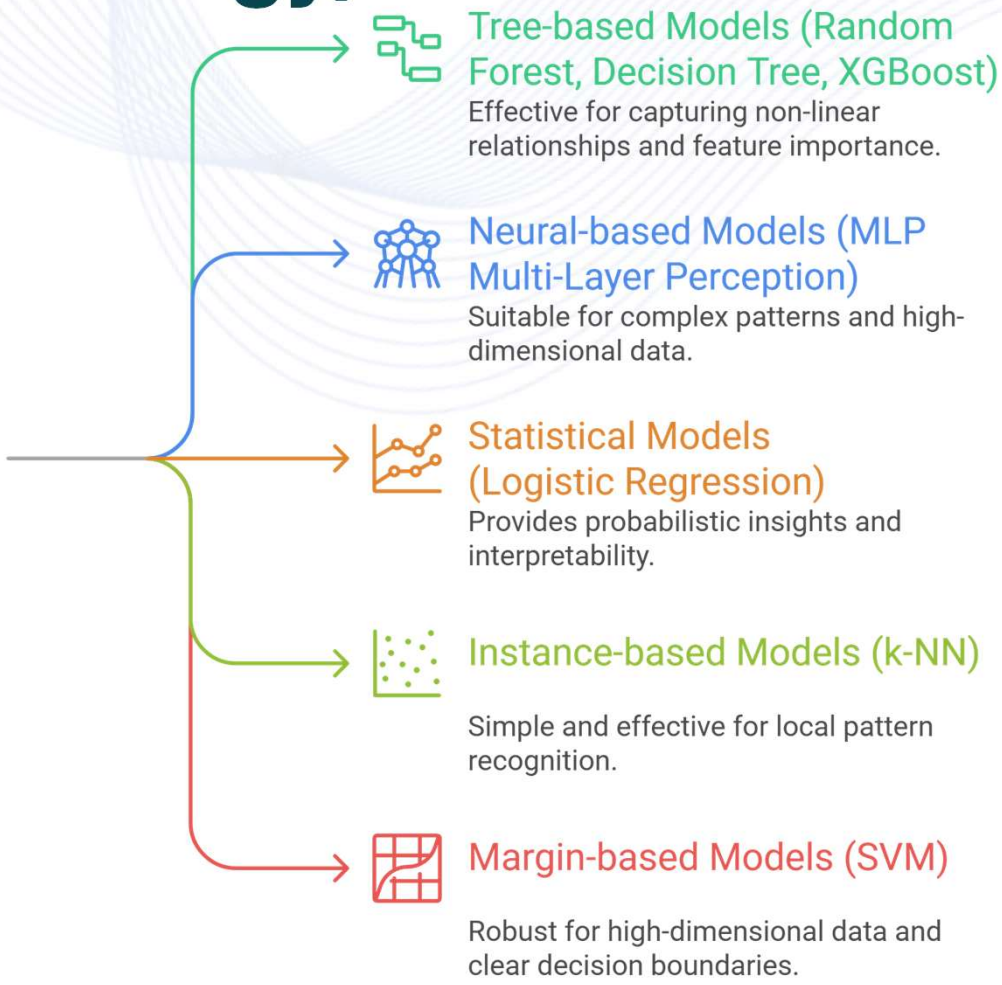
UAV-NIDD Dataset After Feature Selection and Binning

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	frame.len	radiotap.channel.flags.cck	wlan.seq	radiotap.dbm_antsignal	radiotap.rxflags	wlan.rsn.capabilities.mfpc	radiotap.length	an.fcs.bad_checksu	wlan.tag	wlan_radio.frequency	wlan_radio.phy	udp.srcport	Label	category
2	5	3	0	2	1	1	1	4	0	1	1	4	8	3
3	4	4	0	2	1	1	1	4	0	1	1	1	8	3
4	4	4	0	2	1	1	1	4	0	1	1	1	8	3
5	0	4	0	2	1	1	1	4	0	1	1	4	8	3
6	0	4	0	2	1	1	1	4	0	1	1	4	8	3
7	0	4	0	2	1	1	1	4	0	1	1	4	8	3
8	5	4	0	2	1	1	1	4	0	1	1	3	8	3
9	5	4	0	2	1	1	1	4	0	1	1	3	8	3
10	5	4	0	2	1	1	1	4	0	1	1	3	8	3
11	0	4	0	2	1	1	1	4	0	1	1	4	8	3
12	0	4	0	2	1	1	1	4	0	1	1	0	8	3
13	5	4	0	2	1	1	1	4	0	1	1	4	8	3
14	5	4	0	2	1	1	1	4	0	1	1	0	8	3
15	5	4	0	2	1	1	1	4	0	1	1	4	8	3
16	5	4	0	2	1	1	1	4	0	1	1	4	8	3

