Unsupervised Online AutoML for DDoS of Things Prediction by Multimodal Analysis

Ligia F. Borges*, Anderson B. de Neira†, Lucas Albano*, Michele Nogueira*†
*Department of Computer Science - Federal University of Minas Gerais, Brazil
†Department of Informatics - Federal University of Paraná, Brazil
Emails: {ligia.borges, lucasalbano, michele}@dcc.ufmg.br, andersonneira@ufpr.br

***Abstract*—Distributed Denial of Service (DDoS) of Things are becoming increasingly severe, characterized by unprecedented traffic volumes and rates. Predicting these attacks before they escalate is critical for reducing costs. However, the complex and multidimensional nature of DDoS attacks demands adaptive defense strategies, which are lacking in current approaches. Existing methods often depend on labeled datasets, offline processing or context-specific models, resulting in low prediction accuracy. Further, they tend to rely on homogeneous data sources, limiting their adaptability to the variability of real-world network environments. This paper introduces DELIBERATE, a novel technique for DDoS attack prediction that utilizes unsupervised online AutoML and ordinal pattern transformation through multimodal correlation analysis. DELIBERATE adapts itself to changes in network traffic by leveraging the correlation of heterogeneous data and ordinal patterns transformation, a noise-tolerant method suitable for IoT environments. It predicts DDoS attacks up to 47 minutes in advance. The method outperforms traditional approaches that depend on labeled data, extensive training, and complex neural networks.**

***Index Terms*—Cybersecurity, DDoS, Prediction, AutoML, multimodal correlation analysis**

I. Introduction

Distributed Denial of Service (DDoS) attacks are among the most damaging and frequent cyber threats [1]. These attacks rapidly exhaust victims' computational resources, resulting in service disruptions. DDoS of Things attacks, which exploit IoT devices given their vulnerabilities, further amplify this impact. In the first quarter of 2024 alone, the number of DDoS attacks surged by 50%, reaching 4.5 million—up significantly from the same period in 2023 [2]. A recent study found that if an automated mitigation solution takes longer than 10 seconds to respond to a DDoS attack, potential financial losses can soar to as much as $36 million [3]. Given these risks, it is critical to explore methods for predicting DDoS attacks. Anticipating these attacks before they effectively begin significantly lowers the costs associated with mitigation and recovery.

Existing prediction approaches apply Machine Learning (ML) techniques. However, ML models are time-consuming and require significant expertise [4], [5]. Approximately 40% of companies spend over a month developing and configuring these models. The lengthy training periods and manual model selection processes impede the timely prediction of DDoS attacks. Furthermore, as traffic patterns evolve, these models risk becoming obsolete. The complexity of predicting DDoS attacks also stems from their multifaceted nature and the imbalanced data generated during the preparation phase, which produces minimal traffic [4]. Multimodal data, such as cross-layer attributes and log files, can provide valuable insights by identifying patterns. However, the heterogeneous nature of this data makes it susceptible to noise, which can compromise analysis if proper preprocessing and feature selection techniques are not applied [6].

In addition to the time necessary to deliver a model, predicting DDoS attack proposals often do not operate online [1], [4], [5], use neural networks with long training times and high computational demands that are impractical for IoT environments, or rely on supervised methods, which require labeled data and are context-specific [1], [7]–[9]. The extensive training process delays or hinders the ability to predict DDoS attacks [8]. Furthermore, relying on labels limits the ability to predict attacks to those similar to the labeled data, is costly, and requires manual annotation. Also, the solutions employ a reduced set of attributes and features, adhering to a single-modal approach, which provides a less comprehensive understanding of data variability [1], [7]–[9].

This work introduces DELIBERATE, a technique based on unsuperviseD onlinE automL and ordinal pattern transformation for predIcting DDoS attack by hEteRogeneous dATa corrElation. Unlike traditional fixed architectures [8], DELIBERATE dynamically adapts to evolving network traffic. It processes multimodal data (e.g., logs and cross-layer attributes) by converting them into multivariate time series (MTS). These MTS are then transformed into ordinal patterns and transition graphs (i.e., Bandt-Pompe symbolization) to extract features. The Bandt-Pompe transformation is crucial for data correlation and for identifying distribution patterns. It is noise-tolerant and has been used in IoT environments [5], [10]. The new features are used as input for an innovative unsupervised online AutoML component that autonomously predicts DDoS attacks without requiring manual configuration. The online AutoML selects the best models from 165 options without labeled data. Before alerting the security team, DELIBERATE cross-verifies the selected models across heterogeneous data sources to deliberate on whether the identified signal indicates an imminent DDoS attack.

