Detection Algorithms

This supplementary section presents detection algorithm implementations for the cognitive attack detection methods defined in Part 1. These algorithms operationalize the formal definitions from Part 1, Section 5 into executable procedures.

ROC Analysis Algorithms

Algorithm 1: ROC Curve Construction

ROC Curve Construction [1] Detector D, attack samples X_{attack}, benign samples X_{benign}, threshold count n ROC curve, AUC, optimal threshold τ^* Compute scores:
$S_{\text{attack}} \leftarrow [D(x) : x \in X_{\text{attack}}]$ Compute scores:
$S_{\text{benign}} \leftarrow [D(x) : x \in X_{\text{benign}}]$ Generate thresholds:
$T \leftarrow \text{linspace}(\min(S), \max(S), n)$ each $\tau \in T$
$\text{TPR}[\tau] \leftarrow |S_{\text{attack}} > \tau|/|X_{\text{attack}}|$ $\text{FPR}[\tau] \leftarrow |S_{\text{benign}} > \tau|/|X_{\text{benign}}|$
$\text{AUC} \leftarrow \int \text{TPR}\, d(\text{FPR})$ Trapezoidal integration
$\tau^* \leftarrow_{\tau} (\text{TPR}[\tau] - \text{FPR}[\tau])$ Youden's J $(\text{ROC}, \text{AUC}, \tau^*)$

Detector Performance Results