Encoded UAV-NIDD Dataset After Encoding

Modeling (Process & Strategy)

Algorithm Selection (7 models, different families)

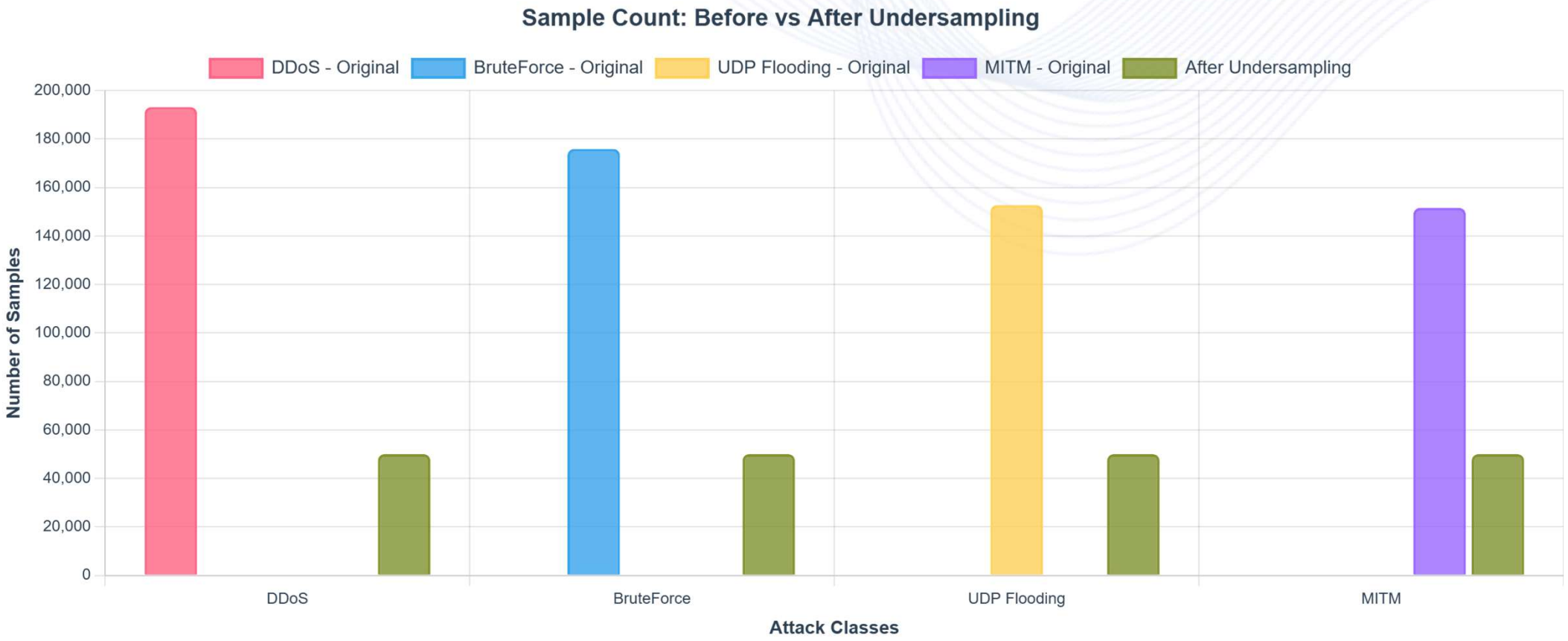


Approach One : Performance on Raw UAV-NIDD Dataset

Model	Accuracy	Precision	Recall	F1-Score
Random Forest	0.92	0.80	0.76	0.78
Decision Tree	0.90	0.78	0.74	0.76
XGBoost	0.91	0.79	0.75	0.77
MLP	0.89	0.76	0.72	0.74
Logistic Regression	0.88	0.74	0.70	0.72
kNN	0.89	0.75	0.71	0.73
Linear SVM	0.87	0.73	0.69	0.71

