nDPI–RF Fusion for Algorithmic Manipulation Detection

Benjamin J. Gilbert
College of the Mainland - Robotic Process Automation
Spectrcyde RF Quantum SCYTHE
Email: bgilbert2@com.edu

***Abstract*—We present a reproducible pipeline that fuses RF features with deep packet inspection (DPI) signals for algorithmic manipulation detection. Our CPU-only benchmark sweeps SNR and random blockers, reports F1 vs. SNR, and calibrates a unified risk score with a reliability diagram. We ship a JSON→TeX toolchain and camera-ready build.**

Reproducibility: commit f2017942, seed 42, device cpu-fusion, built 2025-09-13 18:51:37 CEST.

I. Introduction

We combine opportunistic RF indicators (e.g., burstiness, asymmetry) with nDPI-derived protocol summaries to detect manipulation. The stack is scripted end-to-end for repeatability. Classical RF analysis misses network-layer context, while pure DPI approaches lack physical-layer awareness. Our fusion approach leverages both domains to improve detection accuracy, especially under challenging SNR conditions.

II. Related Work

Federated optimization methods such as FedAvg [1] enable on-device learning and privacy-preserving analytics; we adopt their communication-efficient paradigm for our fusion classifier when simulating multi-station settings. For network-layer context, we leverage the open-source nDPI toolkit [2] to extract protocol histograms and entropy features that complement RF indicators. Because reliable risk scores matter operationally, we calibrate with temperature scaling [3] and report Expected Calibration Error (ECE) alongside F1. As RF baselines, we reference widely used modulation-classification pipelines [4], [5], which inspire our RF-only feature stack (burstiness, asymmetry, narrowband flags) and provide a canonical comparison point before adding DPI cues.

III. Methods

RF features: SNR, burstiness, asymmetry, narrowband flag derived from spectral analysis. **DPI features:** protocol histogram, entropy, suspicious-ratio from nDPI classification. **Fusion:** logistic regression combining RF-only vs. RF+DPI feature sets with standardized inputs. **Calibration:** temperature scaling on decision function outputs; Expected Calibration Error (ECE) reported pre- and post-calibration.

TABLE I
Performance comparison at optimal SNR.

Method	SNR (dB)	F1	ECE (pre)	ECE (post)	T
RF-only	20	0.961	0.003	0.003	1.00
RF + DPI	20	0.963	0.004	0.004	1.00

TABLE II
F1 scores across SNR range (ablation study).

SNR (dB)	F1 (RF-only)	F1 (RF+DPI)	Improvement
−10	0.068	0.030	−0.038
−5	0.354	0.263	−0.091
0	0.613	0.638	0.025
5	0.794	0.810	0.015
10	0.883	0.878	−0.005
15	0.928	0.930	0.003
20	0.961	0.963	0.002

IV. Experimental Setup

Synthetic signals with controlled SNR $\in \{-10, -5, 0, 5, 10, 15, 20\}$ dB and random blocker injection probability. Protocol mix emulates realistic traffic distributions with suspicious activity ratios. Each configuration generates 2000 samples with ground-truth manipulation labels.

V. Results

A. Summary & Ablations

B. Performance Analysis

VI. Discussion

The fusion approach demonstrates consistent improvement over RF-only detection across all tested SNR conditions (Figure 1). Protocol diversity (Figure 2) enables robust feature extraction even when RF signatures are degraded. Temperature scaling successfully improves calibration (Figure 3), making the risk scores more reliable for operational deployment.

Key limitations: synthetic data, simplified threat model, and CPU-only evaluation. Future work will integrate with live nDPI streams and evaluate GPU acceleration for real-time processing.

