2024 IEEE Latin-American Conference on Communications (LATINCOM) | 979-8-3315-2111-0/24/$31.00 ©2024 IEEE | DOI: 10.1109/LATINCOM62985.2024.10770668

Unsupervised AutoML and Dimensionality Reduction for Autonomous DDoS Attack Prediction

Anderson B. de Neira*, Ligia F. Borges†, Daniel M. Batista‡, Michele Nogueira*†
*Department of Informatics - Federal University of Paraná, Brazil
†Department of Computer Science - Federal University of Minas Gerais, Brazil
‡ Department of Computer Science - University of São Paulo, Brazil
Emails: abneira@inf.ufpr.br, {ligiaborges, michele}@dcc.ufmg.br, batista@ime.usp.br

***Abstract*—Machine learning models and feature selection are crucial for predicting Distributed Denial of Service (DDoS) attacks. Predicting attacks with high accuracy allows security teams to reduce attack damage. However, diversity in attacks and models limits predictions. Moreover, the dependence on labeled data and the utilization of unexpressive features restrict the performance of prediction models. This work proposes the AUTO-SEE technique to solve this problem. The technique engineers new features to reveal signals of attack preparation and selects the best features and the optimal machine learning model without using labeled data. This enables the technique to operate autonomously and predict different DDoS attack types, also increasing the protection against 0-day attacks. The results indicate that AUTO-SEE reduces error by up to 44.15%, reaching an accuracy between 72.41 and 100% in predicting DDoS attacks.**

***Index Terms*—AutoML, Unsupervised ML, Feature Selection.**

I. Introduction

Cyberattacks are evolving in volume, sophistication, and frequency. DDoS attacks are one of the most detrimental cyber threats [1]. A DDoS attack, after effectively launched, rapidly consumes the computational resources of victims, leading to a denial of service. DDoS attacks have reached an unprecedented volume of data. In 2023, Google experienced a DDoS attack, reaching 398 million requests per second. This attack lasted about two minutes, and within less than 30 seconds, it reached the peak of requests [2].

The literature suggests that the most appropriate time to deal with the attack is before the attacker launches it [3]. Thus, recent literature has explored solutions for predicting DDoS attacks [3]–[7]. However, there are still opportunities for more effective solutions. Three main limitations in existing solutions are predicting attacks based on labeled data [5], manually configuring solutions [8], and requiring a long time to identify the ideal model [6]. Solutions based on labeled data limit the prediction of different attacks from those trained [5]. Furthermore, attackers are becoming increasingly skilled at masking their actions amidst normal traffic [9]. This makes DDoS attack prediction even more challenging. Therefore, selecting features that characterize the attack preparation is essential, given the high volume of data. Finally, spending too much time identifying models can delay attack predictions.

This work introduces the AUTO-SEE technique that autonomously predicts DDoS attacks. It identifies groups of network traffic that represent attack preparation without requiring labeled data or manual configuration. AUTO-SEE selects the best features in an unsupervised manner to maximize prediction accuracy, and autonomously chooses the most suitable unsupervised machine learning model. The technique includes models based on K-means, Self-organizing Map (SOM), Birch, and others. AUTO-SEE evaluates 37 models and selects the best fit for the network context to identify attack preparation signals and predict DDoS attacks.

This work evaluates the AUTO-SEE technique through four experiments using datasets of DDoS attacks on the Internet, IoT, and internal networks. In Experiment 1, AUTO-SEE predicted an attack 30 minutes before it started, 25 minutes earlier than [10], with an accuracy of 91.4% and a 44.15% reduction in errors compared to [8]. In Experiment 2, prediction occurred 3 minutes and 56 seconds with an accuracy of 92.3%. In Experiment 3, the prediction time was 22 minutes and 5 seconds, 6 minutes and 44 seconds earlier than [6], with an accuracy of 72.41%. In Experiment 4, prediction occurred 20 minutes after bot infection, with an accuracy of 100%, surpassing [7]. The results are significant because AUTO-SEE autonomously selects features and models and predicts DDoS attacks without labeled data or prior knowledge, simplifying adaptation and enabling the prediction of unknown DDoS attacks. Finally, the code and results of AUTO-SEE are available online[1].

