Insights into Boosting Algorithms for DDoS Attacks in the Military Internet of Things

Love Allen Chijioke Ahakonye †, Cosmas Ifeanyi Nwakanma †, Dong-Seong Kim
IT Convergence Engineering, † ICT Convergence Research Center,
Kumoh National Institute of Technology Gumi, South Korea
loveahakonye, cosmas.ifeanyi, dskim@kumoh.ac.kr

***Abstract*—The Joint All-Domain Command and Control (JADC2) initiative prioritizes proactive decision-making through operational terrain analysis. It integrates a vast military Internet of Things (IoT) network with Artificial Intelligence (AI) to enhance efficiency. However, this integration raises security concerns, particularly regarding distributed denial of service (DDoS) attacks. This study presents a time-efficient framework using HistGradient Boosting to detect DDoS attacks effectively. The results show that it outperforms traditional ensemble boosting methods in accuracy, sensitivity, specificity, minimal error loss, and execution time, highlighting its importance in resource-efficient IoT networks.**

***Index Terms*—AI, Ensemble learning, DDoS, Military IoT**

I. Introduction

The Congressional Research Service highlights the urgency of rapid decision-making in conflicts, emphasizing the need for analyzing operational terrain and disseminating expedient directives, as discussed in the Joint All-Domain Command and Control (JADC2) initiative [1]. To expedite and automate this process, the Department of Defense (DoD) leverages a vast military Internet of Things (MIoT) network combined with artificial intelligence [2], [3]. The JADC2 concept aims to integrate data streams from numerous battlefield vehicles, sensors, and intelligent devices across military branches [3] in Fig. 1.

Integrating data from battlefield devices and sensors poses security risks due to increased attack entry points [3]. Ensuring seamless data sharing across platforms requires rapid access for informed decisions within threat timelines [3]. Distributed denial of service (DDoS) attacks threaten JADC2 by overwhelming communication channels, potentially disrupting sensor data and decision systems, causing communication breakdowns between critical components, and hindering real-time decision-making and mission success [3]. Robust ML-based network intrusion detection architectures must withstand DDoS attacks to ensure operational continuity [4], [5], necessitating an ensemble approach.

Ensemble learning methods have enabled attack detection in large heterogeneous IoT networks by incorporating multiple ML algorithms to achieve higher performance and efficiency [6]. According to [3], leveraging a vast MIoT on the battlefield offers advantages such as autonomous surveillance, targeted situational awareness, and troop health monitoring. However, addressing substantial communication and data security challenges by detecting and mitigating DDoS attacks is crucial. Hence, this study implements a memory-efficient ensemble framework for significantly detecting diverse DDoS attack instances.

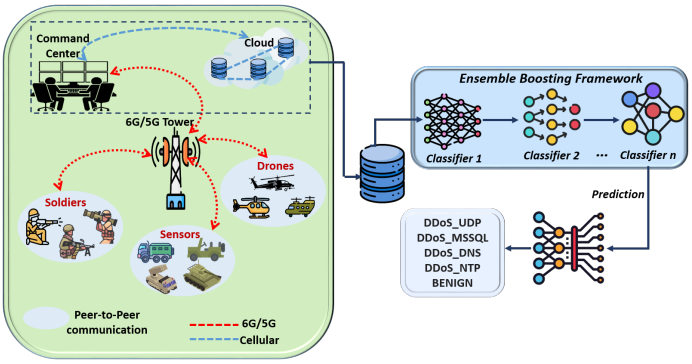

Fig. 1. Framework of the Ensemble Boosting Algorithm for DDoS attack detection.

II. System Methodology

Parallel ensemble techniques, like bagging, use a combiner to aggregate the predictions of separately trained base classifiers. This approach fosters ensemble diversity and reduces variance and overfitting by averaging model predictions, making it suitable for noisy data but less effective with outliers. In contrast, sequential ensemble methods, like boosting, iteratively correct past errors during model training, effectively handling noisy data and outliers [6]. It makes boosting superior to bagging in large, diverse MIoT environments with sparse attack instances. This study proffers insights into the statistical performance of boosting algorithms fostering efficiency and low memory.

Sequentially adding and weighing the base learners derives the sturdy classifier, assigning weights at each occurrence in the training set. Consider n training occurrences $A = (\varphi_1, \varsigma_1)$,..., (φ_i, ς_i),...,(φ_n, ς_n), where ς_i is the target output of instance φ_i, and $\varsigma_i \in \mu = (-1, +1)$, where the weight D_1 of instance φ_i and update D_{t+1} are given in equation 1.

$$D_1(i) = \frac{1}{\rho}, \quad i = 1, 2, \ldots, n$$
$$D_{t+1}(i) = \frac{D_t(i)}{\theta_t} e^{(-\delta_t \varsigma_i \psi_t(\varphi_i))}, \quad i = 1, 2, \ldots, \qquad (1)$$

where $\psi_t(\varphi)$ denotes the base classifier, t = 1,.., Ω represents the iterations, θ is the standardization element, and δ_t indicates the weight of classifier $\psi_t(\varphi)$. ρ_t computes the importance of $\psi_t(\varphi)$ during prediction. False classifications in $\psi_t(\varphi)$ are allotted huge weights in $t+1$ training round. Moreover, D_{t+1} is issued by determining θ_t and δ_t is given by equation 2.