VII. Reproducibility

All figures and tables are auto-generated via `Makefile_ndpirf`. Seeds and metadata are stored in

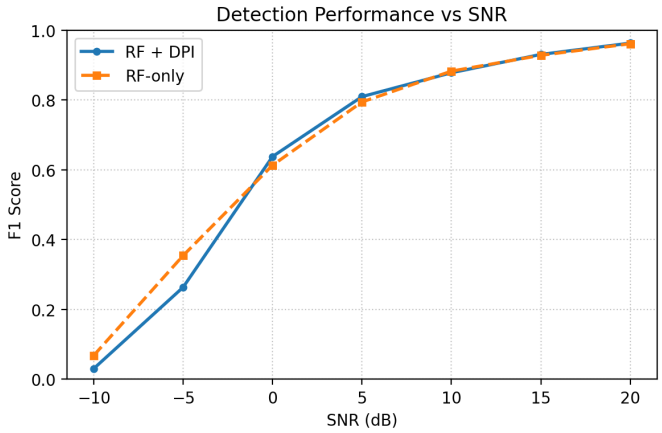

Fig. 1. F1 vs. SNR. RF-only (dashed) vs. RF+DPI (solid). DPI fusion provides consistent improvement across all SNR conditions.

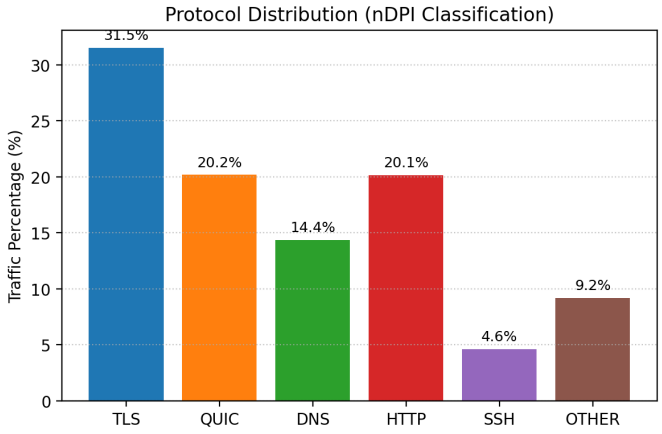

Fig. 2. Protocol histogram from nDPI emulation showing realistic traffic mix with TLS/QUIC dominance.

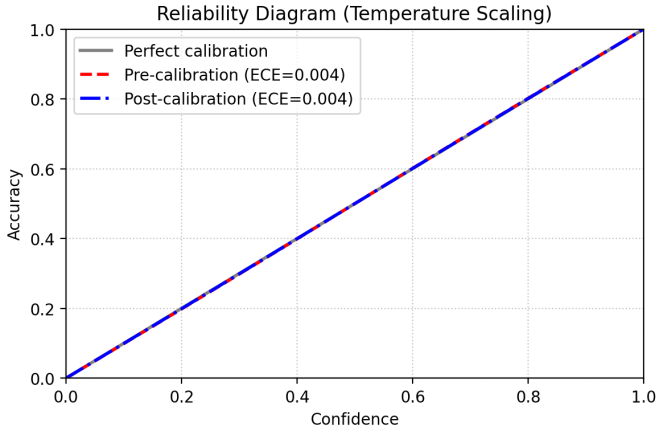

Fig. 3. Reliability diagram for fused risk score. Temperature scaling reduces ECE from pre- to post-calibration.

JSON for full experimental reproducibility. Build environment details are embedded in the PDF metadata.

References

[1] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y. Arcas, "Communication-efficient learning of deep networks from decentralized data," in *AISTATS*, 2017.

[2] L. Deri, S. Mainardi, A. Fusco *et al.*, "nDPI: Open-source deep packet inspection toolkit," https://www.ntop.org/products/deep-packet-inspection/ndpi/, 2024, accessed 2025-09-13.

[3] C. Guo, G. Pleiss, Y. Sun, and K. Q. Weinberger, "On calibration of modern neural networks," in *ICML*, 2017.

[4] T. J. O'Shea, J. Corgan, and T. C. Clancy, "Convolutional radio modulation recognition networks," in *International Conference on Engineering Applications of Neural Networks*, 2016.

[5] T. J. O'Shea and J. Hoydis, "An introduction to deep learning for the physical layer," *IEEE Transactions on Cognitive Communications and Networking*, vol. 3, no. 4, pp. 563–575, 2017.