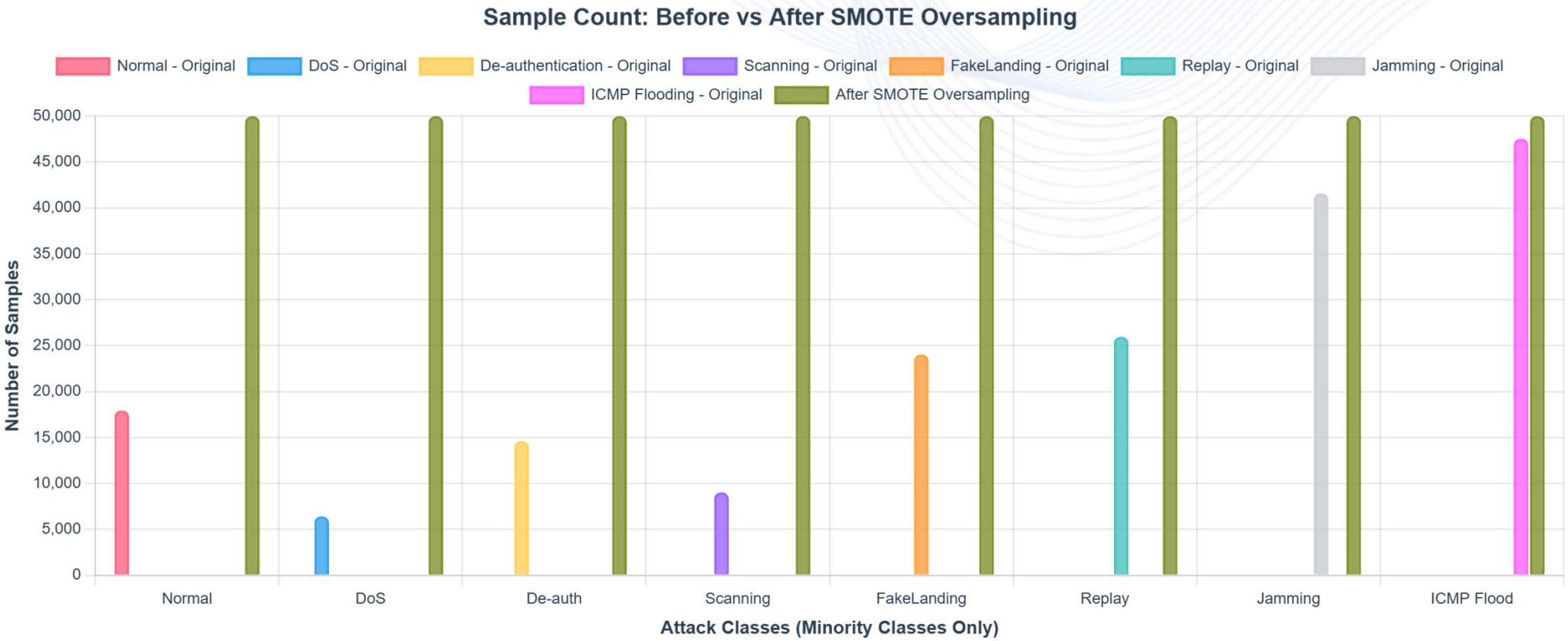
Resampling Strategy – Addressing Class Imbalance

