BGP Buster:
Hybrid Feature Selection and Explainable Machine Learning for BGP Anomaly Detection

Shadi Motaali, Jorge E. López de Vergara, Luis de Pedro
Universidad Autónoma de Madrid
shadi.motaali@uam.es

Jornadas de REDIMadrid 2025-21 Oct

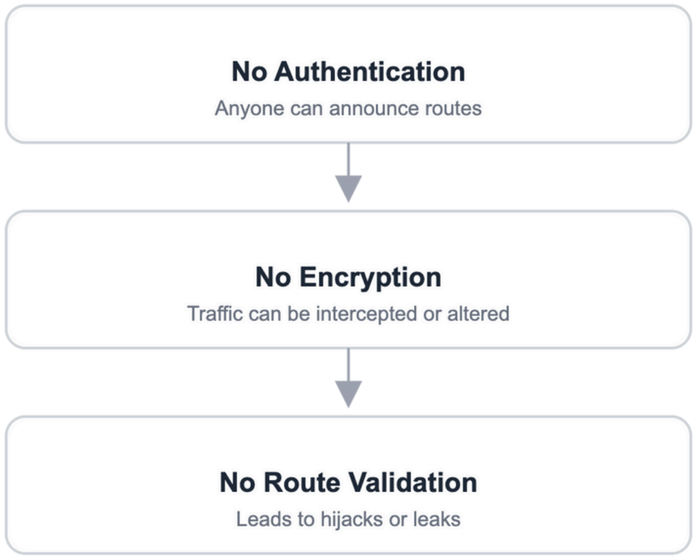
Motivation and Problem Statement

Border Gateway Protocol (BGP) is the Internet's routing foundation

- Enables autonomous systems (ASes) to exchange reachability information
- Critical for global Internet connectivity

Security vulnerabilities

- Lacks built-in security mechanisms
- Vulnerable to route hijacking, route leaks, prefix hijacking
- Attacks can cause service disruptions and data interception



Real-world impact

- 2025: Cloudflare misconfiguration
- 2022: Russian Twitter BGP Hijack
- 2008: Pakistan Telecom hijacked YouTube traffic

Key Challenges in BGP Anomaly Detection:

Highly imbalanced datasets

Data authenticity issues

Feature complexity

Limit explainability

Related Work and Limitations

Study	Approach	Limitations
Allahdadi et al. (2017)	Three-phase pipeline with One-Class SVM	Limited generalization; models trained per specific event
Park et al. (2023)	Tokenization with deep learning	SMOTE introduces artifacts; no per-class analysis
Nassir et al. (2024)	Hybrid SGD-RF model	Simulation-based only; lacks real-world validation
Romo-Chavero et al. (2025)	Hybrid MAD with ML classifiers	Overfitting risk due to resampling; dependence on thresholds

Gap

★Need for a feature selection approach that preserves data authenticity while enhancing model explainability