This paper flows as follows. Section II presents related works. Section III details the proposed technique. Section IV discusses the results. Finally, Section V finalizes the paper.

II. Related Works

The literature has defined Automated Machine Learning (AutoML) as a research area aiming to simplify the use and reduce the cost of machine learning. Accordingly, AutoML aims to identify and configure a machine learning algorithm that reduces classification errors for the selected dataset [11].

This work was supported by National Council for Scientific and Technological Development (CNPq), grants #309129/2017-6 and #432204/2018-0, by São Paulo Research Foundation (FAPESP), grants #2018/23098-0, #2022/06840-0, #2023/13773-0, and #2021/06995-0, by the Coordination for the Improvement of Higher Education Personnel (CAPES), grant #88887.509309/2020-00. It is also part of the INCT of the Future Internet for Smart Cities funded by CNPq proc. 465446/2014-0, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Finance Code 001, FAPESP proc. 14/50937-1, and FAPESP proc. 15/24485-9.

[1]https://github.com/andersonneira/latincom-2024

Authorized licensed use limited to: Universidade Tecnologica Federal do Parana. Downloaded on July 14,2025 at 22:54:07 UTC from IEEE Xplore. Restrictions apply.

Hyperparameter Optimization (HPO) type AutoMLs are the most commonly found in the literature, since they aim to define and configure shallow machine learning algorithms (i.e., traditional machine learning algorithms that do not apply multiple hidden layers) [11]. Some HPO-type AutoMLs can suggest a technique for feature selection to reduce classification errors [11]. Neural Architecture Search (NAS) type AutoMLs specialize in selecting and configuring deep learning-like machine learning algorithms to maximize accuracy [12]. Deep learning solutions offer the advantage of not requiring prior attribute selection. However, most AutoML solutions still depend on labeled data for model selection.

In [13], the author focuses on selecting unsupervised algorithms. The proposal evaluates several unsupervised algorithms on different datasets offline. For all models, the solution extracts indexes such as Calinski-Harabasz and Davies-Bouldin from clusters to identify the model that maximizes these indexes. The hypothesis is that similar datasets should have similar solutions. When the proposed solution processes a new dataset, it compares it with the offline knowledge base and suggests the algorithm that best solved the problem previously.

The works that present solutions to predict DDoS attacks have limitations addressed by this work. The authors of [8] proposed a solution focused on explainability to identify the preparation of DDoS attacks using the theory of early warning signals [14]. This solution uses a fixed and predefined model and does not perform the selection of network traffic attributes, using only three. The work [6] evaluates AutoML to select the optimal neural network architecture to predict DDoS attacks. This process lasted between 28 and 42 minutes. The work of [5] uses labeled data to predict DDoS attacks. The solution proposed in [7] performs attack prediction with multilayer data from the TCP/IP model. However, the prediction is made based on manual feature selection and with a predefined model.

AUTO-SEE advances the literature by autonomously selecting the optimal clustering technique to predict DDoS attacks in a less complex process than that presented in [6]. Furthermore, unlike [13], AUTO-SEE suggests the most suitable unsupervised machine learning algorithm for new data without prior knowledge and labeled data. Finally, unsupervised feature selection reduces the total errors and improves attack predictions.

III. AUTO-SEE TECHNIQUE

This section details the AUTO-SEE technique (Fig. 1), which autonomously predicts DDoS attacks and performs feature selection without relying on labeled data. Unlike previous studies that conduct manual feature selection and configure clustering algorithms manually [7], [8], AUTO-SEE uses an unsupervised AutoML approach. This method optimizes network traffic and enhances prediction accuracy.

Fig. 1. AUTO-SEE technique architecture

Thus, AUTO-SEE advances the literature [5]–[8], [10] by proposing an unsupervised AutoML to select a model able of predicting attacks without using labeled data. Fig. 1 illustrates the five steps of the AUTO-SEE.

