Deep Learning Driven Heuristic IDS

Abhishek Panda 2K21/CO/19
Pranay Kachhap (2K21/CO/338)
Pritesh Das (2K21/CO/348)

Abstract

- Rise of complex cyber threats.
- Introduction to the DL-HIDS.
- Integration of heuristic analysis and deep learning.
- Key benefits: improved accuracy, adaptability, and real-time efficiency.

Motivation

Why DL-HIDS?

- Address limitations of traditional IDS.
- Adaptability for zero-day vulnerabilities.
- Leverage SDN's potential with deep learning models.

Problem Statement

Traditional IDS limitations:

- Failure to detect zero-day attacks.
- High false negatives.
- Need for dynamic, adaptive systems for evolving threats.
- Even though there has been research done on deep learning solutions, not much work has been done in SDN-based networks.

Literature Review

Core Topics:

- Overview of SDN and its architecture.
- Evolution of deep learning in cybersecurity.
- Challenges and innovations in intrusion detection.

Methodology

Steps:

- Data Collection: Benchmark datasets like InSDN.
- Preprocessing: Traffic analysis and feature extraction.
- Model Training: Use of LSTMs and RNNs.

Results

Model Comparisons:

- Newborn Model: Random initial predictions.
- Dumb Model: Limited training, low accuracy.
- Smart Model: Optimized training with high accuracy.
- Highlighted metrics: precision, recall, F-score.

Conclusion

- DL-HIDS effectively combines heuristics and deep learning for robust intrusion detection.
- Enhanced adaptability for real-time and large-scale networks.
- Future scope: Extending capabilities to new network architectures.

Thank You!