$$\begin{aligned}\theta_t &= \sum_{t+1}^{m} D_t(i) e^{(-\delta_t \varsigma_i \psi_t(\varphi_i))} \\ \delta_t &= \frac{1}{2} In\left(\frac{1-\eta_t}{\eta_t}\right),\end{aligned} \tag{2}$$

for η calculating the classifier error rate as in equation 3.

$$\eta_t = Pr[\omega_t(\varphi_i) \neq \varsigma_i] = \sum_{i=m}^{m} D_i(i)\chi[\omega_t(\varphi_i) \neq \varsigma_i]. \tag{3}$$

Consequent upon the completion of the specified number of instances, a final resilient classifier is derived using equation 4

$$\vartheta(\varphi) = sign\left(\sum_{t=1}^{T} \delta_t \psi_t(\varphi)\right). \tag{4}$$

Parameter tuning and optimization capture intricate data patterns, preventing overfitting. It also balances bias and variance and enhances generalization, yielding more accurate and robust models.

III. Performance Evaluation

This study leveraged the well-established CICDDoS2019 dataset [4] in cybersecurity research, consisting of diverse DDoS attacks based on network flow features. Conventional Boosting algorithms like Extreme Gradient (XGB), Adaptive (AdaBoost), Gradient (GB), and HistGradient Boosting algorithms evaluated the CICDDoS dataset to generate insight into its performance. Table I and Fig. 2 highlight the tradeoff in error loss and execution time of the HistGradient approach. The significant performance of the HistGradient is built on its forward stage-wise method, optimizing arbitrary differentiable loss functions, and enables low memory usage and time efficiency. It is vital for timely and accurate decision-making in the vast heterogeneous MIoT network, with extensive sensor data due to the execution speed and support for missing values.

TABLE I
Error Loss and Execution Time Tradeoff of the Evaluated Algorithms

Name	Loss (#)	Time (s)
XGBoost	0.0295	22.28
GB	**0.0077**	490.50
AdaBoost	0.1698	13.19
HistGradient	0.0993	**10.47**

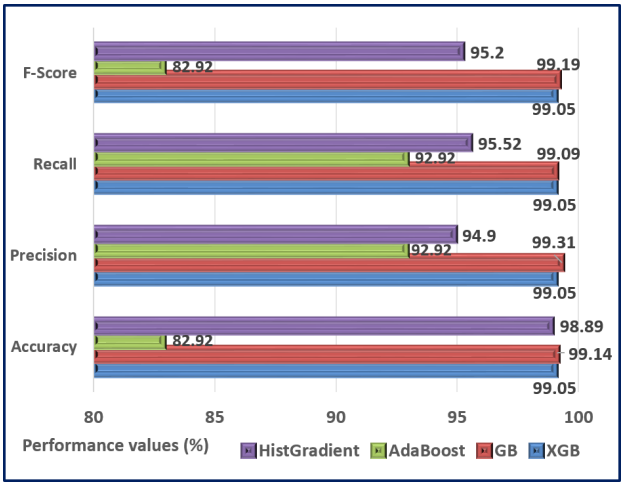

Fig. 2. Framework of the Ensemble Boosting Algorithm for DDoS attack detection.

IV. Conclusion

This study explores boosting algorithms and their optimization to counter DDoS attacks within military IoT networks. It offers valuable insights into this specialized application of ensemble learning techniques in cybersecurity. The findings demonstrate the significance of HistGradient Boosting for efficient and low-resource DDoS detection with a combined advantage of detection accuracy, sensitivity, specificity, minimal error loss and execution time cost. A future direction is evaluating and comparing other ensemble learning techniques for timely intervention in critical scenarios.

Acknowledgment

This research was supported by the Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003) (50%) and by MSIT under the Innovative Human Resource Development for Local Intellectualization support program (IITP-2024-2020-0-01612) (50%) supervised by the IITP.

References

[1] M. G. Molinari, "5G & Edge Computing: The Future of the DoD and JADC2," in *Meeting The Immediate Needs of the Warfighter*. Air Land Sea Space Application (ALSSA) Center, July 1, 2023. [Online]. Available: https://shorturl.at/mBP46

[2] B. Alkanjr and T. Alshammari, "IoBT Intrusion Detection System using Machine Learning," in *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 2023, pp. 0886–0892.

[3] A. Fish, "IoT, AI, and the Future Battlefield," in *Military Embedded Systems*. Omnetics Connector Corporation, September 12, 2022. [Online]. Available: https://shorturl.at/sFPR2

[4] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy," in *2019 International Carnahan Conference on Security Technology (ICCST)*, 2019, pp. 1–8.

[5] L. A. C. Ahakonye, G. C. Amaizu, C. I. Nwakanma, J. M. Lee, and D.-S. Kim, "Classification and Characterization of Encoded Traffic in SCADA Network using Hybrid Deep Learning Scheme," *Journal of Communications and Networks*, vol. 26, no. 1, pp. 65–79, 2024.

[6] I. D. Mienye and Y. Sun, "A Survey of Ensemble Learning: Concepts, Algorithms, Applications, and Prospects," *IEEE Access*, vol. 10, pp. 99 129–99 149, 2022.