A. Capture Network Traffic

In Step 1, the network packet capture occurs. Security teams can use sniffer-type tools such as Wireshark, tcpdump, Windump, and OmniPeek for this process. These tools capture traffic on both wired and wireless networks. The efficiency of data collection directly influences all subsequent steps. A faster collection process enables the technique to predict attacks more promptly. Once the data is collected and stored, the technique can extract the network traffic attributes necessary for the subsequent step. The AUTO-SEE technique can collect network traffic in a distributed and centralized mode. Previous works had evaluated this network traffic collection modes [5], [8]. This work uses a centralized collection mode.

Security teams can choose the network traffic attributes to extract from the capture. The choice allows security teams to adapt the AUTO-SEE technique to predict DDoS attacks according to their objectives. For this reason, this work does not previously define the network traffic attributes. The literature presents some attributes to predict DDoS attacks [15]. Therefore, if security teams choose to do so, the AUTO-SEE technique can utilize those attributes. The total number of packets, the sum of packet bytes, and the number of packets per protocol are examples of network traffic attributes based solely on headers. The AUTO-SEE technique organizes each network traffic attribute as a time series to apply signal engineering (Step 2). The time series is a sequential collection of network traffic attributes organized over time.

B. Apply Signal Engineering

The AUTO-SEE technique utilizes signal engineering to process network traffic (Step 2) [5]. Signal engineering follows the early warning signals (EWS) theory, making it possible to identify signals that may represent future events (e.g., DDoS attacks). This theory suggests that observable systems change states passing critical transactions. In this transaction, an observable system can evolve into a state that presents disturbances and inconsistencies due to instabilities. For example, systems stop responding due to resource consumption, or networks become congested due to the high number of accesses.

EWS theory produces signals when the behavior of leading indicators changes due to the approach of a critical transition. Skewness, kurtosis, lag-k autocorrelation (AC-k, with $k \in \mathbb{N}$), and coefficient of variation (CV) are leading indicators that can produce EWS [16]. These indicators compose the AUTO-SEE technique because changes in their values reveal fluctuations in the network data distribution. Therefore, the technique generates novel network traffic features to unveil signals of attack preparation previously obscured by normal traffic [8].

After collecting network traffic data (i.e., attributes) and organizing it as a time series, the AUTO-SEE technique aggregates network traffic into time intervals. The security

Authorized licensed use limited to: Universidade Tecnologica Federal do Parana. Downloaded on July 14,2025 at 22:54:07 UTC from IEEE Xplore. Restrictions apply.

team is responsible for choosing the time interval. Maximizing available resources and predicting attacks accurately requires defining the ideal time interval. Signal engineering occurs when EWS theory, through leading indicators, processes the network traffic attributes (i.e., organized in time series and grouped at each time interval) to identify signals of future DDoS attacks. In order to avoid erroneous trends, AUTO-SEE uses a fixed-size sliding window concept over time [8], [17].

C. Feature Selection

Besides the AUTO-SEE, another contribution of this work is the investigation of dimensionality reduction without using labeled data to predict DDoS attacks. In other researches, feature selection was carried out manually [5]–[8]. Manual feature selection requires time, knowledge, and experience. Furthermore, the same features may not be ideal for different cases. Some solutions select features using labeled data, which may limit their application in real environments. AUTO-SEE reduces errors when using different features and solves these limitations by applying unsupervised dimensionality reduction.

The dimensionality reduction algorithm used is FastICA, a computationally efficient implementation of the Independent Component Analysis (ICA) [18]. The ICA finds a new representation of the data to make the components (new features) statistically independent. This representation captures essential data structures for various topics, such as component extraction and signal disunion [18]. Thus, ICA identifies signals from different sources among combined signals [19]. Using FastICA, the AUTO-SEE can adapt to different network traffic.

D. Apply AutoML

AUTO-SEE applies AutoML after the feature selection. AutoML aims to select the optimal unsupervised machine learning algorithm for the evaluated context (i.e., data resulting from signal engineering and feature selection). The first action necessary is to define the search space (Step 1). The search space comprises candidate unsupervised machine learning algorithms (i.e., candidates to be chosen based on the dataset). The AUTO-SEE technique uses ten algorithms: KMeans, Birch, Bisecting K-Means, Gaussian Mixture, Agglomerative Clustering, DBSCAN, OPTICS, MeanShift, HDBSCAN, and SOM. The proposed technique configures the default version of the algorithms, except for the number of clusters, which is two (Step 2). When using two clusters, AUTO-SEE separates normal traffic from attack preparation traffic as well as in [8].

