Automatic Attack Detection in Wi-Fi Networks

Fărcășanu Tudor Andrei [1]

[1]Faculty of Mathematics and Computer Science University of Bucharest

Introduction

Wi-Fi networks are vulnerable to various cyber-attacks, necessitating robust intrusion detection systems (IDS). This study leverages deep learning techniques to detect Wi-Fi attacks using the AWID3 (Aegean Wi-Fi Intrusion Dataset) dataset.

Main Contributions:

- Development and evaluation of classical neural network and autoencoder-based approaches for Wi-Fi attack detection and classification
- Preprocessing and feature engineering of the AWID3 dataset for layer 2 OSI attack information

Experimental Setup and Dataset Preprocessing

- AWID3 dataset: designed for developing Wi-Fi intrusion detection systems
- Preprocessing steps: feature selection, null value handling, encoding & hashing
- Final dataset: 15,574,909 records (≈3% anomalies)
- Data split (stratified sampling): 80% training, 10% validation, 10% testing
- Standardization applied to maintain consistent scale across features

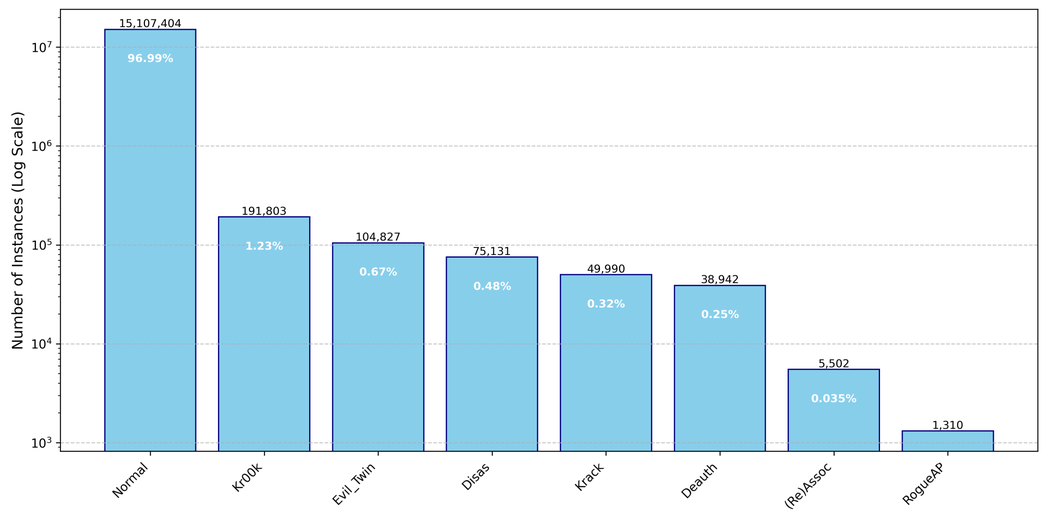
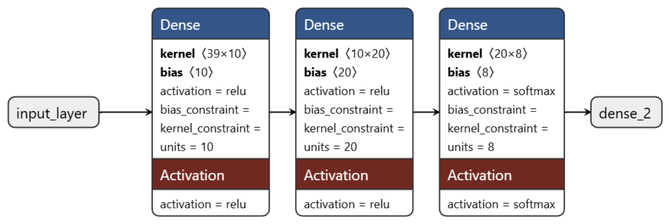


Figure 1. Distribution of attack types in the used data

Approach: Classical Neural Networks

- Simple three-layer architecture (input, hidden, output)



- Interleaved Dropout layers were initially included but later removed due to observable decrease in model performance