The performance evaluation follows four datasets, each

This work was supported by MCTI/FAPESP, grants #2022/06840-0, #2023/13773-0, #2018/23098-0 #2023-13773-0 and CAPES.

representing different DDoS attacks and network scenarios (e.g., Internet, local network and IoT). In Experiment 1, the method predicted the attack 47 minutes and 42 seconds before it began, achieving an accuracy of 92.9%. In Experiment 2, the prediction occurred 2 minutes and 21 seconds in advance, with 92.3% of accuracy. In Experiment 3, the prediction occurred 20 minutes and 37 seconds ahead, while in Dataset 4, It predicted the attack 21 minutes in advance, with an accuracy of 95%. These results demonstrate significantly improved prediction times compared to existing literature [1], [4], [5], [8], while the cross-checked models further reduce errors and enhance reliability.

This paper proceeds as follows. Section II presents the related works. Section III details the DDoS attack prediction technique. Section IV presents the results. Finally, Section V concludes the paper.

II. Related Works

The literature on DDoS attack prediction is still in its emerging stages. As a result, the term prediction is not well-defined. For example, some studies use the term to describe the detection of attacks that are already in progress [11]–[13]. This work focuses on predicting DDoS attacks by identifying signals of attack preparation before the actual launch [1], [5], [7]. Only a few studies have focused on predicting DDoS attacks before they start. However, existing solutions often rely on a limited set of features and follow a single-modal approach, typically based solely on network packet data [1], [4], [5], [7], [8]. This narrow focus provides a less comprehensive understanding of data variability, which limits prediction accuracy. Additionally, many of these approaches require labeled data [1], do not operate online [4], [5] or involve complex neural networks [8], [9], which demand long training times, high computational power, and often neglect feature selection [1], [5], [7], [8], reducing the prediction time.

Feature selection enhances cybersecurity solutions by focusing on the most relevant data. However, it remains little explored in DDoS attack prediction, where many approaches still rely on a limited set of features. Mohmand et al. (2022) [14] proposed a DDoS classification method for model selection. Still, it depends on labeled data, limiting its effectiveness against zero-day attacks, and it is impractical to train models for all potential attacks. Related to data correlation, most existing works address attack or anomaly detection, not attack prediction. For instance, in [15], the authors propose a DDoS attack detection approach using Pearson, Spearman, and Kendall techniques to identify uncorrelated feature subsets. However, the classification considered only single-modal data.

This work advances the literature by presenting an online DDoS attack prediction approach based on heterogeneous data correlation and feature selection. The solution adapts to evolving network traffic, and does not require labeled data or manual configuration, avoiding dependence on specific attack types and delays. It benefits from heterogeneous time series and ordinal patterns—a noise-resistant method that is significant for handling large volumes and heterogeneous data.

III. DDoS Attack Prediction Technique by Online Unsupervised AutoML

This section describes the proposed DELIBERATE technique to predict DDoS attacks using heterogeneous data (Fig.1). The technique applies multimodal data transformation into ordinal patterns to extract features that evidence signals of attack preparation. The features are input for a new unsupervised online AutoML component that autonomously predicts DDoS attacks. The AutoML selects and cross-verifies optimal ML models from 165 options (selected for each data type: logs or network traffic) to deliberate if the identified signal indicates an imminent DDoS attack.

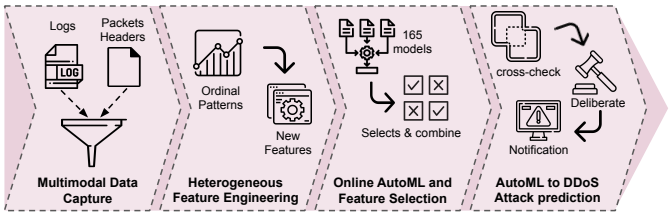

Figure 1. Overview of the DELIBERATE technique

A. Capture of Network Traffic and Logs

In the first step, multimodal data collection (network traffic and logs attributes) occurs. A firewall-integrated monitor captures network packet headers across different layers, forwarding copies to a PCAP file server for storage. The captured header data is temporarily saved in PCAP format. By default, the proposed technique collects 45 cross-layer attributes (e.g., attributes from different network layers of the protocol stack). Even though these attributes are predefined, users can customize them based on their needs. The proposed method extracts the attributes at specified time intervals and organizes them sequentially based on the capture order. The time interval is set to one second by default, but users can modify this according to their needs. Each collected network traffic attribute is represented as a time series and processed by the method accordingly.