Step 1 : RandomUnderSampler



Resampling Strategy – Addressing Class Imbalance

Step 2 : Advanced Oversampling



Approach Two : Performance after SMOTE

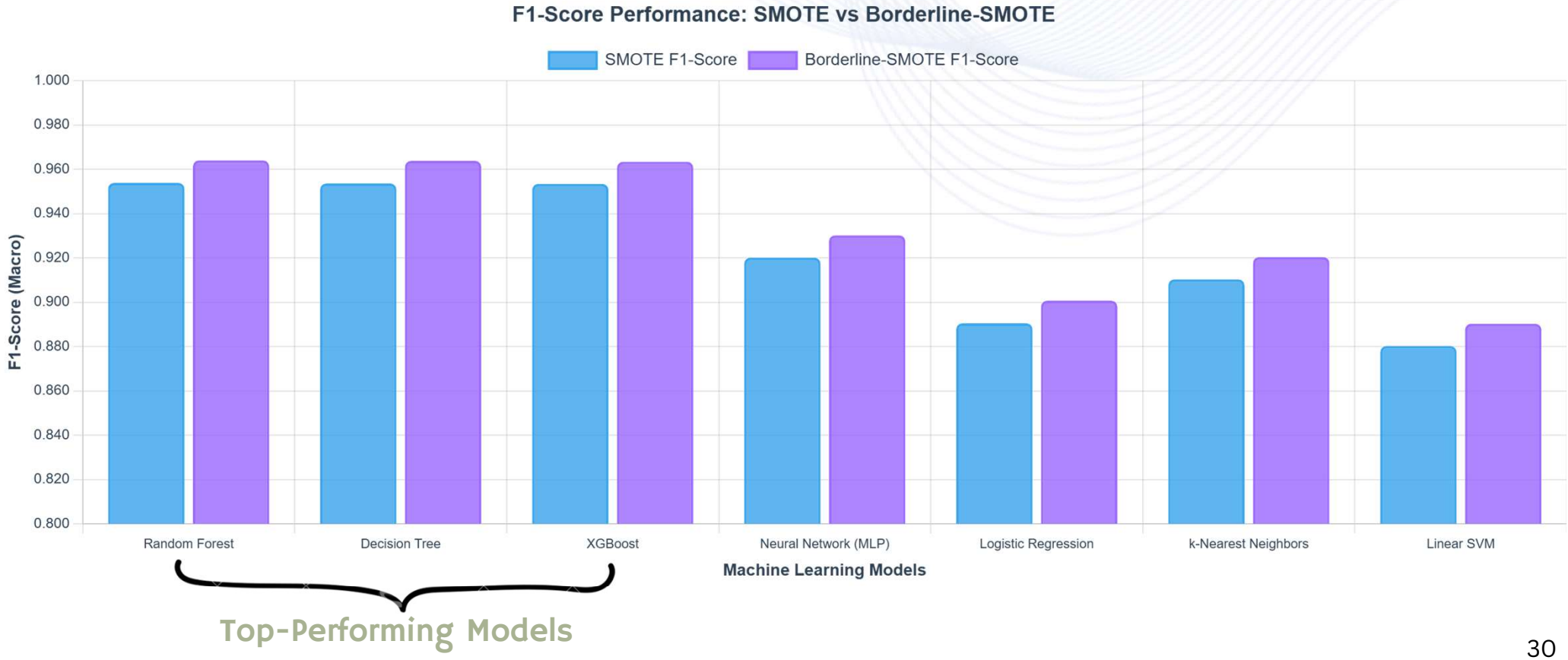
Model	Accuracy	Precision	Recall	F1-Score
Random Forest	0,95	0,95	0,95	0,9539
Decision Tree	0,95	0,95	0,95	0,9536
XGBoost	0,95	0,95	0,95	0,9534
MLP	0,92	0,92	0,92	0,9201
Logistic Regression	0,89	0,89	0,89	0,8905
kNN	0,91	0,91	0,91	0,9103
Linear SVM	0,88	0,88	0,88	0,8802