Methodology Overview

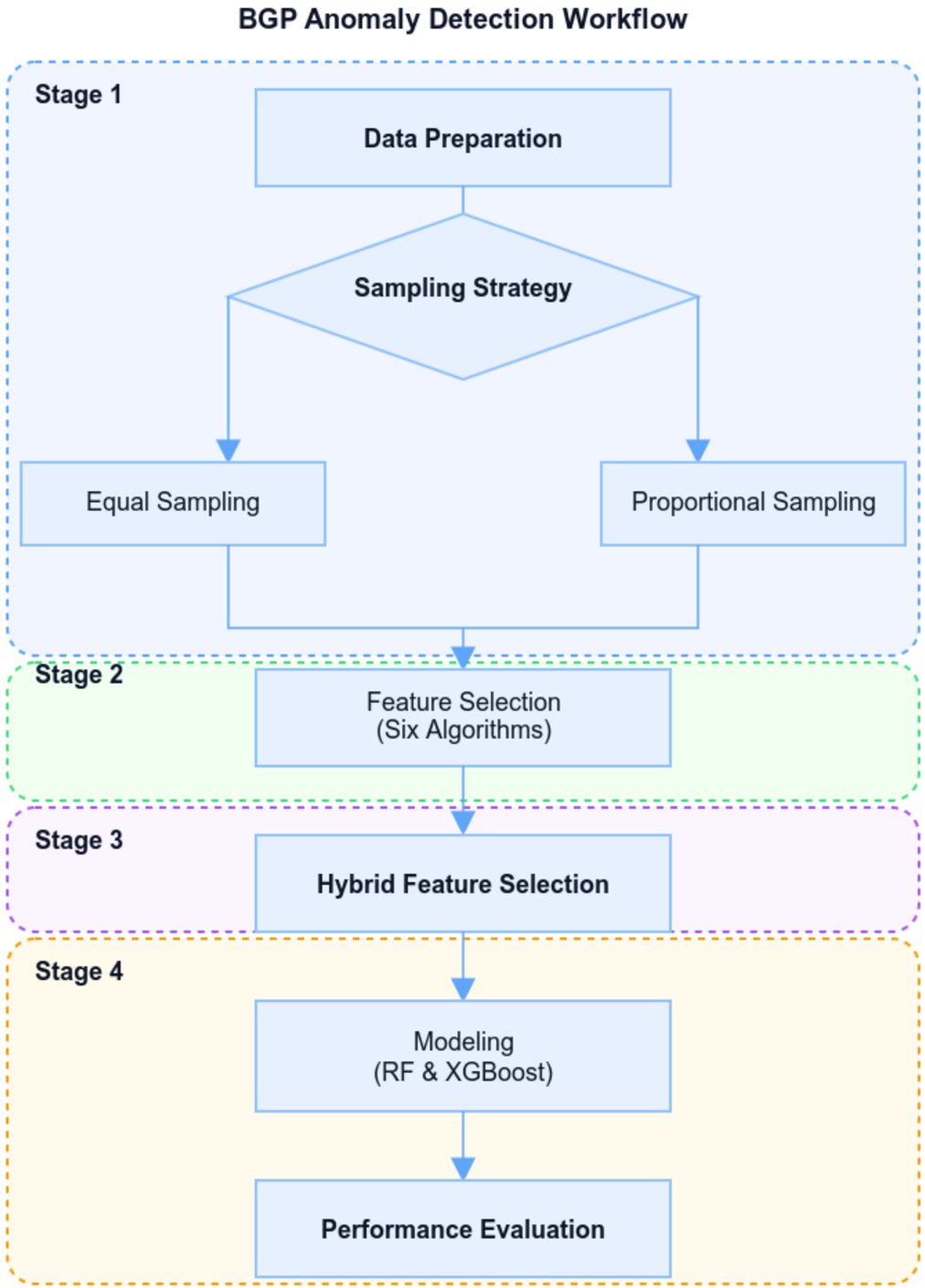
Four-stage approach

1.Dataset preparation and balancing

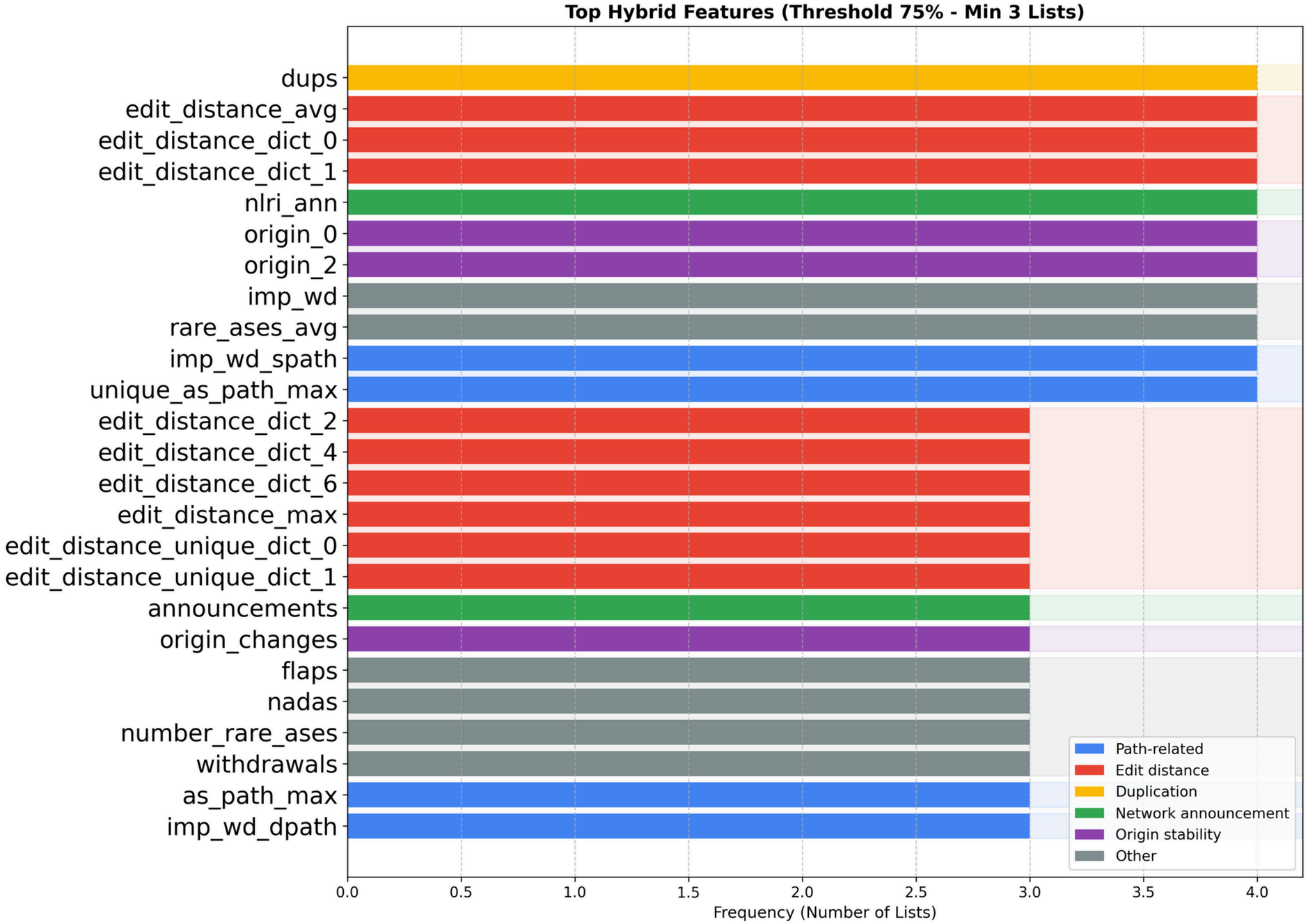
2.Feature selection using six algorithms

3.Hybrid feature ensemble with 75% agreement threshold

4.Evaluation using Random Forest and XGBoost



Selected Features Visualization



Machine Learning Models and Experimental Design

Classification Algorithms

Random Forest

- **Ensemble approach**: 100 decision trees with bagging
- **Split criterion**: Gini impurity optimization
- **Key advantage**: Native feature importance via mean decrease in impurity

XGBoost

- **Sequential approach**: Gradient-based tree construction
- **Regularization**: L1/L2 for generalization
- **Key advantage**: State-of-the-art on tabular data

Experimental Setup (Binary Classification Scenarios)

- Normal vs. Class 1 (indirect attack), Class 2 (direct attack), Class 3 (Outage), and All Anomalies