In addition to network traffic attributes, the technique analyzes text from Apache Web Server access logs and firewall logs (i.e., configured with iptables rules to reject packets on all ports except 80 and 22). These logs are collected and grouped into one-second intervals. From this data, various attributes are extracted, such as the total number of access or firewall logs, the number of unique URLs, and the type of service identified by the firewall. The proposal extracts the multimodal attributes (i.e., network traffic and logs) per capture cycle, forming a Multivariate Time Series (MTS) where each selected attribute represents a dimension in the MTS. The technique is adaptable and functions effectively even when only partial or single-modal data (e.g., only cross-layer attributes) is available. The complete list of extracted features is available online*.

*https://github.com/mentoredproject/WP2-Deliberate-IEEEICC2025.git

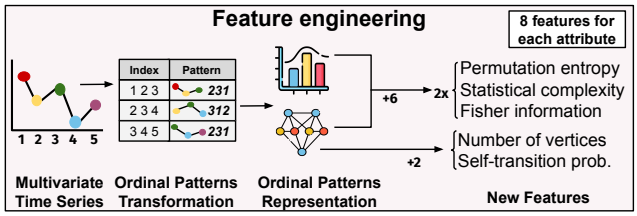

Figure 2. Feature Engineering

B. Heterogeneous Feature Engineering

In this step, the technique engineers relevant features for DDoS attack prediction (Fig. 2). First, the proposal applies the Bandt-Pompe transformation to the MTS, a robust method that significantly reduces noise sensitivity and minimizes false positives [5], [10]. Rather than analyzing raw data, it extracts data complexity representations that enable faster processing, making it suitable for real-time applications and IoT environments [5]. This process takes MTS as input and outputs ordinal patterns by dividing the MTS into size d=3 subsets at each time (t = 1 second) in a sliding window, generating ordinal patterns by sorting each value of the subsets in ascending order. The transformed time series (ordinal patterns) are then represented as transition graphs and probability distributions. After these processes, the solution leverages information theory quantifiers to evaluate the complexity and behavior of the multivariate time series (distribution pattern). This makes it possible to identify deviations from regular network activity.

Key features include normalized permutation entropy, statistical complexity, Fisher information, the number of vertices in the transition graph, and metrics related to edge-weighted distributions and vertex self-transitions. At the end of this process, the technique generates eight features based on these metrics for each input attribute. The engineered feature was evaluated in previous work [5], demonstrating suitability for highlighting signs of attack preparation. However, that work was conducted in a different context, lacking the possibility of incorporating heterogeneous data, feature selection, or online processing (i.e., required a separate training step for prediction) and required manual model identification and configuration.

C. Online AutoML and Feature Selection

One of the key contributions of this work is the proposal of a new online unsupervised AutoML component designed to identify the optimal model for predicting DDoS attacks. The first action of AutoML is to employ FastICA to reduce the dimensionality of the multimodal data (e.g., network traffic features and logs) preprocessed in the preceding step. By minimizing the dataset size, the online AutoML effectively reduces resource consumption (both in terms of time and computational power) while preserving the most relevant features. FastICA offers a highly efficient implementation of Independent Component Analysis (ICA), providing remarkable computational speed. ICA extracts statistically independent components, which are essential for capturing the underlying data structure required for component extraction and signal separation tasks [16]. In this way, ICA isolates signals from different sources within a mixture of combined signals [17]. FastICA requires reporting the total number of components. The DELIBERATE technique uses 21 components to maximize the DDoS attack prediction.