Approach Three : Performance after Borderline-SMOTE

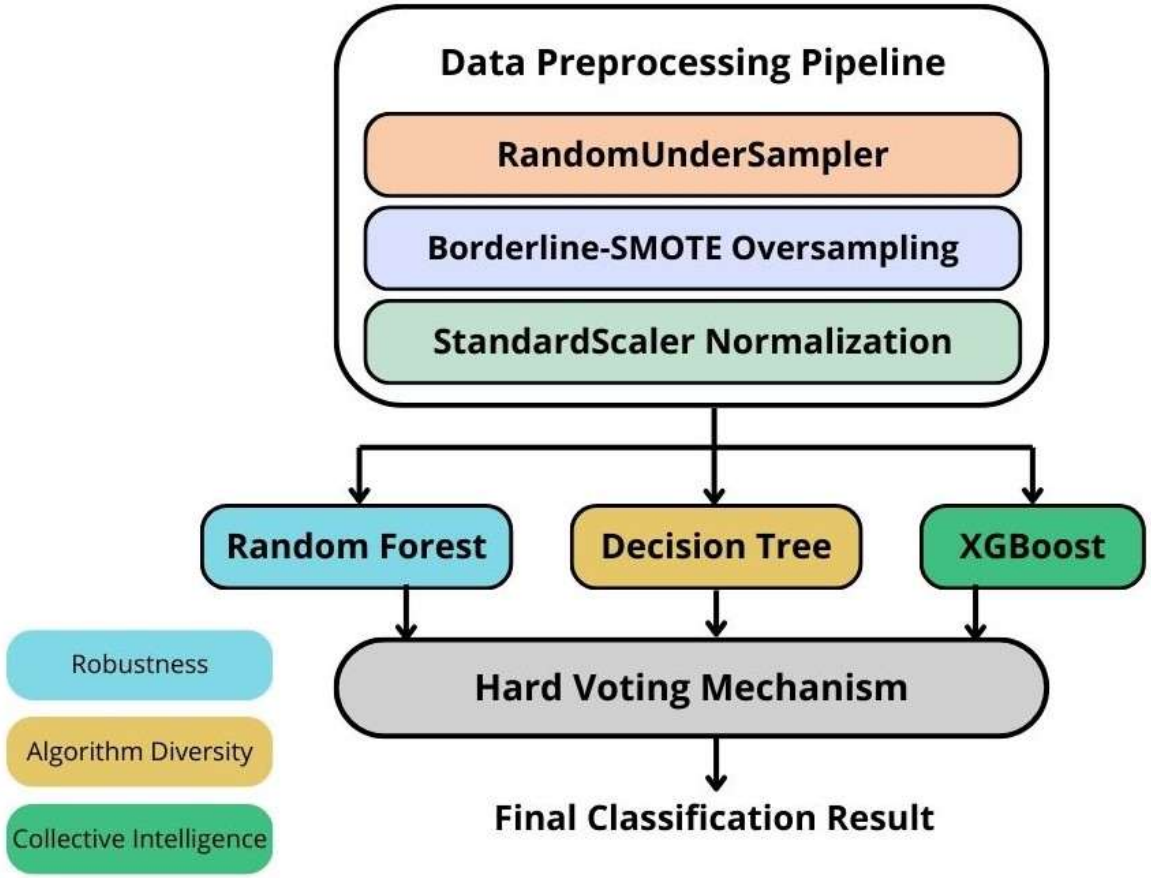
Model	Accuracy	Precision	Recall	F1-Score
Random Forest	0,96	0,96	0,96	0,9640
Decision Tree	0,96	0,96	0,96	0,9638
XGBoost	0,96	0,96	0,96	0,9634
MLP	0,93	0,93	0,93	0,9302
Logistic Regression	0,90	0,90	0,90	0,9007
kNN	0,92	0,92	0,92	0,9204
Linear SVM	0,89	0,89	0,89	0,8903

SMOTE VS Borderline-SMOTE

The winner is : Borderline-SMOTE !



