Unsupervised Feature Engineering Approach to Predict DDoS Attacks

Anderson B. de Neira*, Ligia F. Borges†, Alex M. Araujo*, Michele Nogueira*†
*Department of Informatics - Federal University of Paraná, Brazil
† Department of Computer Science - Federal University of Minas Gerais, Brazil
Emails: {abneira, amaraujo}@inf.ufpr.br, {ligiaborges, michele}@dcc.ufmg.br

***Abstract*—Predicting Distributed Denial of Service (DDoS) attacks is crucial given the large volume of generated attack traffic, particularly that generated by infected Internet of Things (IoT) devices. Attackers conceal their actions to delay detection as much as possible, increasing their damage when effectively launched. Hence, predicting signals of the attack plays a vital role in anticipating DDoS attacks and enhancing service protection. This work presents SEE, an unsupervised feature engineering approach to assist in predicting DDoS attacks. SEE evaluations encompass four experiments employing multiple datasets (CTU-13, CIC-DDoS2019, and IoT-23) and DDoS attacks. The approach predicts a DDoS attack 30 minutes before it effectively starts, reaching up to 100% accuracy.**

***Index Terms*—Zero-day attacks, IoT, Early Warning Signals.**

I. Introduction

The Internet of Things (IoT) is a trend worldwide with multiple applications in academia, society, and industry. However, the lack of standardization regarding the security of IoT devices makes them an easy target for attackers. Adversaries exploit vulnerabilities and abuse the low-security requirements to create massive attacks. An example is the Distributed Denial of Service (DDoS) attack, one of the most harmful existing cyber threats [1]. After the launch of a DDoS attack, thousands of committed IoT devices quickly consume the victims' resources, causing a denial of service and harming legitimate users. A recent investigation revealed that 6,797,959 DDoS attacks from 230 countries occurred in the second half of 2022 [2]. DDoS attacks reach a large volume of data at an unprecedented speed. In November 2022, a DDoS attack against a target in the USA reached 978.5 Gbps [2].

Previous research has highlighted the importance of curbing DDoS attacks before they start [3]–[5]. However, identifying evidence of attack preparation is challenging. Attackers avoid actions that impact network traffic features usually detected by traditional DDoS attack detection systems. The preparation phase produces negligible network traffic compared to attack traffic. The lack of attack-related information causes a significant imbalanced data, making it difficult to classify the attack preparation data from the regular network traffic. Thus, most DDoS attacks are only detected after the attack launch.

Identifying early warning signals – EWS (i.e., a group of signals used to anticipate a critical change in the system behavior) has the potential to predict future events [6]. In other areas, EWS has predicted new waves of COVID-19 [7] and anticipated population changes in some species [8]. The literature on using EWS to predict cyber threats is minimal. In [9], the authors proposed a distributed architecture that applies EWS to predict DDoS attacks. The solution predicts attacks 5 minutes and 41 seconds in advance. However, it predicts attacks using only one feature of the network traffic, which can be easily obfuscated by the attacker, affecting the prediction. Other works consider representative network features, but they follow a supervised approach, restricting their adoption in real networks [10].

This work proposes SEE, an un**S**upervised f**E**ature **E**ngineering approach to systematize the prediction of DDoS attacks. The SEE approach processes network traffic data and generates new features that give signals of DDoS attack preparation. SEE predicts DDoS attacks using the new features and unsupervised machine learning (ML). Unsupervised ML does not require labeled data, it is fast, and it contributes to zero-day attack prediction. SEE improves the applicability in real scenarios and presents a novel concept for explaining prediction based on data visualization.

Performance evaluations of the SEE approach follow four experiments. The experiments employed four datasets with different DDoS attack types. In the first two ones, SEE has predicted DDoS attacks on internal networks up to 30 minutes in advance, with an accuracy of 92.9%. In the third experiment, the approach predicted an Internet attack 15 minutes and 1 second before it effectively began. Finally, in the last experiment, the approach has identified a DDoS attack 20 minutes after the execution of malware in an IoT network with 100% accuracy. The results show that SEE increases the DDoS prediction time regarding the literature.

This paper is organized as follows. Section II introduces the literature on EWS and attack prediction. Section III describes the SEE approach. Section IV shows the results. Finally, Section V concludes the paper.

II. Related Works

In the literature, approaches employ EWS to predict future occurrences in different areas, such as weather forecasting. Takimoto (2009) [8] used the skewness, the standard deviation,

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 and 2022/06840-0, by the Coordination for the Improvement of Higher Education Personnel (CAPES), grants #88887.501287/2020-00 and #88887.509309/2020-00.

and the rate of return to predict changes in the species population. The author applied EWS to predict a sudden invasive population explosion that can pull native species toward extinction. Boers and Rypdal (2021) [11] evaluated EWS (variance the lag 1 autocorrelation – AC-1) to predict Greenland ice sheet melting. The literature on using EWS to predict DDoS attacks is recent and limited. In [4], the authors proposed a solution to predict DDoS attacks based on the network traffic extrapolating spline. Spline extrapolation predicted the peak of the traffic based on self-similar traffic. The solution used network traffic before, during, and after a DDoS attack to predict similar attacks. Although implementing the spline extrapolation method is simple, the solution only predicts DDoS attacks that correspond to the trained ones. Thus, the solution does not recognize other DDoS attacks and requires labeled data, which is impracticable in real scenarios.