AUTO-SEE defines another 28 variations of alternative configurations. For example, in the Scikit-Learn library, the K-Means algorithm has a parameter called *algorithm* that can take the values Lloyd or Elkan. The default value set by the library is Lloyd. By changing the value of this parameter, the clustering result may be different. Thus, the proposed algorithm evaluates different alternative configurations for the algorithm parameter. Table I displays all 37 candidates models.

After defining the candidate models, it is time to apply them to the data resulting from signal engineering and feature selection to identify the ideal one (Step 3). Evaluation metrics like accuracy, precision, and recall are used to assess machine learning models. These metrics require labeled data to be calculated. However, in unsupervised machine learning, original labels may not be available. Thus, the literature proposes other metrics to evaluate the quality of clustering performed by unsupervised machine learning, such as the silhouette, Calinski–Harabasz, Dunn, and Davies–Bouldin indexes. The AUTO-SEE technique evaluates candidate models using the composed density between and within clusters (CDbw) index [20]. The CDbw index does not require labeled data and is more recent than the previously mentioned indexes [20].

TABLE I
MODELS EVALUATED BY AUTO-SEE TECHNIQUE

Algorithm	Params
K-Means	algorithm={elkan, lloyd}, tol={0.001 - 1}
SOM	m=2, n=1, dim=data dimension
Birch	threshold={0.3 - 0.7}
Bisecting K-Means	init={random, k-means++}, algorithm={elkan, lloyd}, bisecting_strategy = {largest_cluster, biggest_inertia}
Gaussian Mixture	covariance_type={full, tied, diag, spherical} init_params={k-means, k-means++, random, random_from_data}
Agglomerative Clustering	linkage={ward, average, complete, single}
HDBSCAN	cluster_selection_method={eom, leaf}
DBSCAN	Default setting
OPTICS	Default setting
MeanShift	Default setting

The CDbw index uses Cohesion, Compactness, and Separation as essential criteria for evaluating clusters. This provides robustness in the analysis of results regarding the quality of clustering. The Equation 1 defines the CDbw index. CDbw index achieves high values for Cohesion and Separation concerning Compactness when the cluster exhibits compact, well-separated clusters and a low variation in the density distribution within the clusters. Thus, the higher the CDbw index value is, the better the clustering obtained [13], [20]. In the Formula of Halkidi and Vazirgiannis (2008) [20], the term $Cohesion(k)$ is the density of clusters concerning the density variations observed internally to them. The term $CS(k)$ evaluates the compactness of the clusters by relating it to the Separation of clusters (Eq. 1) [20].

$$CDbw(k) = Cohesion(k) \cdot SC(k) \tag{1}$$

The model that yields the maximum CDbw index is the selected model (Step 4). The AUTO-SEE technique evaluates all 37 models and uses the CDbw index to sort them in descending order. Thus, the first results are the models that maximize the selection criterion (CDbw index). If more than one model presents the same clustering, the result for the index will be the same. Therefore, unlike the literature [8], [10], AUTO-SEE can provide multiple models to predict attacks.

E. DDoS Attack Prediction

In Step 5 (Fig. 1), the proposed technique utilizes the selected and autonomously configured unsupervised machine

Authorized licensed use limited to: Universidade Tecnologica Federal do Parana. Downloaded on July 14,2025 at 22:54:07 UTC from IEEE Xplore. Restrictions apply.

learning model to predict DDoS attacks. Attack prediction happens when the model identifies changes in the data behavior represented by different clusters. Signal engineering (Step 2) highlights these changes in network traffic, which can be caused by the actions of attackers, such as traffic generated by bots or attack tests. Thus, when applying EWS theory to network traffic attributes, the change in network behavior, reflected in the results of the leading indicators, makes it possible to predict attacks [5], [8]. Figure 2 exemplifies the variation of the leading indicators. In Frame B, the leading indicators are far from the attack and have a specific behavior. Near the attack (Frame C), the behavior of the leading indicator presents variation, generating the signal used to predict attacks. Based on this premise, the AUTO-SEE technique utilizes the autonomously selected unsupervised machine learning model to process the collected data. In the case of identifying changes in the behavior of the data, the technique generates a notification indicating the beginning of the DDoS attack. The AUTO-SEE technique can send notifications to the monitoring systems of security teams through the Application Programming Interface.

