Supervised Network Intrusion Detection at the Session Level: A Machine Learning Approach with Class Imbalance Aware Evaluation

Yetunde Saka
Dr. Atakin Sahin

Aims & Objectives

This research aims to develop, evaluate and interpret a high-performance, supervised machine learning model for network intrusion detection at the session level.
To achieve this aim, the study pursues the following objectives:

- Develop a machine learning model that prevents data leakage.
- Achieve high detection performance on imbalanced data.
- Bridge the gap between performance and explainability

This research systematically addresses the following core research questions:
RQ1: How can a session-level preprocessing and evaluation pipeline be designed to prevent data leakage and ensure realistic assessment of intrusion detection models?
RQ2: Which supervised machine learning model, Random Forest or XGBoost, delivers superior performance and computational efficiency when detecting intrusions in a highly imbalanced dataset?
RQ3: What are the most discriminative features for identifying malicious network sessions at the session level?

Methods

This research adopted an iterative experimental methodology designed to uncover the strengths and weaknesses of intrusion detection models under realistic constraints. A series of experimental cycles was conducted. Early trials, which used temporal partitioning and imbalance strategies such as class weighting and SMOTE, revealed vulnerabilities to concept drift and excessive false positives. Subsequent experiments with SVM classifiers produced deceptively high single-split performance, but were prone to overfitting. Insights from these missteps guided the refinement of the pipeline as seen below:

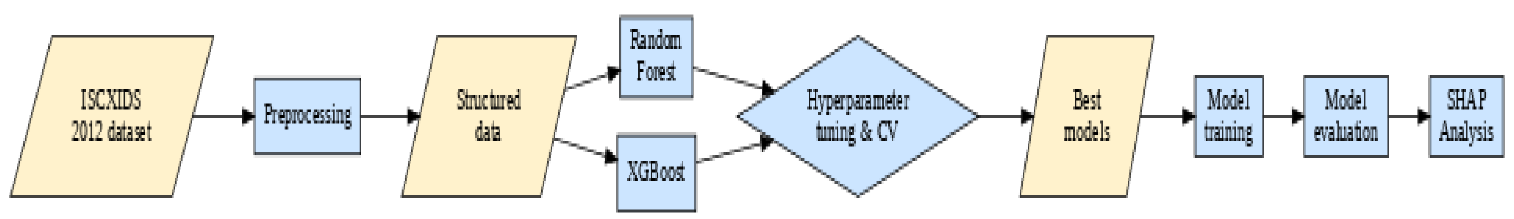

Fig 1.0: Methodological Pipeline

Results

RF Evaluation on Held-out 20%:
Training time: 1280.27 sec
Prediction time: 9.18 sec

	precision	recall	f1-score	support
0	0.9986	0.9991	0.9989	398318
1	0.9751	0.9594	0.9672	13849
accuracy			0.9978	412167
macro avg	0.9869	0.9793	0.9830	412167
weighted avg	0.9978	0.9978	0.9978	412167

ROC AUC: 0.9990
Average Precision: 0.9924

Fig 2.0: RF Performance Metrics

XGBoost Evaluation on Held-out 20%:
Training time: 19.02 sec
Prediction time: 3.01 sec

	precision	recall	f1-score	support
0	0.9986	0.9991	0.9989	398318
1	0.9742	0.9600	0.9670	13849
accuracy			0.9978	412167
macro avg	0.9864	0.9796	0.9830	412167
weighted avg	0.9978	0.9978	0.9978	412167