Salemi *et al.* (2021) [12] predicted DDoS attacks using the Recurrent Neural Echo State Network (SCESN). The system analyzes the network traffic and projects the network traffic behavior for the subsequent few moments. Then, it uses the future traffic projection to predict the projection error using SCESN. The authors trained the SCESN using historical network traffic data. The solution predicted the attacks 20 seconds in advance in the DARPA 1998 dataset. However, using historical data for training limits the capability of the solution to predict different attacks than the trained ones.

The literature on cybersecurity focused mainly on predicting attacks using conventional network traffic features. An example is the solution proposed in [9], which employs only packet size as a feature to detect attacks. This is not an appropriate strategy because attackers hide their actions by generating the most minor traffic possible. Besides that, the works commonly employ labeled data to train solutions making the DDoS attack prediction unfeasible other than those trained, including the *zero-day* attacks. This work proposes a solution that applies a signal engineering approach to support the prediction of DDoS attacks by generating representative network traffic features without requiring labeled data.

III. Unsupervised Feature Engineering

This section describes the un**S**upervised f**E**ature **E**ngineering (SEE) approach to predict DDoS attacks. The SEE approach analyzes network traffic from the EWS perspective. It creates new features to identify changes in the network and anticipate possible attacks without depending on prior knowledge. This work fully differentiates from our previous one [10] because this one follows an unsupervised perspective, which fits better with the nature of DDoS attacks.

A. The EWS background

Dynamic systems and time series analysis are the EWS theory base. Systems can be in equilibrium; even if the system parameters vary, the system tends to compensate for this variation. Some systems transit from one equilibrium point to another as system parameters change. The new equilibrium presents similar or different aspects to those previously observed. Predicting changes helps their management [6].

A system transits smoothly, abruptly, or critically between equilibrium metastates faced with changes in the system parameters. In critical transitions, when the system parameters vary enough, the system overcomes the tipping point and moves on to the new behavior. In this case, the system does not follow a smooth transition. The transition from tipping points is called critical transition. During the critical transition, a system may experience instabilities where a DDoS attack has been launched. An important aspect of critical transitions is that even if the system parameters return to the previous level, the system may not return to the old equilibrium state, reaching a completely new equilibrium state. Thus, it is not trivial to recover systems from critical transitions [6].

There are methods to identify evidence that represents the occurrence of critical transitions. The evidence represents changes in values calculated on the observed data from statistical metrics before the critical transition. Variance, skewness, kurtosis, AC-1, and CV are statistical metrics to produce EWS [13], [14]. Statistical metrics are generic because they depend on common aspects of critical transitions to calculate EWS. Hence, EWS operates in different contexts. Thus, the proposed approach uses statistical metrics to predict DDoS attacks without prior knowledge.

Three statistical metrics (skewness, coefficient of variation, and kurtosis) were evaluated to provide a high level of ML model explainability. The first is **skewness**, which estimates data asymmetry in time series. Variations in asymmetry indicate a trustworthy early warning [13]. In Eq. 1, T represents the total amount of observed items. The term x_t indicates the observed and stored items in the time series. The μ refers to the simple arithmetic mean of the set, and s represents the standard deviation of the time series (Eq. 2).

$$Skewness = \frac{T\sum_{t=1}^{T}(x_t - \mu)^3}{(T-1)(T-2)s^3} \quad (1) \qquad s = \sqrt{\frac{\sum x - \mu^2}{(T-1)}} \quad (2)$$

This work uses the **coefficient of variation** (CV) as an EWS. The CV indicates the diversity of the mean of the analyzed datasets. The lower limit of CV ($CV = 0$) represents complete data uniformity [15]. Increases in CV can indicate the occurrence of a critical transition. Thus, the CV is an EWS [13]. CV formula divides the analyzed time series standard deviation (s) by the average of the time series (μ), where $\mu \neq$ [15].

The third EWS is **kurtosis**. The kurtosis value relates to the degree of flattening of the time series curve. The literature has identified that the kurtosis value varies or presents peaks near critical transitions [13]. Thus, data distribution can vary or show a peak pattern near a critical transition. These variations indicate changes in data distribution, anticipating critical transitions [13] and enabling DDoS attack prediction. In Eq. 3, the term T represents the total amount of items observed in a time series. The kurtosis calculation follows Eq. 4. The μ is the simple average of the entire time series. The x_t refers to each observed item in the time series with its index.

$$Kurt = \frac{(T-1)}{(T-2)(T-3)}(T-1)\hat{y}+6 \quad (3) \qquad \hat{y} = \frac{T\sum(x_t-\mu)^4}{[\sum(x_t-\mu)^2]^2} \quad (4)$$

B. The SEE approach description

SEE follows an unsupervised approach to predict DDoS attacks using EWS on network traffic data to create new features that evidence signals of the DDoS attack preparation. Fig. 1 presents the general functioning of the approach composed of four steps: collect network data, calculate early warning signals, predict DDoS attack, and visually present the results.

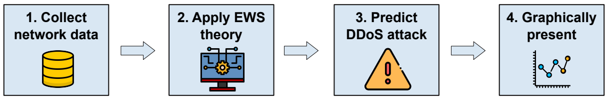


Fig. 1. Overview of the SEE approach

Step 1 defines the collection of network traffic. There are some ways to collect network traffic. In a centralized collection, the router forwards a copy of the packet header to a device executing the approach. Centralized processing requires many resources depending on the volume of data transferred. Thus, the network administrator can collect the network traffic in a distributed manner. