

Subject : Assiment2 .

Name: ABDULKAREM AMER ASIRI

Student ID:261002036

Section: Artificial intelligent

Research Title: Robust and Efficient IoT Botnet Detection using Deep Learning and Ensemble Methods

1. Problem Statement

The rapid expansion of the Internet of Things (IoT) has introduced significant security vulnerabilities, primarily due to the proliferation of botnet attacks. While traditional Signature-based Intrusion Detection Systems (IDS) were once effective, they are now inadequate for handling the heterogeneity and complexity of modern IoT environments. The core challenge lies in achieving a balance between detection accuracy, computational efficiency, and robustness against adversarial manipulation.

Current research has shown impressive results in controlled environments, with some models claiming up to 100% accuracy. However, these results are often "idealistic" and may not be reproducible in high-noise, real-world networks. Furthermore, there is a significant conflict regarding feature selection; some advocate for extreme reduction to improve speed, while others argue that multi-source features are essential for maintaining accuracy. Additionally, most existing systems focus solely on detection, leaving the AI models themselves vulnerable to adversarial attacks. This gap in research—balancing resource-constrained deployment with high-level security—justifies the need for a more comprehensive and robust framework.

2. Research Objectives

The primary goal of this research is to develop a robust and lightweight detection framework for IoT botnets that maintains high accuracy while resisting adversarial attacks. The specific objectives are:

To analyze the impact of multi-source feature extraction (system calls and network data) on the accuracy of collaborative machine learning models.

To design a lightweight Deep Neural Network (DNN) architecture optimized for resource-constrained IoT devices without compromising detection rates.

To implement an ensemble learning mechanism that combines diverse algorithms to minimize the bias inherent in imbalanced IoT datasets.

To evaluate the effectiveness of adversarial retraining and MGAN integration in protecting the IDS against perturbed data samples.

To validate the proposed framework using the Bot-IoT dataset to ensure performance consistency across both binary and multi-class classification scenarios.

3. Literature Review

The following synthesis summarizes the current state of research in IoT botnet detection:

Collaborative and Deep Learning Approaches: Recent studies emphasize dynamic feature capture. Nguyen et al. (2022) achieved 99.37% accuracy using a collaborative approach with "V-Sandbox". Similarly, Idrissi et al. (2021) demonstrated that CNNs outperform RNNs and LSTMs with a prediction time under 0.34 ms.

Efficiency vs. Accuracy: A critical tension exists between model complexity and speed. Rezaei (2021) utilized ensemble learning to reduce features from 204 to 20, reaching 100% lab accuracy. Conversely, Jithu P et al. (2021) focused on a lightweight DNN for DDoS detection, prioritizing deployment readiness for limited-resource devices.

Data Imbalance and Security: Addressing data bias is vital for real-world application. Popoola et al. (2021) employed SMOTE with DRNN to handle class imbalance, reaching 99.50% precision. Finally, Wang et al. (2021) highlighted the necessity of defending the IDS itself, proposing Def-IDS to counter adversarial attacks with 97.9% accuracy

References

- Idrissi, I., Azizi, M., & Moussaoui, O. (2021). BotIDS: Deep learning-based intrusion detection system for IoT botnets. *Journal of Reliable Intelligent Environments*, 7, 241–254. doi.org
- Jithu, P., Jayasubha, J., & Senthil Kumar, T. (2021). A lightweight deep neural network for botnet detection in IoT networks. *Journal of Physics: Conference Series*, 1911(1), 012015. doi.org
- Nguyen, H. T., Ngo, Q. D., & Le, V. H. (2022). A novel collaborative learning approach for IoT botnet detection. *Journal of Information Security and Applications*, 64, 103058. doi.org
- Popoola, S. I., Adebisi, B., Hammoudeh, M., Gui, G., & Gacanin, H. (2021). Hybrid deep learning for botnet attack detection in the internet of things networks. *IEEE Internet of Things Journal*, 8(12), 10227-10244. doi.org
- Rezaei, M. (2021). An ensemble-based intrusion detection system for IoT botnet detection using feature reduction. *Soft Computing*, 25, 14457–14470. doi.org
- Wang, L., Pan, Y., & Liu, J. (2021). Def-IDS: An ensemble defense mechanism against adversarial attacks in IoT intrusion detection systems. *IEEE Access*, 9, 112456-112469. doi.org