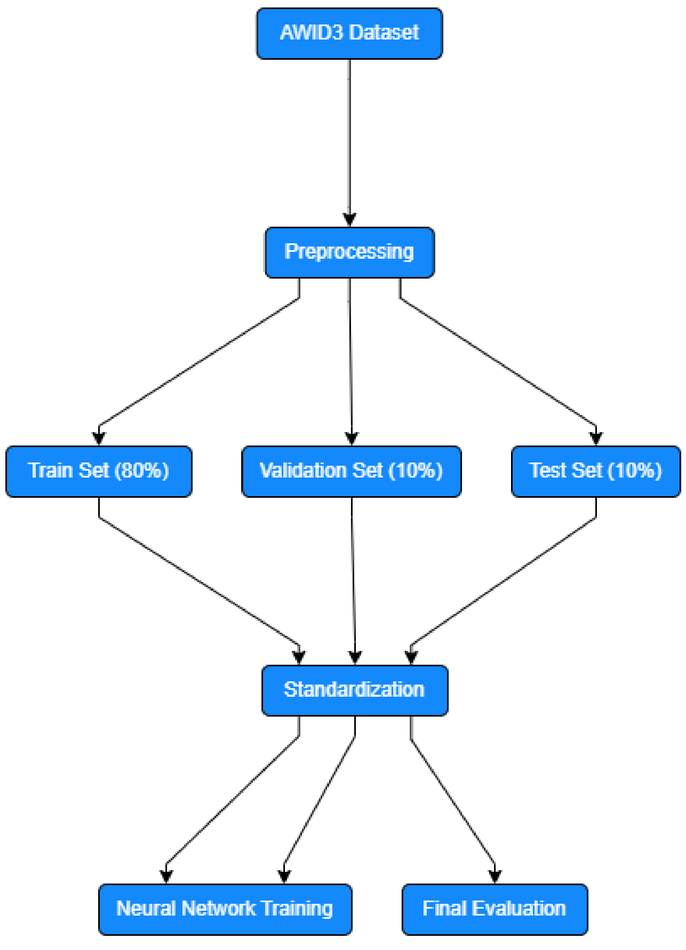
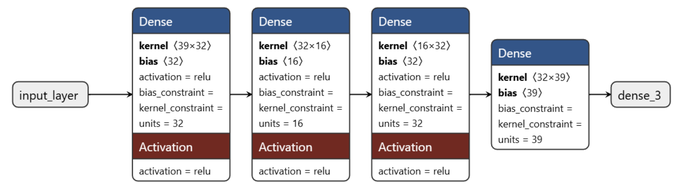


Figure 2. Neural Network training & classification flow

Approach: Autoencoders

- Separate models trained for each attack category
- Best performing architecture: five layers (2 encoding, 1 latent, 2 decoding)



Classification Strategies:

- Threshold-based: Determines optimal reconstruction error thresholds for each class using the validation set, by searching through 250 values
- Normal distribution-based: Determines reconstruction error distribution for each class's validation set, then computes probabilities for each test instance