ROC AUC: 0.9987
Average Precision: 0.9913

Fig 3.0: XGBoost Performance Metrics

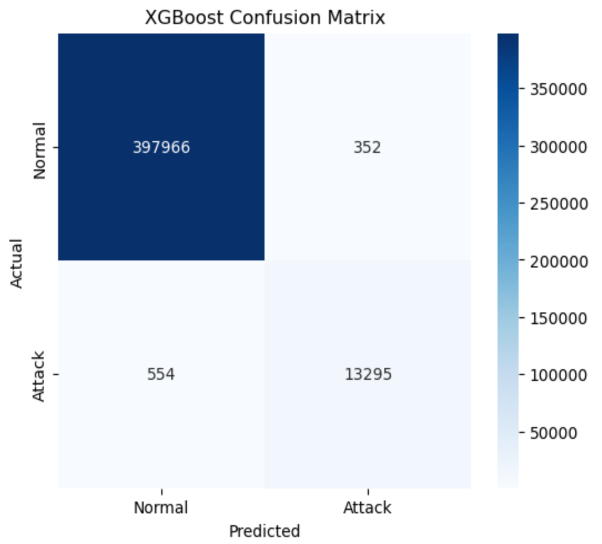

Fig 4.0: XGBoost Confusion Matrix

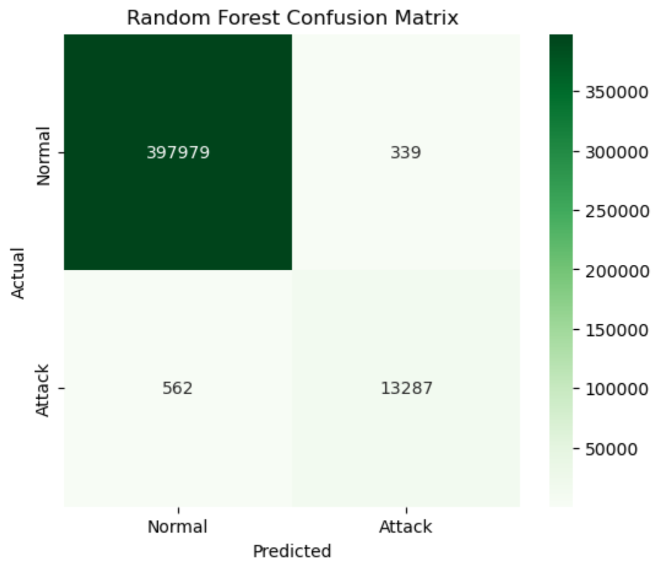

Fig 5.0: RF Confusion Matrix

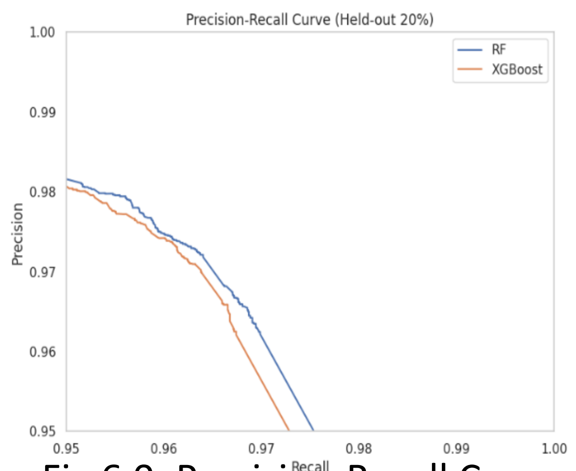

Fig 6.0: Precision-Recall Curve

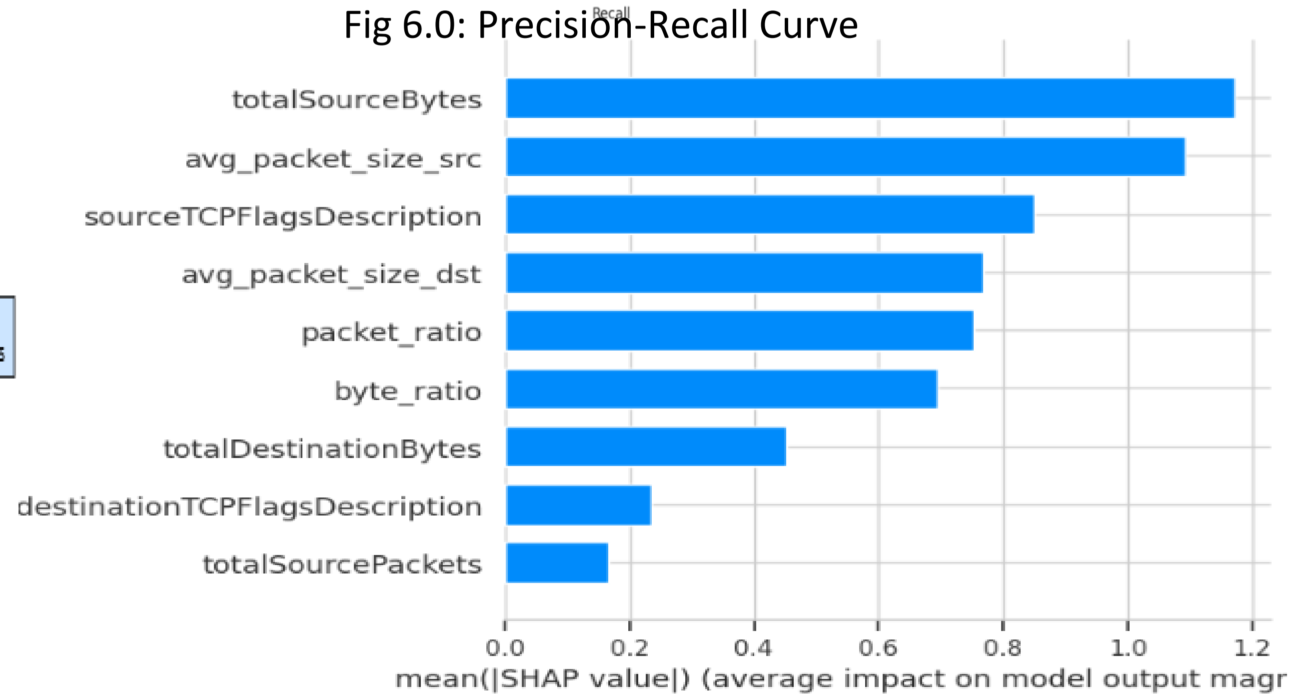

Fig 7.0: Global Importance Plot

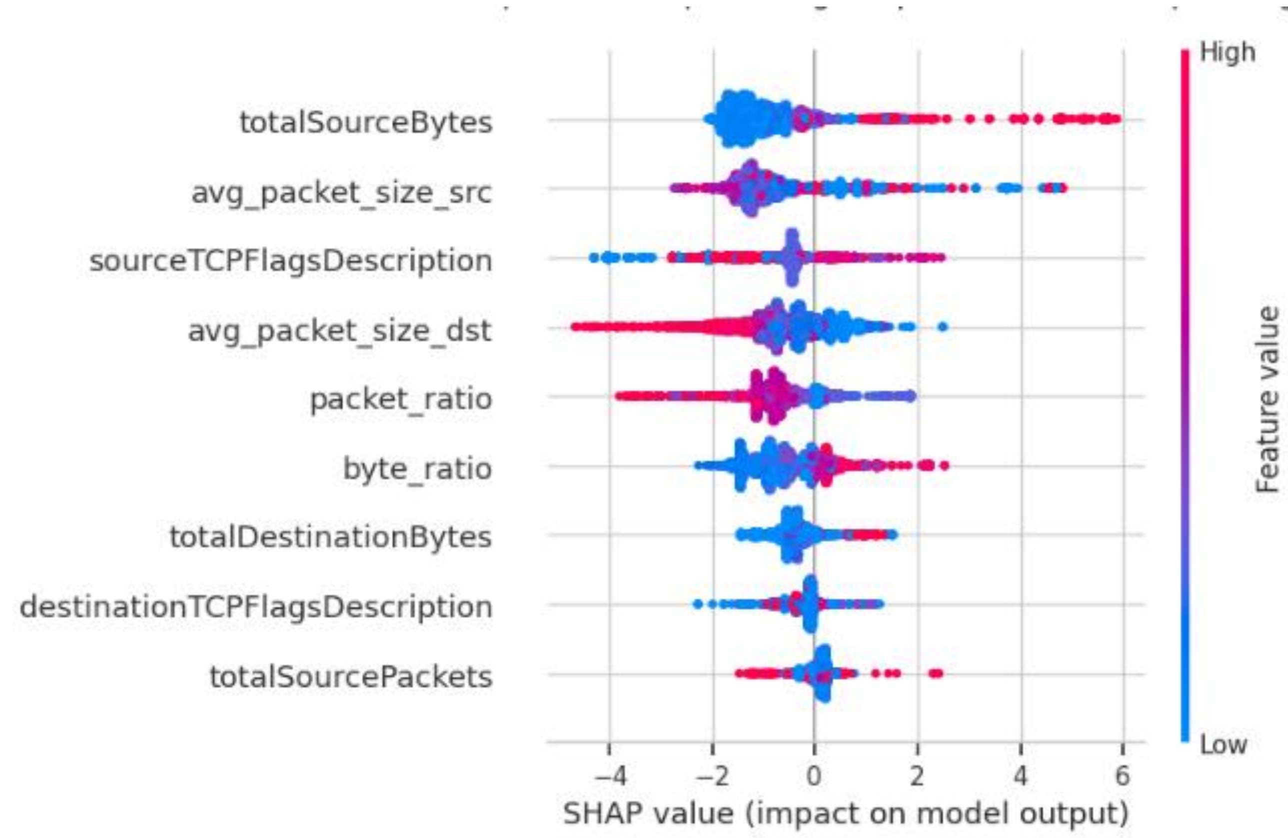

Fig 8.0: Feature Impact Direction Plot

Conclusion & Future Work

This research developed a session-level NIDS using Random Forest and XGBoost, evaluated on the ISCXIDS dataset (Shiravi et al., 2012). By enforcing session-aware evaluation, the study avoided data leakage and produced results that reflect true generalisation, addressing key methodological weaknesses in prior IDS research (Hindy et al., 2020). Both models achieved near-perfect performance, with XGBoost outperforming Random Forest in recall and computational efficiency.
Future work should validate this pipeline on newer datasets (e.g. CICIDS2017, UNSW-NB15), extend to multi-class detection, and explore adaptive learning to handle concept drift (Lu et al., 2018.

References

Shiravi, A., Shiravi, H., Tavallaee, M., & Ghorbani, A. A. (2012). Toward developing a systematic approach to generate benchmark datasets for intrusion detection. Computers & Security, 31(3), 357–374. 10.1016/j.cose.2011.12.012
H. Hindy, D. Brosset, E. Bayne, A. K. Seeam, C. Tachtatzis, R. Atkinson, & X. Bellekens. (2020). A Taxonomy of Network Threats and the Effect of Current Datasets on Intrusion Detection Systems. IEEE Access, 8, 104650–104675. 10.1109/ACCESS.2020.3000179
Lu, J., Liu, A., Dong, F., Gu, F., Gama, J. and Zhang, G., 2018. Learning under concept drift: A review. *IEEE Transactions on Knowledge and Data Engineering*, 31(12), pp.2346–2363. https://doi.org/10.1109/TKDE.2018.2876857

RGU ABERDEEN
SCHOOL OF COMPUTING, ENGINEERING & TECHNOLOGY

MSc IT with Cyber Security