The online unsupervised AutoML analyzes 165 models based on One-Class SVM, One-Class SVM with Stochastic Gradient Descent (SGD), Local Outlier Factor (LOF), and Elliptic Envelope algorithms. The objective of using 165 models is to combine them to improve the DDoS attack prediction and identify the most suitable combination of models for this task. One-Class SVM functions as a decision mechanism, creating a boundary encompassing most normal data. Data points within this boundary are classified as normal (e.g., regular network traffic), while those outside are identified as outliers (e.g., DDoS attack preparation). This work relates One-Class SVM to unsupervised ML, as the results (predictions) dot required label data [18]. These features make One-Class SVM particularly well-suited for predicting DDoS attacks, where data is often imbalanced.

One-Class SVM has parameters that characterize fundamental roles in the algorithms' capability to operate with high-dimensional data. The kernel parameter (poly, linear, RBF, sigmoid, and precomputed) determines data separation[†] and the nu serves as a threshold (upper bound) for the error rate during the process and a lower limit for the proportion of support vectors. The nu value must be in the $(0, 1]$ range, representing the percentage of data points (e.g., network traffic) classified as outliers (i.e., DDoS attack preparation). Adjusting nu within the range $(0, 1]$ controls the proportion of data flagged as abnormal, including potential DDoS attack traffic. This work varied the kernel and nu parameters to generate 30 One-Class SVM models. The kernel was set to either RBF or $sigmoid$. For each kernel, the nu parameter ranged from 0.05 to 0.20, with increments of 0.01. This resulted in 15 models using the RBF kernel and 15 using the $sigmoid$ kernel, with nu varying within the specified range. These parameters were chosen to ensure diversity in the ensemble and address the data imbalance inherent in predicting DDoS attacks [19].

The online AutoML uses 60 SGD One-Class SVM models, which optimize resource usage while maintaining accuracy[‡]. SGD One-Class SVM includes essential parameters, such as the nu parameter, which operates in the same manner as in the standard version. Furthermore, the SGD One-class SVM has the learning rate parameter $learning\_rate$ (i.e., set as constant, optimal, invscaling, or adaptive) that modifies the improvement stage by adjusting the parameter space. Thus, the 60 models were generated by varying the parameter nu from 0.05 to 0.20 in increments of 0.01, alongside four learning rates (constant, optimal, invscaling, and adaptive). Each learning rate generated 15 models, totaling 60 models.

[†]scikit-learn.org/stable/modules/generated/sklearn.svm.OneClassSVM.html
[‡]scikit-learn.org/stable/modules/sgd.html#online-one-class-svm

In addition to 30 One-Class SVM-based models and 60 SGD one-class SVM-based models, the online AutoML includes 15 Elliptic Envelope-based models and 60 Local Outlier Factor (LOF) based models. The Elliptic Envelope assumes that network traffic follows a specific distribution, such as Gaussian. Based on this assumption, it models the inliers' shape, representing normal traffic[§]. In this context, outliers indicate network traffic affected by DDoS attack preparation. LOF [¶] calculates density deviation to neighbors, making it suitable for high-dimensional datasets. For the Elliptic Envelope, only the contamination attribute, indicating the percentage of outlier data points (0.05 to 0.20), was varied, generating 15 models. For LOF, both the $contamination$ parameter (ranging from $[0.05$ to $0.20)$ in steps of 0.01) and the $algorithm$ parameter (with values *auto*, *ball_tree*, *kd_tree,* and *brute*) were varied, generating 60 models.

Figure 3 illustrates the unsupervised online AutoML. After applying the Bandt-Pompe transformation (step 2) to the heterogeneous data (e.g., network traffic features and logs) in 1-second cycles, the proposal temporarily accumulates 45 capture cycles (45 seconds of heterogeneous data) to use online AutoML. Temporarily storing 45 cycles allows unsupervised online AutoML to eliminate the need for a model training phase without delaying DDoS attack prediction. Therefore, every 45 seconds, the unsupervised online AutoML analyzes data for DDoS attack indicators using Scikit-Learns' *fit_predict* across 165 models. The DELIBERATE technique applies this process to network traffic and logs.