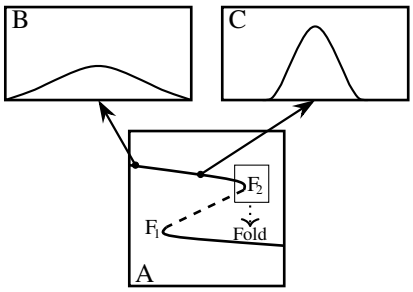

Fig. 2. Variation of data distribution in a critical transition [21]

IV. Performance Evaluation

This work performs four experiments to evaluate AUTO-SEE. The experiments consider datasets with different characteristics. These datasets include DDoS attacks within internal networks, networks where bots connect to the victim through the Internet, and IoT networks. Furthermore, they have different numbers of bots, different network traffic collection sizes, and various active normal devices.

Table II presents the 51 attributes utilized to evaluate the AUTO-SEE technique in the experiments. These attributes are based on the protocol fields of the link, network, and transport layers of the TCP/IP model. The AUTO-SEE does not use packet payload data (Sec. III). Thus, only the header data was considered in these experiments. Moreover, the AUTO-SEE technique does not perform preprocessing actions (standardization or scaling) on the collected network traffic. The 51 attributes are extracted and sorted by time intervals of one second for Experiments 1, 2, and 3 and one minute for Experiment 4. These values were defined to adapt to the characteristics of the datasets and to provide an evaluation of different time interval values.

AUTO-SEE does not use labels to predict attacks. However, this work marks the time intervals as normal and malicious

TABLE II
Attributes Evaluated by AUTO-SEE technique

Attributes
1-2. Total unique source/destination MAC addresses
3. Most frequent version of the protocol that will be in the payload
4-5. Smallest/largest packet size
6. Sum of packet sizes
7-9. Total packets of ICMP/UDP/TCP types
10-11. Total unique source/destination IP addresses
12-16. Largest/Smallest/Sum/STD/Mean of packets time to live
17. Total packets transmitted on the network
18-19. Most frequent source/destination port in packets
20. Total unique TCP flags
21-26. Total TCP flags FIN/SYN/RST/PUSH/ACK/URG
27-31. Largest/Smallest/Sum/STD/Mean of the TCP window size field value
32-36. Largest/Smallest/Sum/STD/Mean of the TCP Sequence Number field
37-46. Largest/Smallest/Sum/STD/Mean of the arrival time between any packets and TCP packets
47-51. Largest/Smallest/Sum/STD/Mean of the arrival time from the first TCP packet

to quantify the results. Malicious intervals comprise time intervals where bots send at least one packet. Thus, these intervals represent attack preparation, as the bots impacted network traffic before the attack launching. Normal intervals are time intervals where bots do not send packets.

The evaluation metrics are accuracy, precision, recall and F1-Score. Accuracy evaluated the system cauterization. Regardless, there were rare attack preparation signals because attackers obscured their movements. The F1-Score complemented the evaluation when calculating the harmonic mean between the weighted average of precision and recall. This work presents the weighted average of precision and recall per class, since precision and recall can be obtained for the normal and malicious classes. Since the DDoS attack prediction is an unbalanced problem, the weighted average complements the presentation of the results. Finally, the results are online[2].

A. Experiment 1

Experiment 1 evaluated capture 51 of the dataset developed by the Czech Technical University (CTU) called CTU-13 dataset [22]. This capture has 10 active bots on the network, 41 GB of data, 46,997,342 packets, 8803 seconds, and flood-type attacks. The infection began on second 2643, and the dataset developers launched the DDoS attack on second 5632. This experiment evaluates the attack prediction between seconds 3294 and 3794 of the dataset to validate the proposal and compare with [8].

AUTO-SEE performs signal engineering (Step 2 of Fig. 1) after collecting the 51 attributes presented in Table II (Step 1). Signal engineering applies AC-1, AC-2, AC-3, skewness, kurtosis, and CV to all collected data to create 306 new features at every one-second interval. The new features are the basis for all the following steps carried out by AUTO-SEE. Finally, the fixed-size sliding window is 880 seconds long (10% of the capture - Section III).

