Title: Securing the Unseen: A Comprehensive Exploration Review of AI-Powered Models for Zero-Day Attack Detection

Authur names: Abdullah Al Siam, Nuruzzaman Faruqui, Akm Azad, Mohammad Ali Moni

Abastact: Zero-day exploits remain challenging to detect because they often appear in unknown distributions of signatures and rules. The article entails a systematic review and cross-sectional synthesis of four fundamental model families for identifying zero-day intrusions, namely, convolutional neural networks (CNN), deep neural networks (DNN), Bayesian networks (BN), and reinforcement learning (RL). A PRISMA-style protocol is used to extract evidence, test across popular corpora, and test models in zero-day faithful regimes, time-split, and cross-dataset transfer. In addition to aggregate accuracy and F1, we also highlight operating-point reporting the true-positive rate at a fixed false-positive rate, ranking measures in the presence of class imbalance, and calibration of probability predictions as a measure of expected error probabilistic calibration, which may include syntactic measures such as time-to-alert, throughput, and memory compute footprint. Reported results suggest that DNNs demonstrate the aggregate performance on richly feature inputs (nearly 99.56% accuracy on CICDDoS2019), CNNs on tensorized flows/bytes with advantageous latency at the edge 92.17% on Bot-IOT), BN provides interpretable uncertainty with acceptable accuracy (99.74% on NSL-KDD), and RL shows promise as an adaptive detection-response when there are rewards and safe training environments (96.18% on CSE-CIC-IDS2018). We unify the heterogeneity of our datasets and suggest a coherent, leakage-wary evaluation environment to facilitate comparability and reproducibility. Language or code models of logs and transformer traffic encoders, along with lightweight backbones of edge IDS, become available as subjects of future head-to-head studies under equal protocol conditions. The review provides tactical advice on model-data fit, operating points, calibration, and latency budgets, the precursor to deployment ready, adaptive defence against unknown attacks.

Keywords: artificial intelligence Bayesian networks cyber security cyberattack deep learning | machine learning reinforcement learning zero- dayattack

https://onlinelibrary.wiley.com/doi/10.1111/exsy.70217