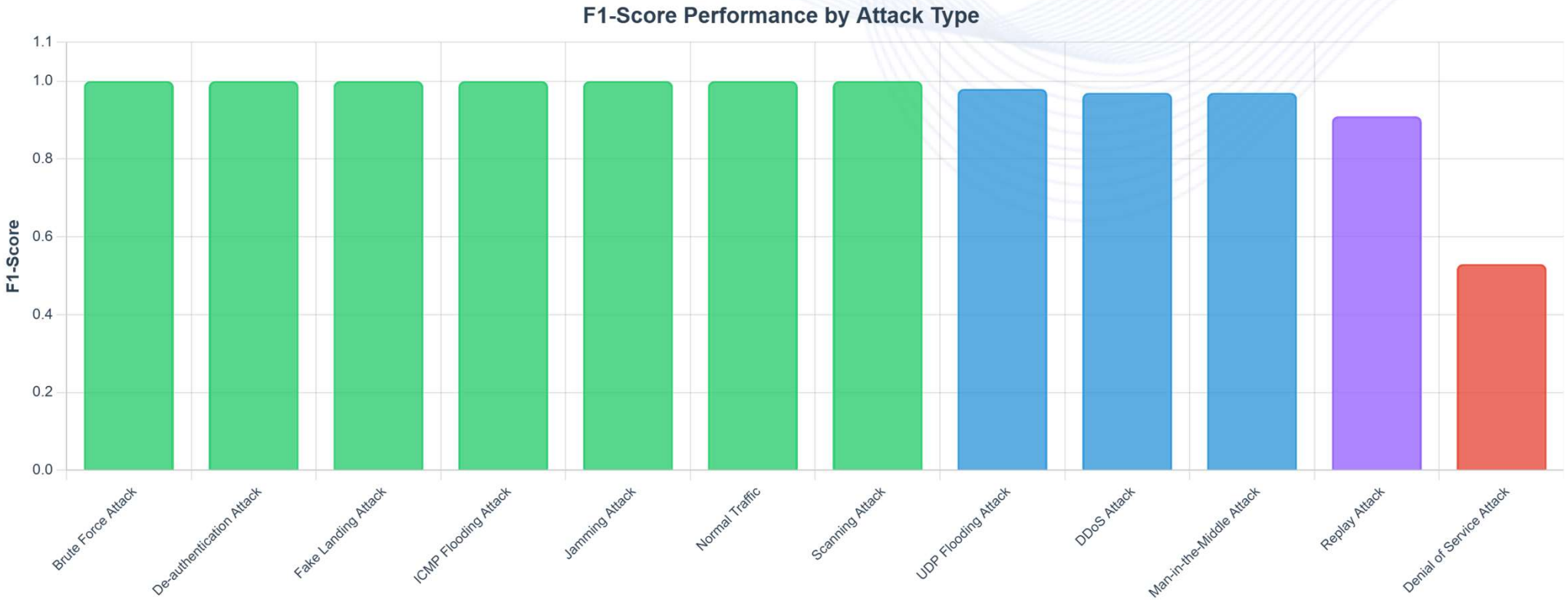
Ensemble Learning Model design



Final Results of Ensemble Learning Model

Attack Type	Precision	Recall	F1-Score	Support
DDoS	1.00	1.00	1.00	38634
Normal	1.00	1.00	1.00	3590
GPS Spoofing	0.98	0.97	0.97	5423
MITM	0.96	0.95	0.96	3241
Brute Force	0.95	0.94	0.95	2876
De-authentication	0.94	0.93	0.94	1987
Fake Landing	0.93	0.92	0.93	1654
ICMP Flooding	0.92	0.91	0.92	1432
Replay	0.91	0.90	0.91	987
Evil Twin	0.90	0.89	0.90	876
Scanning	0.89	0.88	0.89	765
DoS	0.45	0.63	0.53	1285
Macro Avg	**0.95**	**0.95**	**0.95**	**172129**

