SS-BRBES: A Semi-Supervised Belief Rule-Based Expert System for Explainable and Uncertainty-Aware Intrusion Detection

Amira Gourbal Abdallah, Mohammad Shahadat Hossain, Karl Andersson

Intrusion detection systems based on supervised machine learning depend on large, labeled datasets, which are difficult to obtain in real cybersecurity environments. Most existing models also operate as black boxes and do not quantify the uncertainty of their predictions, which limits their use by security analysts. This work proposes SS-BRBES, a Semi-Supervised Belief Rule-Based Expert System for network intrusion detection. The framework integrates a Belief Rule Base, optimized through Differential Evolution, with a co-training procedure that learns from a small set of labeled flows and a large set of unlabeled flows. Feature selection uses the Belief-Guided Feature Importance (BGFI), a new scheme introduced in this work that scores features by the divergence between their class-conditional belief distributions and the marginal belief distribution in Dempster-Shafer space. The selected features are grouped into four categories, namely packet size, packet variation, timing, and idle behavior, each handled by a sub-rule base of 27 rules, and aggregated through a top-level rule base consisting of 81 rules. Using the CICIDS2017 dataset, SS-BRBES achieves 90\% accuracy with an F1-macro of 85\% using only 5\% labeled data. BGFI is a fairly innovative feature selection scheme defined directly on the output of evidential reasoning. It integrates a BRBES with semi-supervised learning for intrusion detection.