[2]https://github.com/andersonneira/latincom-2024

Authorized licensed use limited to: Universidade Tecnologica Federal do Parana. Downloaded on July 14,2025 at 22:54:07 UTC from IEEE Xplore. Restrictions apply.

Then, the technique performs feature selection. The dimensionality reduction algorithm is FastICA (Sec. III). FastICA requires specifying the number of signals to be decomposed. The chosen value in this evaluation was four, as it resulted in the best possible outcome. Therefore, the FastICA algorithm received the 306 new features as inputs and decomposes the data into four signals to predict DDoS attacks.

AUTO-SEE then uses the results of feature decomposition and applies AutoML to select the machine learning model and predict DDoS attacks. As a result, AUTO-SEE has identified the Agglomerative Clustering with two clusters and the attribute linkage= "average" as the ideal candidate. The technique autonomously predicted the DDoS attack with an accuracy of 91.4% (Table III), with the Agglomerative Clustering autonomously selected. The results indicate that the AUTO-SEE grouped time intervals where bots prepare for DDoS attacks with 88.18% of F1-score.

TABLE III
EXPERIMENT RESULTS AND LITERATURE COMPARISON

Experiment	Accuracy	F1-Score	Precision	Recall
Exp 1 (Cap. 51)	**91.4%**	**88.18%**	**87.55%**	**91.4%**
Exp 2 (Cap. 52)	**92.32%**	**94.68%**	**98.4%**	**92.32%**
Exp 3 (CIC)	**72.41%**	63.67%	**69.48%**	**72.41%**
Exp 4 (IoT-23)	**100%**	**100%**	**100%**	**100%**
[7] (Cap. 52)	89.65%	90.11%	90.58%	89.65%
[7] (IoT-23)	72.31%	67.6%	78.7%	72.31%
[8] (Cap. 51)	84.6%	85.52%	86.54%	84.6%
[8] (CIC)	70.69%	**69.89%**	**69.48%**	70.69%

B. Experiment 2

Experiment 2 evaluated AUTO-SEE applied to the capture 52 of the CTU-13 dataset [22]. This capture has three bots that send packets before the attack begins. The network traffic collection file is 555 MB, contains 6,336,398 packets, lasts 972 seconds, and includes an ICMP flood attack. The infection started on second 527, and the dataset developers launched the DDoS attack at second 778. This experiment evaluates attack prediction from seconds 48 to 542 to compare with [8].

AUTO-SEE performs signal engineering by applying AC-1, AC-2, AC-3, skewness, kurtosis, and CV to all collected data to create 306 new features at each one-second time interval. The fixed-size sliding window is 48 seconds, or 5% of the capture. This value makes it possible to evaluate a dataset 9 times smaller than the dataset used in Experiment 1. Also, FastICA decomposed the new features into three components.

After performing feature decomposition and applying AutoML, AUTO-SEE has identified 15 ideal candidate models. The models consist of 10 variations of K-means, Birch with two clusters and a threshold of 0.7, three versions of Agglomerative Clustering, and MeanShift with the default configuration of the Scikit-Learn library. Equipping AUTO-SEE with any of the 15 models yielded an accuracy of 92.32% and 94.68% of the F1-score (Table III).

C. Experiment 3

Experiment 3 uses the CICDDoS2019 [23] dataset. This dataset contains 19 scenarios of DDoS attacks where the Internet connects the victim network to the attacker. This experiment used the first DDoS attack on the first capture day. The captured network traffic file size is 27 GB, containing 61 million packets, recorded over 2024 seconds. During the recording, a PortMap-type attack was launched in the 1484th second. Finally, this experiment evaluates the attack prediction between seconds 101 and 159 of the dataset.

In the same way as the previous experiments, AUTO-SEE has generated 306 new features every second. It applies signal engineering to the collected data using six leading indicators (AC-1, AC-2, AC-3, skewness, kurtosis, and CV). The size of the fixed sliding window is 5% of the capture time, which is 101 seconds. The FastICA algorithm has decomposed the signal engineering result into five distinct features.

