



Subject : Learning and Ensemble Methods for IoT Botnet Detection

Name: ABDULKAREM AMER ASIRI
Student ID: 261002036
Section: Artificial intelligent

Literature Review: IoT Botnet Detection and Security

.1 Summary of Research Papers

- **Paper 1**

(**Nguyen et al., 2022**) :Proposes a collaborative machine learning approach using "V-Sandbox" to capture dynamic features (Syscalls, Network, Resources). It achieved **%99.37** accuracy with a fast detection time of **6 seconds** once data is gathered.

- **Paper 2**

(**Idrissi et al., 2021**) :Introduces "BotIDS" based on **CNN** ,comparing it with RNN, LSTM, and GRU using the Bot-IoT dataset. CNN outperformed others with **%99.94** accuracy and a prediction time under **0.34 ms**.

- **Paper 3**

(**Rezaei, 2021**) :Employs an **Ensemble Learning** ANN & DT) to minimize features from 204 to **.20** It claims an exceptional **%100** accuracy in a lab environment within 11.39 seconds.

- **Paper 4**

(**Popoola et al., 2021**) :Addresses the "Class Imbalance" problem using **SMOTE** with **DRNN** .It achieved **%99.50** precision in an 11-class classification scenario, significantly reducing bias toward majority classes.

- **Paper 5**

(**Jithu P et al., 2021**) :Designed a **Lightweight DNN** for DDoS Botnet detection. It balances data manually (7:1 ratio) and achieves **%94** accuracy, prioritizing deployment readiness for resource-constrained IoT devices.

- **Paper 6**

(**Wang et al., 2021**) :Proposes **Def-IDS** ,an ensemble defense against **Adversarial Attacks** .It integrates MGAN and Adversarial Retraining to protect the IDS itself, reaching **%97.9** accuracy against perturbed samples.

.2Critical Analysis

The reviewed studies demonstrate a strong trend toward using **Deep Learning (DL)** and **Ensemble Methods** to mitigate IoT security threats. A major strength across these papers is the adoption of the **Bot-IoT dataset** ,which provides a realistic benchmark for modern attacks. However, a recurring weakness is the "idealism" of laboratory results; for instance, the 100% accuracy reported in Paper 3 may not be reproducible in high-noise, real-world networks. Furthermore, while Papers 1-5 focus on detection accuracy, Paper 6 highlights a critical vulnerability often ignored: the susceptibility of the AI models themselves to adversarial manipulation.

.3Connections & Conflicts

- **Connections** :All papers agree that traditional, signature-based IDS cannot handle the heterogeneity of IoT. There is a clear consensus on using **Machine Learning** to achieve "Real-time" or "Early" detection (Papers 1, 2, and 5).
- **Conflicts** :There is a significant conflict regarding **feature selection** ;Paper 3 advocates for extreme feature reduction (down to 20), whereas Paper 1 argues that multi-source features (System calls + Network) are essential for accuracy. Additionally, Paper 5 uses **Binary Classification** ,while others (2, 4, 6) insist on **Multi-class Classification** for a more granular incident response.

.4Synthesis Matrix for Literature Review

Limitations	Key Findings/Results	Methodology	Year	Study
High total processing time per sample.	99.37% Accuracy, 6s detection.	Collaborative ML (KNN, RF)	2022	Nguyen et al.
Unbalanced data affects rare attacks.	99.94% Acc, <0.34ms prediction.	CNN vs. (RNN, LSTM, GRU)	2021	Idrissi et al.
Tested only in controlled lab settings.	100% Accuracy, 20 features.	Ensemble (ANN & DT)	2021	Rezaei
Increased training time due to SMOTE.	99.50% Precision, 99.75% Recall.	SMOTE + DRNN	2021	Popoola et al.
Limited to Binary classification.	94% Accuracy, 0.98 AUC.	Lightweight DNN	2021	Jithu P et al.

High computational cost for retraining.	97.9% Acc against Adv-Attacks.	Def-IDS (MGAN + MAT)	2021	Wang et al.
---	--------------------------------	----------------------	------	--------------------

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