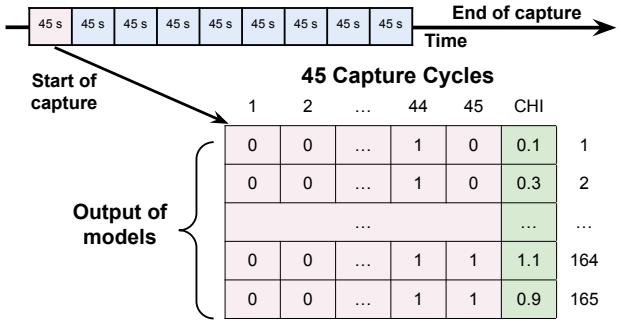

Figure 3. Unsupervised Online AutoML Execution Overview

Each output of the models (i.e., DDoS attack preparation signals) is evaluated using the Calinski–Harabasz Index (CHI). The CHI is the metric used to assess the quality of clustering [20]. CHI is based on the average sum of squared distances between and within clusters and has no upper limit. Higher CHI values indicate dense clusters (i.e., samples within clusters are close). Thus, a higher CHI suggests better clustering [20].

D. DDoS Attack Prediction

In Step 4, the unsupervised online AutoML selects the models that best distinguish abnormal (i.e., DDoS attack preparation signals) from normal (regular traffic data) observations. This is achieved by identifying the model that maximizes the CHI value, indicating the optimal separation of the data. The abnormal observations, representing subtle changes in data across capture cycles, were highlighted in Step 2, where ordinal transformation and feature engineering enabled the correlation of data patterns. The DELIBERATE technique combines the outputs with the AND logic gate. Thus, for the prediction to occur, both models chosen as ideal for each data source type must agree that the data collected in the capture cycles represent the DDoS attack preparation signals. Outlier capture cycles identified by the CHI-maximizing models alert security teams to potential DDoS attack preparations.

IV. Evaluation

The DELIBERATE technique evaluation involves four experiments using datasets with various DDoS attacks, network scenarios, and heterogeneous data. The datasets' documentation includes information on the device infections and/or timing of DDoS attacks. This is important to ensure an accurate evaluation, as the technique predicts the attack before it is launched by identifying the attack preparation signals. The technique analyses multimodal data sources to improve DDoS attack predictions. However, it can also operate on cross-layer attributes when that is the only available information. The evaluation considered both scenarios. Each experiment defines the data utilized. All findings can be found online[*].

A. Experiments Definition

Experiment 1 (Exp 1) analyzes traffic from a local network using the capture 51 of the CTU-13 dataset [21]. This dataset includes 8803 seconds of traffic, 41 GB of data, 46 million packets, ICMP and UDP flood DDoS attacks, and 10 bots. Researchers have launched the attacks at 5632 second and combined the attacks with real data. Thus, the test went up to the second 5632, grouping the capture cycles (1 second of network traffic) in groups of 45 seconds.

Experiment 2 (Exp 2) employs the IoT-23 dataset with 23 DDoS attack scenarios in IoT environments [22]. Scenario 17 contains infected and active bots, has 8.3 GB, and 109 million packets sent in 24 hours. The researchers started the capture at 06:43:20, and the malware execution was at 11:43:43. Thus, the pre-infection traffic capture has legitimate traffic, and the post-infection traffic contains traces of the attack preparation (used for prediction). The documentation reported an electrical issue at the university, likely compromising the DDoS attack started.

Experiment 3 (Exp 3) evaluates cross-layer traffic from the CIC-DDoS2019 dataset with 19 DDoS attacks launched by researchers in two days [23]. The dataset has 27 GB of attack and legitimate traffic data and 61 million packets. Bots connected to the victim over the Internet. The first attack started on the second 1484. The experiment employs the DELIBERATE technique until the second 1484. Experiment 4 (Exp 4) examines traffic from a simulated network distributed

[§] scikit-learn.org/stable/modules/outlier_detection.html
[¶] https://shorturl.at/6v2wv

Table I
EXPERIMENT RESULTS AND LITERATURE COMPARISON

Exps	Acc.	Prec.	Rec.	Prediction	Dataset
Exp 1	92.93%	97.86%	92.93%	47m42s	CTU-13 (51)
Exp 2	89.7%	98.86%	89.7%	60s*	IoT-23
Exp 3	81.67%	77.55%	81.67%	20m37s	CIC-DDoS19
Exp 4	95.05%	94.25%	95.05%	21min51	Mentored
[5]	91.52%	85.6%	91.52%	34m55s	CTU-13 (51)
[5]	72.31%	78.70%	72.31%	34m55s*	IoT-23
[5]	69.26%	78.72%	69.26%	13m22s	CIC-DDoS19
[4]	100%	N/A	N/A	20ms*	IoT-23
[1]	99.60%	N/A	N/A	3m55s	CIC-DDoS19
[7]	N/A	N/A	N/A	5m41s	CTU-13 (51)
[8]	97.89%	97.4%	97.9%	29m51s	CTU-13 (51)