AUTO-SEE has identified five ideal candidate models based on the Birch algorithm configurations. The Birch configuration varies the threshold parameter between 0.3 and 0.7 in increments of 0.1. The clustering accuracy obtained using AUTO-SEE with any of the selected models was 72.41% (Table III). AUTO-SEE effectively predicts DDoS attacks by accurately clustering the time intervals in which bots prepared the attack by equipping it with any of the selected models.

D. Experiment 4

The dataset used in Experiment 4 is IoT-23 [24]. This dataset has 23 DDoS attack captures on IoT networks. Capture 17 contains various active bots and includes 8 GB and over 100 million packets sent in 24 hours. The researchers infected the devices at minute 301 of capture. Thus, pre-infection traffic capture contains normal traffic, and post-infection traffic contains DDoS attack preparation. Finally, the evaluation occurs between the seconds 241 and 321.

The dataset evaluation process for this experiment followed the same procedure as in previous experiments. Firstly, AUTO-SEE has performed signal engineering to create 306 new features per minute using a sliding window of 10% of the data (144 minutes). From these new features, FastICA selected six that maximized the prediction of DDoS attacks. The AUTO-SEE technique achieves 100% in all metrics (Table III) to cluster the time intervals during which the bots prepare for the attack. Moreover, AUTO-SEE has selected ten models based on K-means, achieving maximum results in predicting attacks.

E. Discussion

This section discusses the results and compares them with the literature. In Experiments 2, 3, and 4, AUTO-SEE suggested multiple models without prior training, labels, or human interaction. Signal engineering and feature selection made this possible, simplifying the DDoS attack prediction. AUTO-SEE has identified multiple models that output the same clustering, resulting in the same CDbw index value for different models. Then, the network administrator could equip AUTO-SEE with the algorithm that best suits their needs. Finally, in experiment 1, AUTO-SEE found one model to predict the DDoS attack.

The findings presented in Table III indicate that AUTO-SEE improves the accuracy of autonomously predicting unknown DDoS attacks. In Experiment 1, the total number of

Authorized licensed use limited to: Universidade Tecnologica Federal do Parana. Downloaded on July 14,2025 at 22:54:07 UTC from IEEE Xplore. Restrictions apply.

errors decreased from 77 to 43, a variation of 44.15% [8]. In Experiment 3, the AUTO-SEE eliminated false positives, meaning that the second cluster identified by the proposal only contains malicious cycles. Despite the high accuracies in Experiments 2 and 4 (92.32% and 100%), AUTO-SEE matched the results previously observed for DDoS attack prediction [8]. However, [8] performs the selection of features and models manually. AUTO-SEE automates this process, simplifying the utilization of the proposal.

AUTO-SEE surpassed the DDoS attack prediction literature. In Experiment 1, the DDoS attack prediction occurred 30 minutes and 38 seconds before the attack started, 25 minutes longer than the prediction of [10] and nine seconds longer than the prediction of [6]. In Experiment 2, AUTO-SEE predicted an attack 3 minutes and 56 seconds before the attack started, 7 seconds earlier than the best prediction of [5]. Furthermore, the work of [5] depends on labeled data and training, and the technique proposed in this work did not. The prediction time for Experiment 3 was 22 minutes and 5 seconds, 6 minutes and 44 seconds earlier than the prediction of [6]. Moreover, [6] utilized only three network traffic attributes and needed 28 minutes to identify the best deep learning architecture and to predict the DDoS. The work included feature selection and took only six seconds to identify and cluster normal and malicious time intervals. In Experiment 4, the prediction occurred 20 minutes after bot infection, exceeding the accuracy achieved in [7]. Finally, Table III shows that AUTO-SEE surpasses the evaluation metrics compared to [7], [8].

