Cognitive Detection at Big-Data Scale: A CNN-LSTM-DQN Framework with Prioritized Experience Replay for Cross-Attack-Family Generalization and Multi-Seed Initialization Sensitivity Analysis

Big Data and Cognitive Computing • Article • *Open Access* • 2026 • DOI: 10.3390/bdcc10070239

Rushendra [a] ; Ramli, Kalamullah [a] ; Purnamasari, Prima Dewi [a] ; Gunawan, Teddy Surya [b] ; Salman, Muhammad [a]

[a] Department of Electrical Engineering, Universitas Indonesia, Jawa Barat, Depok, 16424, Indonesia

Abstract

Real-world IoT network security generates traffic at big-data scale with extreme class imbalance, temporal non-stationarity, and continuously evolving attack strategies that overwhelm static supervised classifiers. This paper presents a cognitive computing framework for network intrusion detection: a CNN–LSTM–DQN architecture with Prioritized Experience Replay (PER) evaluated on a 5,000,000-flow naturalistic sample of the TON_IoT Processed_Network dataset (4,000,000 training/1,000,000 temporally held-out test flows; 94.5% attack ratio) under a strict temporal split. The cognitive agent optimizes detection decisions using an Alerts per Million Flows (ARMF)-aware reward function that encodes both alert-fatigue cost and missed-attack penalty. We conduct a cross-attack-family generalization study: the methodology—architecture template, reward design, and hyperparameter calibration—is inherited from a framework previously validated on CSE-CIC-IDS2018, re-instantiated and retrained on the structurally different TON_IoT environment, and compared against the previously published benchmark. Initialization sensitivity is characterized across five independent random seeds using paired Wilcoxon signed-rank and t-tests. Across the five seeds, the proposed X2 model attains recall

0.833 ± 0.306 and F1 0.874 ± 0.241 (mean ± sample SD), versus the supervised X1 baseline at 0.858 ± 0.178 and 0.912 ± 0.116; the best-performing seed (42) achieves 97.52% accuracy, 98.02% attack recall, 99.46% precision, and 98.73% F1-score on 1,000,000 held-out XSS flows—an attack family entirely absent from training—with temporal stability variances of 4.63×10^{-7} (recall) and 1.38×10^{-7} (F1). The X2 advantage observed among the four stable seeds is not statistically demonstrated at n = 5 (statistical power ≈ 5.1%); the initialization-sensitivity finding itself, including one degenerate alert-suppression seed, is reported as a primary contribution. A formal, exactly additive ARMF decomposition distinguishes the detected-attack (structural) component (99.46%) from the model-induced false-positive component (0.54%), and we report a multi-seed, ARMF-aware cognitive IDS evaluation on naturalistic TON_IoT traffic under an unseen-attack-family test condition that, to the best of our knowledge, has not been reported in the surveyed RL-based NIDS literature.

Author keywords

ARMF; big data security; class imbalance at scale; CNN–LSTM; cognitive computing; cross-attack-family generalization; deep reinforcement learning; intrusion detection system; IoT network security; multi-seed sensitivity analysis; prioritized experience replay; TON_IoT

Indexed keywords

Engineering controlled terms

Benchmarking; Big data; Cognitive systems; Computer architecture; Computer crime; Deep learning; Intrusion detection; Network architecture; Network intrusion; Network security; Statistical tests

Engineering uncontrolled terms

Alert per million flow; Big data security; Class imbalance; Class imbalance at scale; CNN–LSTM; Cognitive Computing; Cross-attack-family generalization; Experience replay; Generalisation; Intrusion Detection Systems; IoT network security; Multi-seed sensitivity analyze; Networks security; Prioritized experience replay; Reinforcement learnings; Seed sensitivity; Sensitivity analyzes; TON_IoT

Engineering main heading

Sensitivity analysis

Funding details

Details about financial support for research, including funding sources and grant numbers as provided in academic publications.

Funding sponsor	Funding number	Acronym
Universitas Indonesia See opportunities by UI ↗	PKS-291/UN2.RST/HKP.05.00/2025	UI

Funding text

This publication was supported by Universitas Indonesia through Hibah Publikasi Terindeks Internasional (PUTI) Q1 Kolaborasi Internasional Scheme under Contract: PKS-291/UN2.RST/HKP.05.00/2025.

Corresponding authors

Corresponding author	K. Ramli
Affiliation	Department of Electrical Engineering, Universitas Indonesia, Jawa Barat, Depok, 16424, Indonesia
Email address	kalamullah.ramli@ui.ac.id
Corresponding author	M. Salman
Affiliation	Department of Electrical Engineering, Universitas Indonesia, Jawa Barat, Depok, 16424, Indonesia
Email address	muhammad.salman@ui.ac.id

About Scopus

Language

日本語版を表示する

查看简体中文版本

查看繁體中文版本

Просмотр версии на русском языке

Customer Service

Help

Tutorials

Contact us

ELSEVIER