Evaluation Framework

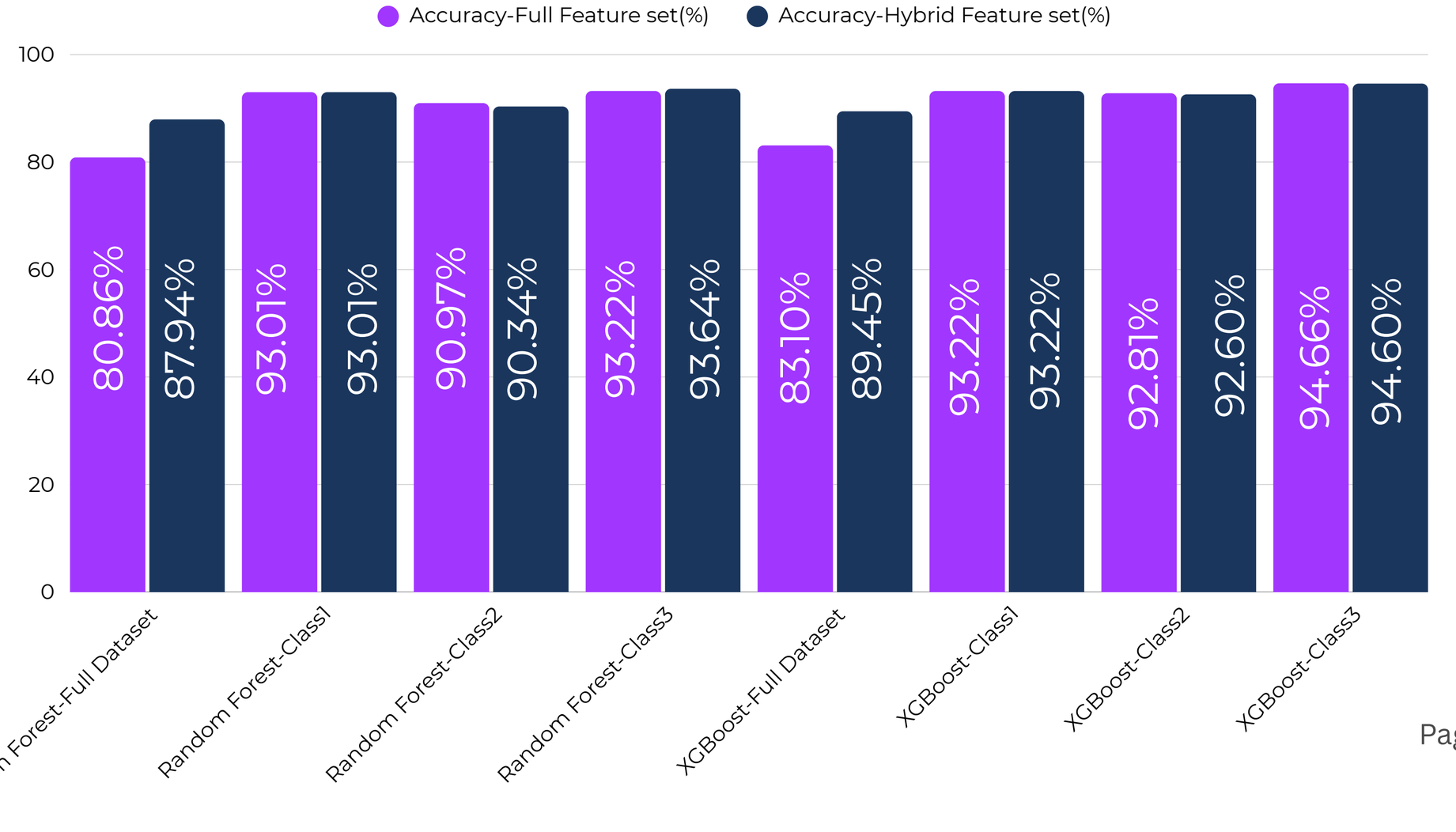
- Parameters: Default configuration to isolate feature selection effects
- Hyperparameter tuning yields 0.26-1% additional F1-score gains

Class-Specific Insights

- **Class 2 (direct)**: Benefits from deeper trees, stronger regularization
- **Class 3 (outages)**: Optimal with moderate depth, lower regularization

