

Enhancing Botnet Detection in IoT Networks Using Hybrid Deep Learning and Ensemble Models

Problem Statement

In the ever-expanding domain of Internet of Things (IoT) security, botnet detection has become an increasingly critical challenge. This is largely due to the decentralized architecture and limited computational capabilities of IoT devices, which make them attractive targets for attackers and simultaneously difficult to protect.

While machine learning (ML) and deep learning (DL) techniques have shown considerable success in detecting malicious activities, most of these solutions are designed and tested in controlled environments. As a result, they often struggle to perform effectively in real-time and real-world IoT settings, where networks are dynamic, devices are resource-constrained, and threats constantly evolve.

The importance of protecting IoT ecosystems from botnet attacks cannot be overstated. These attacks not only compromise user privacy but also threaten the reliability of critical infrastructure, from smart homes to healthcare systems. Although various solutions have been proposed—ranging from CNN-based intrusion detection systems (Idrissi et al., 2021) to ensemble learning models such as AdaBoost, RUSBoost (Abu Al-Haija & Al-Dala'ien, 2022), and transfer learning approaches (Kadhim et al., 2022)—most fall short when it comes to scalability, adaptability, and lightweight deployment.

Therefore, there is a clear and pressing need for a hybrid, lightweight, and adaptive detection framework that balances high detection accuracy with real-time performance and minimal computational overhead. Closing this gap could pave the way for practical, deployable security solutions that align with the diverse and evolving nature of modern IoT environments.

Research Objectives

The overarching goal of this research is to develop an efficient and lightweight hybrid detection model that leverages both ensemble learning and deep learning to identify botnet attacks in real-time IoT environments.

The specific objectives are:

1. To review and benchmark current ML and DL-based approaches for IoT botnet detection with respect to their accuracy, scalability, and computational efficiency.
2. To design a hybrid detection framework that integrates ensemble learning with deep transfer learning for improved detection performance.
3. To optimize the model for deployment on low-resource IoT devices, enabling practical real-time use.
4. To validate the model's effectiveness using both benchmark datasets (e.g., CSE-CIC-IDS2018, N-BaIoT) and live IoT network traffic.
5. To test the model's generalizability, particularly its ability to detect emerging and previously unseen botnet attack types.

Literature Review

Recent research has demonstrated significant progress in applying machine learning (ML) and deep learning (DL) techniques for botnet detection in IoT networks. Idrissi et al. (2021) proposed a CNN-based intrusion detection system trained on the CSE-CIC-IDS2018 dataset, which achieved high detection accuracy but required substantial computational resources.

In a similar effort to enhance detection performance, Kadhim et al. (2022) implemented an ensemble deep transfer learning approach that leveraged pre-trained models such as ResNet101 and VGG16. Their method involved transforming binary network traffic data into grayscale images, which improved classification accuracy.

Building on ensemble techniques, Abu Al-Haija and Al-Dala'ien (2022) introduced ELBA-IoT, a comprehensive framework combining AdaBoost, RUSBoost, and Bagging. This model, validated on the N-BalIoT dataset, achieved an impressive 99.6% detection accuracy while maintaining relatively low computational overhead.

Meanwhile, Srinivasan and Deepalakshmi (2023) developed ECASP, an ensemble-based classifier with a focus on optimal feature selection; however, the model faces limitations in terms of scalability.

Rezaei (2021) proposed a method combining supervised, unsupervised, and regression learning, reaching 100% accuracy, but its lack of real-world testing raises questions about practical applicability.

Lastly, Khoa et al. (2022) explored a novel collaborative learning framework integrating federated learning and transfer learning, reporting a 40% improvement in detection performance over baseline models, albeit with considerable computational cost.

Despite these promising advancements, a recurring challenge across most studies is the difficulty of transitioning from controlled lab environments to real-world deployment. High resource consumption, limited adaptability to new and evolving threats, and a lack of real-time validation remain pressing concerns. These issues highlight the need for detection models that not only deliver high accuracy but are also lightweight, scalable, and adaptable to the dynamic nature of IoT ecosystems.

References

- Idrissi, I., Boukabous, M., Azizi, M., Moussaoui, O., & El Fadili, H. (2021). Toward a deep learning-based intrusion detection system for IoT against botnet attacks. *IAES International Journal of Artificial Intelligence (IJ-AI)*, 10(1), 110–120.
- Kadhim, Q. Kh., Al-Sudani, A. Q. A. S., Almani, I. A., Alghazali, T., Dabis, H. Kh., Mohammed, A. T., Talib, S. G., Mahmood, R. A., Sahi, Z. T., & Mezaal, Y. S. (2022). IOT-MDEDTL: IoT malware detection based on ensemble deep transfer learning. *Majlesi Journal of Electrical Engineering*, 16(3), 47–54.
- Abu Al-Haija, Q., & Al-Dala'ien, M. (2022). ELBA-IoT: An ensemble learning model for botnet attack detection in IoT networks. *Journal of Sensor and Actuator Networks*, 11(1), 18.
- Srinivasan, S., & Deepalakshmi, P. (2023). Enhancing the security in cyber-world by detecting the botnets using ensemble classification-based machine learning. *Measurement: Sensors*, 25, 100624.
- Khoa, T. V., Hoang, D. T., Trung, N. L., Nguyen, C. T., Quynh, T. T. T., Nguyen, D. N., Ha, N. V., & Dutkiewicz, E. (2022). Deep transfer learning: A novel collaborative learning model for cyberattack detection systems in IoT networks. *IEEE Internet of Things Journal*. Advance online publication.
- Rezaei, A. (2021). Using ensemble learning technique for detecting botnet on IoT. *SN Computer Science*, 2(3), 148.