After bot infection*

across Brazil[‖]. The capture includes 5578 seconds of data, 13.6 GB, about 42.5 million packets, an HTTP flood attack, and five bots (IoT devices) controlled by an adversary. The attacker initiated a port scan at second 3601, followed by an automated vulnerability search and bot-to-target connection tests. The DDoS things with HTTP flood began at second 5282. Following the default configuration, the DELIBERATE technique was initially applied to each data source separately. Then, the AutoML selects models for each data type were combined and cross-checked to enhance DDoS prediction, reduce false positives, and improve accuracy.

In all experiments, a one-second interval was used to group packets to obtain more accurate predictions [1]. This study labeled each interval as normal or malicious. Data labeling was used only to quantify the results since the unsupervised online AutoML does not require labels to predict DDoS attacks. The normal interval comprises all network traffic, where bots send or receive no packets. The malicious interval contains network traffic where at least three packets have a bot as their origin.

B. Results

Table I summarizes the results of all experiments and compares them to results of literature that predict DDoS attacks (i.e., before they start) applying different methodologies (N/A = not appear) [1], [7], [8]. In Exp 1, DELIBERATE correctly identified four malicious intervals where bots transfer data (true positive – TP). Thus, the proposed method issues two alerts indicating a DDoS attack preparation signal. The first correct alert occurred 47 minutes and 42 seconds before the attack started. The method correctly identified 4412 normal intervals (true negative — TN), 288 normal intervals as outliers (false positives — FP), and 48 malicious intervals were incorrectly identified as normal intervals (false negatives – FN). The results indicate an accuracy of 92.93%, weighted precision of 97.86%, and weighted recall of 92.93%.

Exp 2 results focus on 80 minutes before and 50 minutes after malware execution. The analysis used 50 minutes to show that DELIBERATE quickly identifies attack preparation signals, even in an imbalanced scenario. DELIBERATE identified the attack preparation only 60 seconds after malware execution with 89.87% accuracy (Tab. I), 2 VPs, 1063 FPs, 58 FNs, and 9760 VNs. This yields a weighted precision of 98.86% and a weighted recall of 89.70%. In Exp 3, the technique has correctly identified 21 malicious intervals (TP). Thus, it would issue 21 alerts indicating an upcoming DDoS attack. The attack prediction occurred 20 minutes and 37 seconds before the attack started. The FP was 77, with 158 FN and 1026 TN. Results indicate an accuracy of 81.67%, a weighted precision of 77.55%, and a weighted recall of 81.67%.

In Exp 4, DELIBERATE has correctly indicated 5 TPs, 9 FPs, 196 FNs, and 4514 TNs with an accuracy of 95.66%, a weighted precision of 93.28%, and a weighted recall of 95.66%. The technique identified the attack preparation 21 minutes and 51 seconds before the DDoS attack was launched. These results consider the standard execution of the DELIBERATE, where the technique combines the outputs of the best ML models for each data source. As mentioned in the previous section, the AND logic gate performs the combination. Thus, for the prediction to occur, ML models selected by the DELIBERATE technique must "agree" that the capture cycles are malicious. For the purpose of comparison, this work also presents the results obtained using a single data source. Applying the DELIBERATE technique only to network traffic, the results indicate an accuracy of 90.41%, a weighted precision of 92.06%, and a weighted recall of 90.41%. These results show that considering heterogeneous data sources in the analyses improves attack prediction regarding accuracy and error reduction.

C. Discussion

The DELIBERATE technique successfully predicted diverse DDoS attacks in all experiments with different scenarios. In Exp 1, the first one-second interval correctly identified by the technique as malicious was the second 2749. Since it is necessary to wait for the 45-second temporary storage to run the online AutoML (Subsection III-C), the first correct prediction occurred in the second 2770. This represents 47 minutes and 42 seconds before the attack started. This prediction time exceeds those obtained in [1], [4], [5], [7], [8] (Table I). The findings suggested that temporary storage has minimal impact on prediction time.