F1-Score Performance Per Class



DoS Attack Detection Challenge: Root Cause Analysis

Insufficient Training Data → Poor Generalization → Low F1-Score

05

Critical Analysis & Future Work

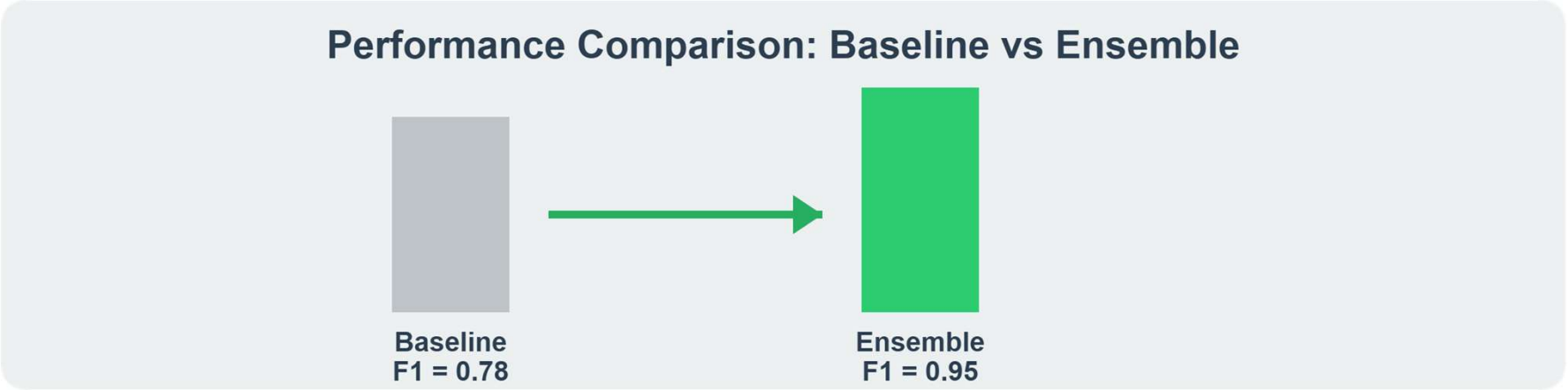
Ensemble Learning Model Performance

Overall Accuracy
98.4%

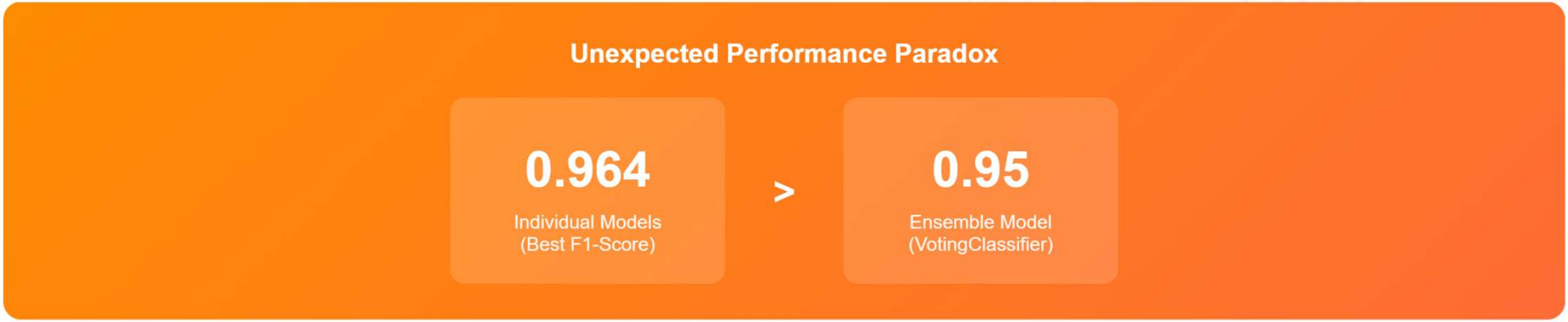
Macro Precision
0.95

Macro Recall
0.96

Improvement
+21.8%



Ensemble Learning Model Performance



Identical Training Environment

All three models (Random Forest, Decision Tree, XGBoost) were trained on the same balanced dataset created using Borderline-SMOTE preprocessing, resulting in highly similar decision patterns.