Quantitative Performance Analysis

Classification Performance Analysis



Model Interpretability

Feature Importance Distribution

Class	SHAP (XGBOOST)	Gini (Random Forest)	Consensus Features
Class 1	edit_distance_dict_1	edit_distance_dict_1	edit_distance_dict_1
	imp_wd_spath	flaps	dups
	flaps	dups	flaps
	origin_0	edit_distance_unique_dict_1	imp_wd_spath
	dups	imp_wd_spath	_
Class 2	nlri_ann	nlri_ann	nlri_ann
	dups	imp_wd_path	imp_wd_path
	unique_as_path_max	edit_distance_avg	_
	flaps	announcements	_
	imp_wd_path	edit_distance_dict_0	_
Class 3	dups	dups	dups
	edit_distance_dict_1	edit_distance_unique_dict_1	edit_distance_dict_1
	origin_2	edit_distance_dict_1	origin_2
	origin_0	imp_wd_spath	imp_wd_spath
	imp_wd_spath	origin_2	_

Dimensionality Analysis

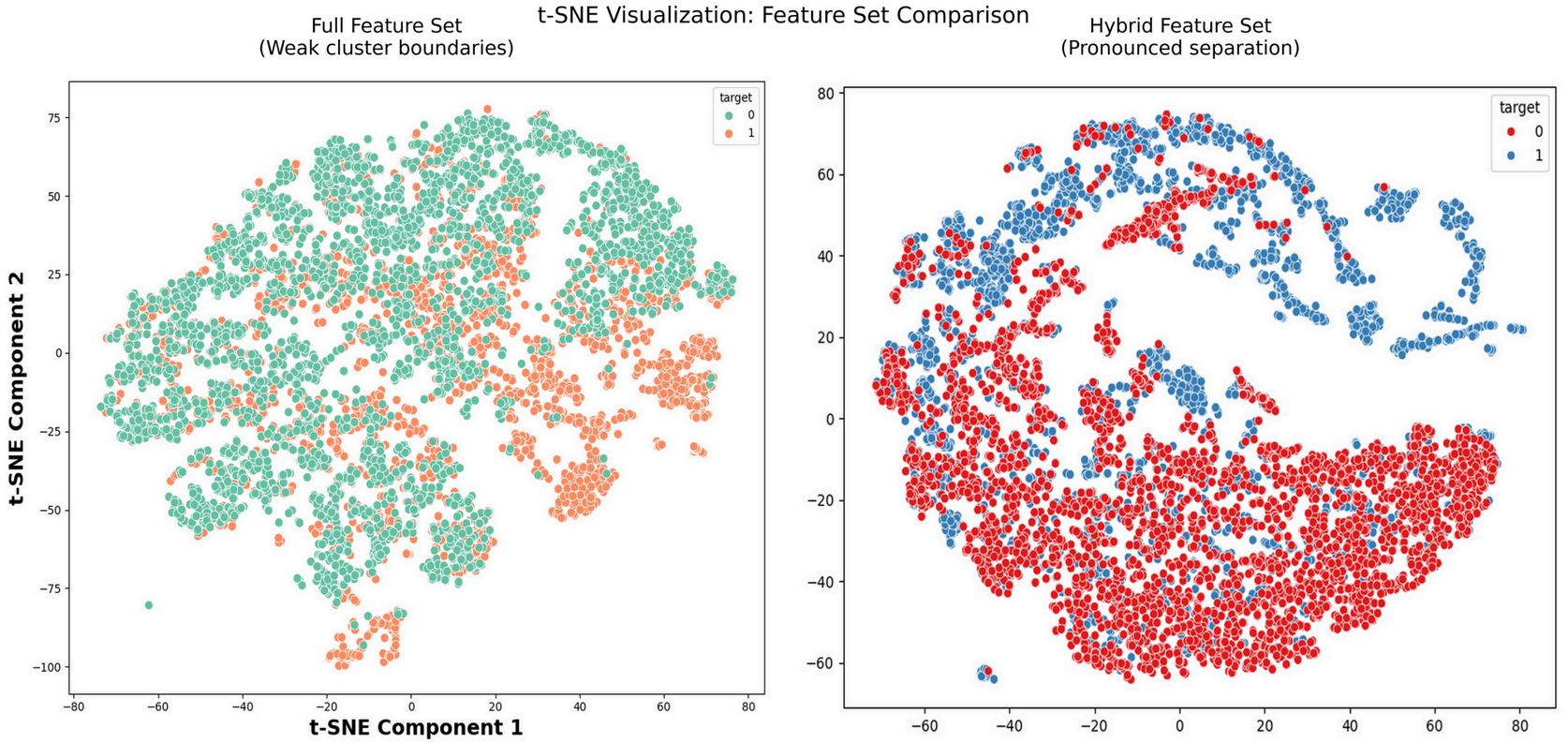
Dimensionality Reduction Analysis

- **Principal Component Analysis:**

1. 22 to 26 principal components explain 99% of variance
2. Significant dimensionality reduction without information loss

- **t-Distributed Stochastic Neighbor Embedding (t-SNE):**

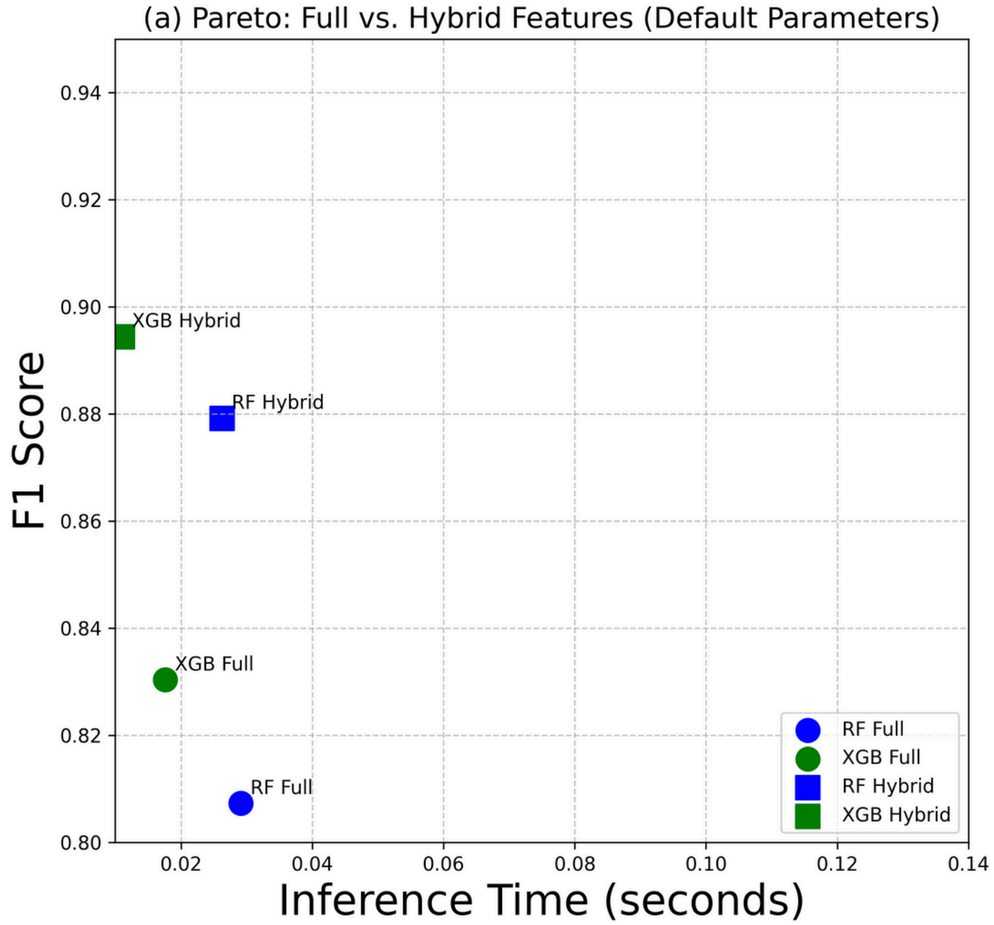
1. Enhanced class separability with hybrid features