The accuracy obtained in this experiment surpasses that of [1], [4], [5], [7]. While the method in [8] took 42 minutes to find the best neural network for the dataset, the DELIBERATE technique required only 58 seconds (i.e., considering temporary storage time). In addition, the DELIBERATE selects different techniques as the network traffic evolves. While the work [8] selects a neural network architecture and finalizes its operation, DELIBERATE achieves these results without labeled data, highlighting the contribution of this study.

Exp 2 highlighted the importance of identifying attack preparation, though the attack launch time could not be determined. The results indicate that the prediction occurred just 60 seconds after bot infection in an IoT environment. In contrast, previous studies [4], [5] identified the attack signals only 34

[‖]https://github.com/mentoredtestbed

and 20 minutes after bot infection. Thus, DELIBERATE has maximized the time to deal with attack.

In Exp 3, the prediction occurred 20 minutes and 37 seconds before the DDoS attack started. This result is notable as it surpasses the prediction time in [1], [5] while maintaining competitive metrics with existing literature. Unlike [1], which uses labeled data to achieve 99.60% accuracy on the CIC-DDoS19 dataset, the DELIBERATE technique adapts to network traffic changes, reaching 81.67% accuracy without labeled data by selecting optimal models for each context.

In Exp 4, the prediction occurred 21 minutes and 51 seconds before the DDoS attack, with an accuracy of 95.05% by combining two data sources: network traffic and firewall logs. This is significant, as using only network traffic or firewall logs alone would yield accuracies of 90.41% and 95.05%, respectively. By integrating the model outputs (as detailed in Section III), the proposed solution minimizes errors, reducing false positives (FPs) from 270 (network traffic) and 85 (firewall logs) to just 9 when combined. This sharp reduction in FPs significantly aids network administrators in defending against DDoS attacks by minimizing incorrect predictions.

In addition to utilizing different data sources, AutoML also played a key role in achieving the results observed in this work. In Exp 1, the technique selected 29 models throughout its execution. The most frequently chosen models were EllipticEnvelope (contamination=0.05), LocalOutlierFactor (n_neighbors=5, algorithm=auto), and EllipticEnvelope (contamination=0.07), selected 18, 17, and 14 times, respectively. In Exp 2, DELIBERATE selected 9 different models, with EllipticEnvelope (contamination=0.05), EllipticEnvelope (contamination=0.07), and LocalOutlierFactor (n_neighbors=6, algorithm=auto) being chosen most often, each selected three times. In Exp 3, 17 different models were used, with the most frequently selected being LocalOutlierFactor (n_neighbors=5, algorithm=auto), chosen six times during the evaluation.

In Exp 4, the DELIBERATE technique selected 28 different models for network traffic. The most frequently chosen were EllipticEnvelope (contamination = 0.05), with 39 selections, and LocalOutlierFactor (n_neighbors = 5, algorithm=auto), with 23 selections. The technique selected only five models for processing firewall logs because several capture cycles lacked logs. Consequently, it had no data to predict DDoS attacks or select a model during those periods. The DELIBERATE technique chosed three versions of OneClassSVM with $kernel = rbf$ and $nu = [0.06, 0.11, 0.12]$, one version of OneClassSVM with $kernel = sigmoid$ and $nu = 0.17$, and one LocalOutlierFactor (n_neighbors=5). All details of the selected techniques are available online*.

V. Conclusion

Identifying early signs of DDoS attack preparation is crucial for staying ahead of attackers and minimizing damage. This work introduces the DELIBERATE technique, which leverages multimodal data analysis and a unique unsupervised online AutoML to predict diverse DDoS attacks across different network scenarios (e.g., Internet, local networks, and IoT) with lower error rates. DELIBERATE dynamically selects the optimal machine learning model for DDoS attack prediction as network traffic evolves, adapting to new behaviors without needing labeled data. It combines predictions from various data sources for more reliable and accurate results, surpassing the current literature on DDoS attack prediction time and nearing the performance of labeled data solutions.

References

[1] A. B. d. Neira, A. M. d. Araujo, and M. Nogueira, "An intelligent system for DDoS attack prediction based on early warning signals," *IEEE TNSM*, vol. 20, no. 2, pp. 1254–1266, 2023.