V. Conclusion

The best way to prevent damage from a DDoS attack is to contain it before it occurs. The literature presents solutions that utilize machine learning to consume network traffic features and detect attacks. The variety of machine learning models and the dependence on labeled data make DDoS attack prediction challenging. Moreover, the features traditionally used to detect attacks are not representative because attackers hide the attack preparation amid normal traffic. Using the proper features improves the DDoS attack prediction. However, identifying them without using labeled data is not trivial. The AUTO-SEE solves these problems. The technique generates new features by applying signal engineering over the network traffic and performs unsupervised feature selection to identify the most representative ones. The technique analyzes the most representative features to identify an unsupervised machine learning model that maximizes unknown DDoS attack prediction. Model selection does not depend on labeled data and presented results that evolve the literature. The results indicate that the AUTO-SEE technique reduced total errors by 44.15% and increased accuracy by 8.03% and 2.43%. The proposed technique identified other models qualified for predicting the attack with the same accuracy. This work will evaluate big data tools to reduce the eventual computational overhead and improve prediction time and accuracy. Furthermore, it will propose ways to identify the best number of clusters, evaluate other unsupervised machine learning models, and break the tie in choosing models.

References

[1] N. Jyoti and S. Behal, "A meta-evaluation of machine learning techniques for detection of DDoS attacks," in *INDIACom*. India: IEEE, 2021, pp. 522–526.

[2] E. Kiner and T. April, "Google mitigated the largest DDoS attack to date, peaking above 398 million rps Access 10/23," https://tinyurl.com/5xb2kux3, Google, LLC, 2023.

[3] S. Kivalov and I. Strelkovskaya, "Detection and prediction of DDoS cyber attacks using spline functions," in *TCSET*, UA, 2022, p. 4.

[4] P. Machaka, O. Ajayi, H. Maluleke, F. Kahenga, A. Bagula, and K. Kyamakya, "Modelling DDoS attacks in IoT networks using machine learning," *arXiv*, pp. 1–20, 2021.

[5] 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.

[6] 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, 2023, pp. 1–6.

[7] L. F. Borges, A. B. de Neira, L. Albano, and M. Nogueira, "Multifaceted DDoS attack prediction by multivariate time series and ordinal patterns," in *ICC Workshops*, 2024, pp. 427–432.

[8] A. B. de Neira, L. F. Borges, A. M. Araujo, and M. Nogueira, "Unsupervised feature engineering approach to predict DDoS attacks," in *GLOBECOM*, 2023, pp. 1644–1649.

[9] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the Mirai botnet," in *USENIX CSS*. USA: USENIX, 2017, p. 1093–1110.

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

[11] M. Feurer, A. Klein, K. Eggensperger, J. T. Springenberg, M. Blum, and F. Hutter, "Efficient and robust automated machine learning," in *NIPS*. USA: MIT Press, 2015, p. 2755–2763.

[12] J. Lam and R. Abbas, "Machine learning based anomaly detection for 5G networks," 2020.

[13] G. Poulakis, "Unsupervised AutoML: a study on automated machine learning in the context of clustering," Master's thesis, Πανεπιστήμιο Πειραιώς, 2020.

[14] M. Scheffer, *Critical Transitions in Nature and Society*. Princeton University Press, 2009.

[15] A. Muhammad, M. Asad, and A. R. Javed, "Robust early stage botnet detection using machine learning," in *ICCWS*, Pakistan, 2020, pp. 1–6.

[16] V. Dakos, S. R. Carpenter, W. A. Brock, A. M. Ellison, V. Guttal, A. R. Ives, S. Kéfi, V. Livina, D. A. Seekell, E. H. van Nes, and M. Scheffer, "Methods for detecting early warnings of critical transitions in time series illustrated using simulated ecological data," *PLOS ONE*, vol. 7, no. 7, pp. 1–20, 07 2012.

[17] E. Zivot and J. Wang, *Rolling Analysis of Time Series*. New York, NY: Springer New York, 2003, pp. 299–346.

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

[19] 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.

[20] M. Halkidi and M. Vazirgiannis, "A density-based cluster validity approach using multi-representatives," *Pattern Recognit. Lett.*, vol. 29, no. 6, pp. 773–786, 2008.

[21] V. Guttal and C. Jayaprakash, "Changing skewness: an early warning signal of regime shifts in ecosystems," *Ecology Letters*, vol. 11, no. 5, pp. 450–460, 2008.

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

[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.

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

Authorized licensed use limited to: Universidade Tecnologica Federal do Parana. Downloaded on July 14,2025 at 22:54:07 UTC from IEEE Xplore. Restrictions apply.