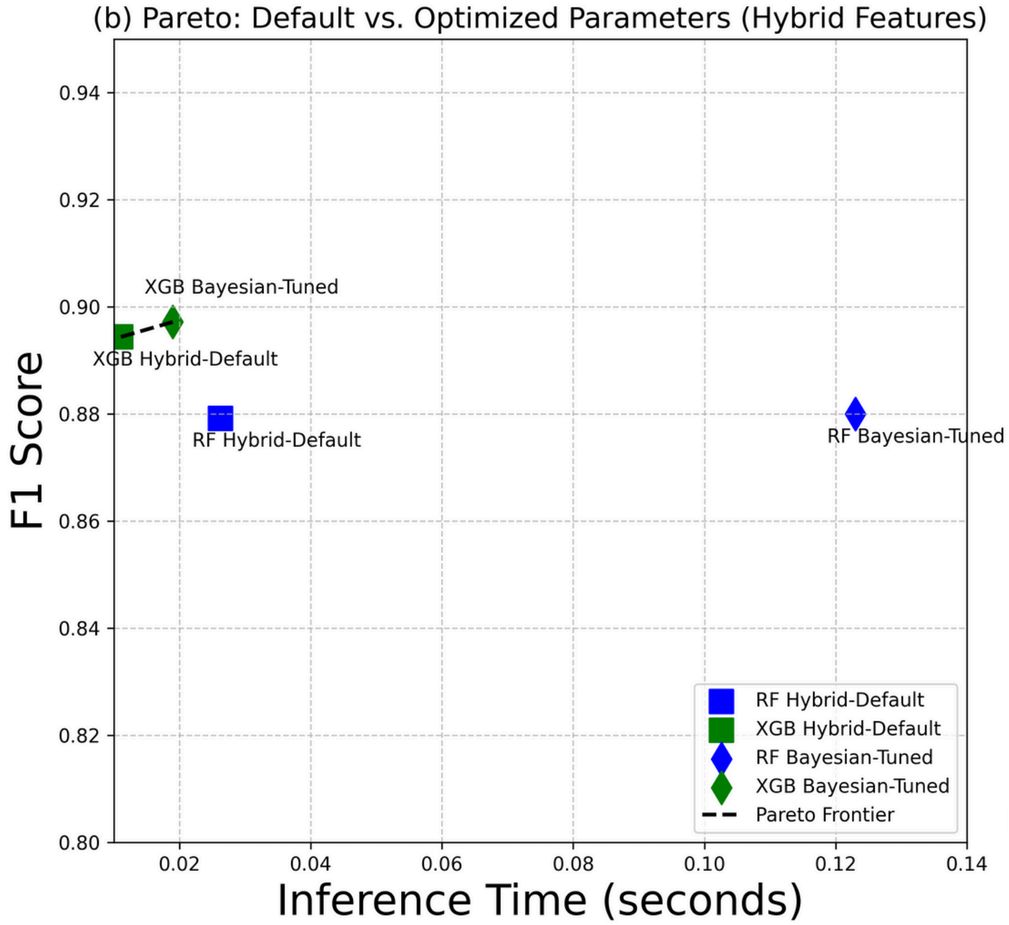


Pareto Analysis - Balancing Performance & Efficiency

Pareto Efficiency Analysis

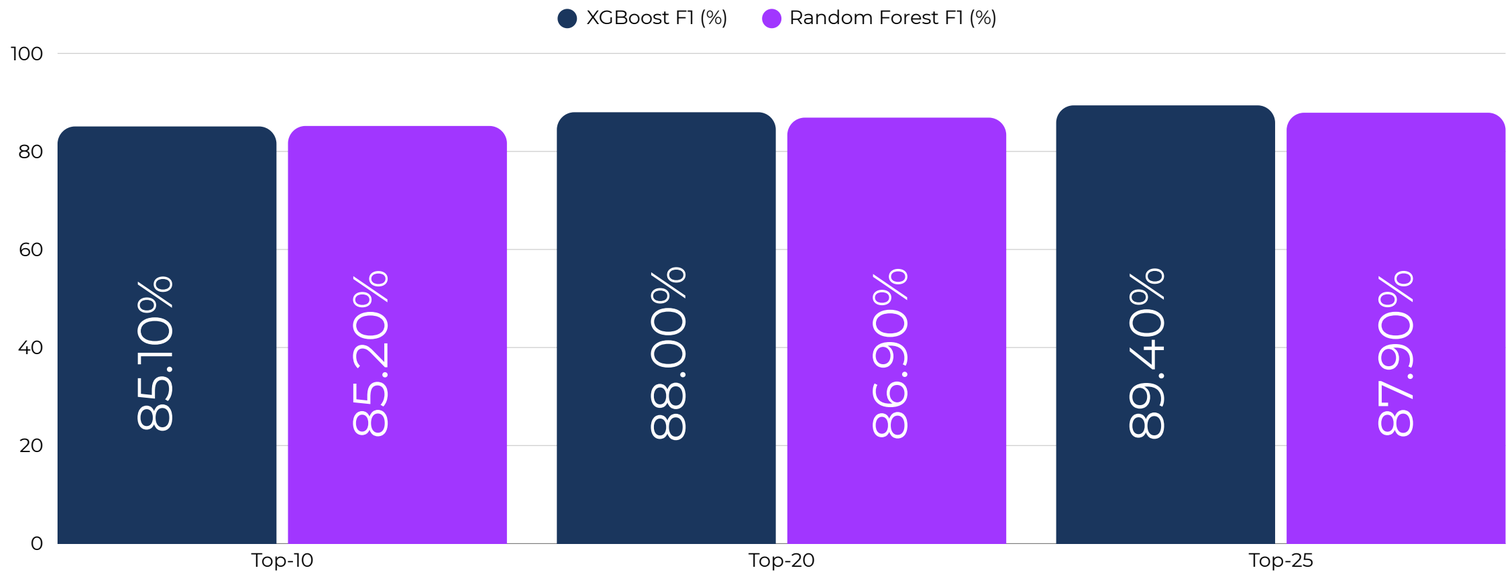
- **Feature Selection Impact(Left Graph)**: Hybrid features dominate - better accuracy AND faster!
- **Hyperparameter Optimization(Right Graph)**: Trade-off +0.3% accuracy for 1.7× inference time





Ablation Analysis and Computational Efficiency

Top-N Feature Analysis



Critical Feature Impact

Most Important Features (by removal impact):

- dups: -2.10% F1 (most critical)
- origin_2: -1.31% F1 (origin stability)
- rare_ases_avg: -0.66% F1 (despite low variance!)

Computational Efficiency Gains

48 → 25 Features (47.9% reduction):

- **XGBoost**: 36.9% faster inference (0.0176s → 0.0111s)
- **Random Forest**: 9.6% faster (0.0291s → 0.0263s)
- **Training**: 20-26% faster across all models

Conclusions and Research Contributions

01

Dimensionality Reduction

- Ensemble approach identifies 25 optimal features with 47.9% dimensionality reduction

02

Performance and Efficiency Improvements

- XGBoost: 89.7% accuracy
- Random Forest: 88.0% accuracy
- 36.9% faster inference time

03

Explainability

- SHAP/Gini consensus features

Future Research Directions

01

Methodological Extension

- Multiclass classification framework for simultaneous detection and categorization
- Implement various network scenarios using Scapy.
- Conduct the experiment using neural network–based algorithms such as LightGBM.

02

Operational Deployment

- Real-time system implementation with sliding window feature computation
- Integration with RPKI validation and automated mitigation systems

Thank you

Contact Us

shadi.motaali@uam.es

Research Group: HPCN-UAM

Funding: RAMONES-CM Project (TEC-2024/COM-504)

Comunidad de Madrid

Dirección General de Investigación e Innovación Tecnológica
CONSEJERÍA DE CIENCIA, UNIVERSIDADES E INNOVACIÓN

SCAN ME

LinkedIn