[2] O. Yoachimik and J. Pacheco, "DDoS threat report for 2024 Q1 [Accessed in: 07/2024]," https://blog.cloudflare.com/ddos-threat-report-for-2024-q1, Cloudflare, 2024.

[3] CORERO, "The need for always-on in real-timeddos security solutions[(Accessed on: October 2023)]," https://abrir.link/3L3Jo, CORERO NETWORK SECURITY, 2020.

[4] A. Neira, L. Borges, A. Araújo, and M. Nogueira, "Unsupervised feature engineering approach to predict DDoS attacks," in *IEEE Globecom*. Malaysia: IEEE, 2023.

[5] L. Borges, A. B. de Neira, L. Albano, and M. Nogueira, "Multifaceted DDoS attack prediction by multivariate time series and ordinal patterns (to appear)," in *ICC Workshops*, USA, 2024.

[6] P. J. Brockwell and R. A. Davis, *Time series: theory and methods*. Springer science & business media, 2009.

[7] B. M. Rahal, A. Santos, and M. Nogueira, "A distributed architecture for DDoS prediction and bot detection," *IEEE Access*, vol. 8, p. 17, 2020.

[8] D. Brito, A. B. de Neira, L. F. Borges, and M. Nogueira, "An autonomous system for predicting DDoS attacks on local area networks and the Internet," in *LATINCOM*. Panama: IEEE, 2023, pp. 1–6.

[9] G. L. F. M. E Silva, A. B. de Neira, and M. Nogueira, "A deep learning-based system for DDoS attack anticipation," in *LATINCOM*, 2022, p. 6.

[10] C. Bandt and B. Pompe, "Permutation entropy: a natural complexity measure for time series," *PL*, vol. 99, no. 17, p. 1541, 2002.

[11] D. R. Manikandan, S. Dharshini, and N. Pavithra, "DDoS attack prediction system," *IJRASET*, vol. 11, no. 5, p. 7629–7633, May 2023.

[12] P. Verma, A. R. K. Kowsik, R. K. Pateriya, N. Bharot, A. Vidyarthi, and D. Gupta, "A stacked ensemble approach to generalize the classifier prediction for the detection of DDoS attack in cloud network," *Mobile Networks and Applications*, Aug. 2023.

[13] H. Zhou, Y. Zheng, X. Jia, and J. Shu, "Collaborative prediction and detection of DDoS attacks in edge computing: A deep learning-based approach with distributed SDN," *CN*, vol. 225, p. 109642, 2023.

[14] M. I. Mohmand, H. Hussain, A. A. Khan, U. Ullah, M. Zakarya, A. Ahmed, M. Raza, I. U. Rahman, M. Haleem *et al.*, "A machine learning-based classification and prediction technique for DDoS attacks," *IEEE Access*, vol. 10, pp. 21 443–21 454, 2022.

[15] K. B. Dasari and N. Devarakonda, "Tcp/udp-based exploitation ddos attacks detection using ai classification algorithms with common uncorrelated feature subset selected by pearson, spearman and kendall correlation methods," *RIA*, vol. 36, no. 1, pp. 61–71, 2022.

[16] A. Hyvärinen and E. Oja, "Independent component analysis: algorithms and applications," *NN*, vol. 13, no. 4–5, p. 411–430, Jun. 2000.

[17] D. Li, J. Zhao, H. Liu, and D. Hao, "The application of FastICA combined with related function in blind signal separation," *MPE*, vol. 2014, p. 1–9, 2014.

[18] G. James, D. Witten, T. Hastie, R. Tibshirani, and J. Taylor, *Unsupervised Learning*. Cham: Springer, 2023, pp. 503–556.

[19] M. Abdlhamed, K. Kifayat, Q. Shi, and W. Hurst, *Intrusion Prediction Systems*. Cham: Springer, 2017, pp. 155–174.

[20] T. Caliński and J. Harabasz, "A dendrite method for cluster analysis," *Communications in Statistics*, vol. 3, no. 1, pp. 1–27, 1974.

[21] S. Garcia, M. Grill, J. Stiborek, and A. Zunino, "An empirical comparison of botnet detection methods," *C&S*, vol. 45, pp. 100–123, 2014.

[22] S. Garcia, A. Parmisano, and M. J. Erquiaga, "IoT-23: A labeled dataset with malicious and benign IoT network traffic," 2020.

[23] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy," in *ICCST*, 2019.