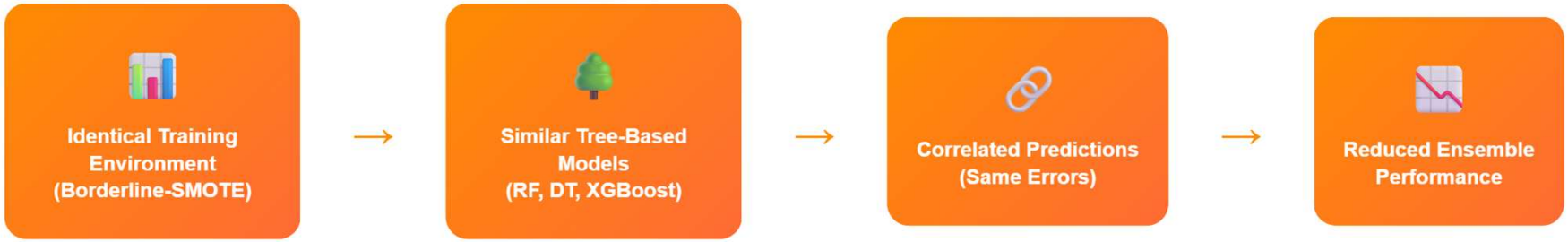
- Same synthetic samples generated through Borderline-SMOTE technique
- Identical feature distributions across all three models
- Similar tree-based architectures interpret features in comparable ways
- Uniform class balancing creates consistent learning patterns

Correlated Error Patterns

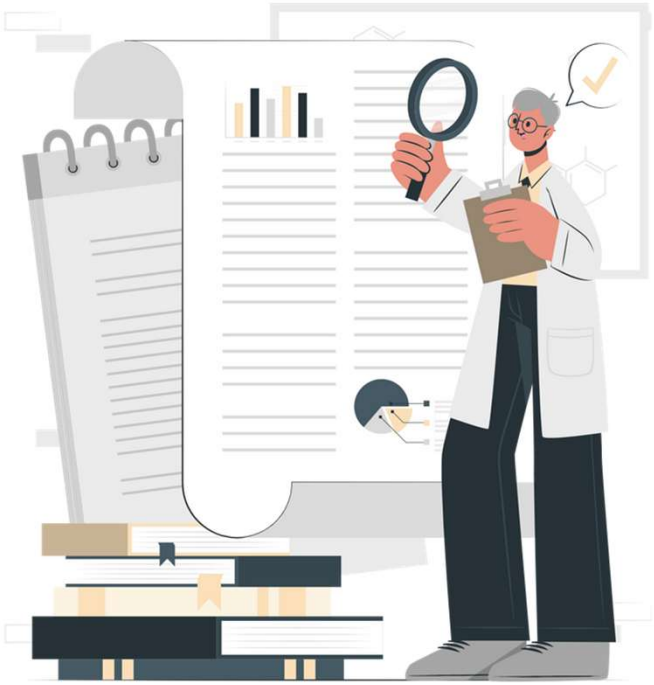
When models make similar errors on the same instances, the ensemble voting mechanism cannot correct these mistakes - instead, it reinforces them through majority consensus.

- All three models failed on identical challenging instances
- Majority voting amplifies shared mistakes rather than correcting them
- No diversity in prediction disagreements to enable error correction
- Consensus on wrong predictions reduces overall performance

Error Correlation Mechanism



Perspectives for Improvement



Future Research Directions

Immediate Improvements

- **Broaden datasets with new UAV types & protocols**
- **Improve ensemble by mixing diverse models**
  (trees + neural nets)
- **Train models on different feature subsets**
  for robustness

Advanced Research

Multi-modal security framework:

- Detect anomalies in UAV sensors
  (physical layer attacks)
- Link IDS with farm management systems
  for context
- Correlate with environment data
  to reduce false alarms

Real-World Deployment

- **Optimize IDS for edge computing on UAVs**
- **Enable real-time automated threat response**
- **Integrate with agricultural IoT infrastructure**

06

Conclusion

Conclusion

Main Achievement :

- Developed AI-based IDS for agricultural UAV communications Achieved F1-
- score of 0.95, exceeding target of 0.90 by 21.8% improvement

Technical Contributions :

- Ensemble model combining Random Forest, Decision Tree, and XGBoost
- Borderline-SMOTE technique for handling class imbalance Detects 11
- different attack types effectively

Impact :

- Our approach enhances food security and sustainability by protecting UAV-driven precision agriculture tasks

Thank you for your attention !

Any Questions?

https://github.com/AnisCharfi/UAV-NIDD-IDS-Analysis

anischarfi2001@gmail.com ayed.samiha@gmail.com lamiachaari1@gmail.com gtsochev@tu-sofia.bg