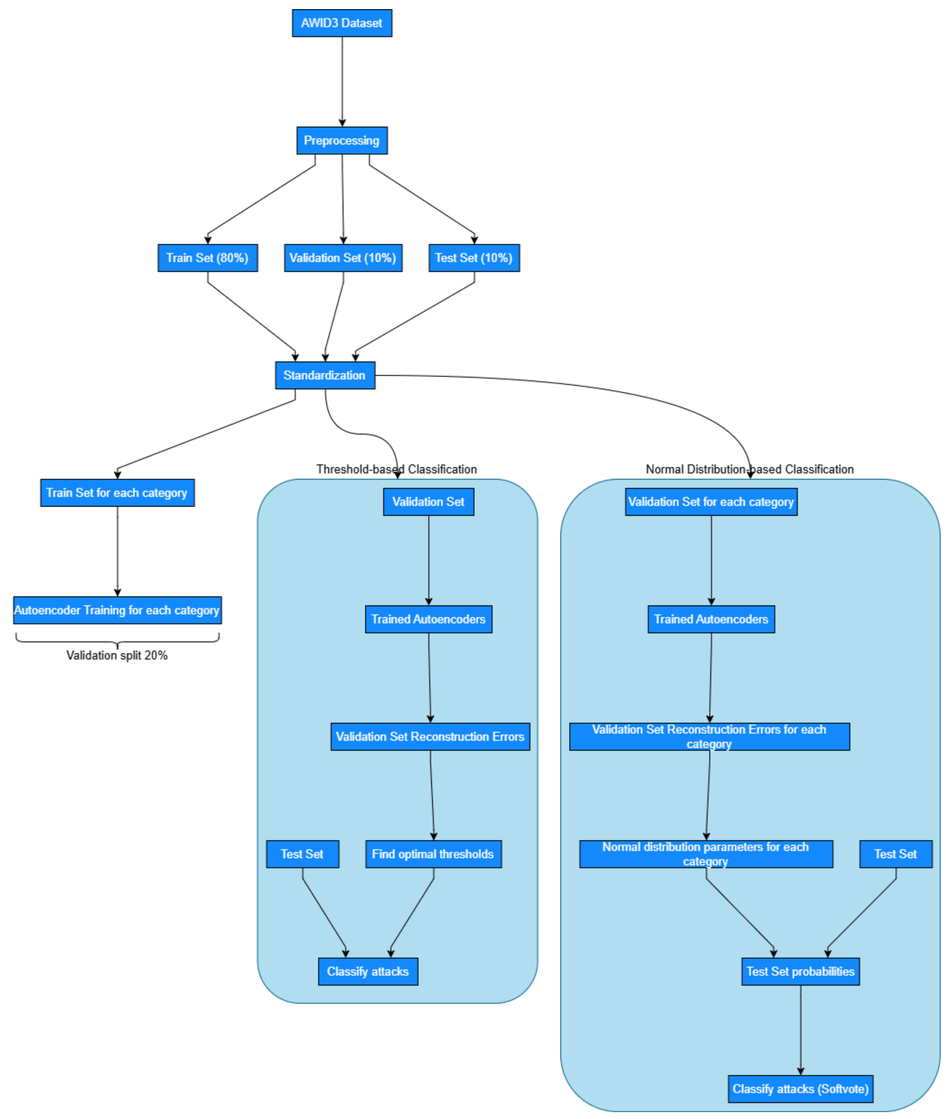


Figure 3. Autoencoder training & classification flow

Results

- Classical neural networks outperform autoencoders, especially when not using dropout, when it achieved near-perfect classification for most attack categories, with only a slight decrease in performance for the Krack attack (F1 score of 0.94).
- Threshold-based classification performs better overall than normal distribution-based classification for autoencoders, with performance differences for the Krack and (Re)Assoc attack classes.

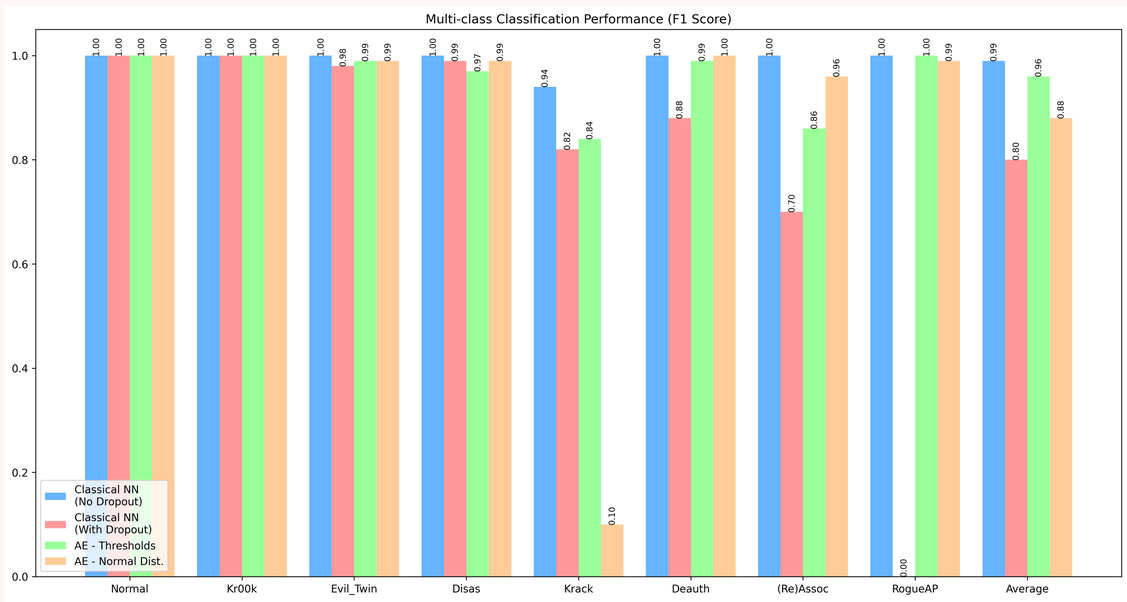


Figure 4. Multiclass classification results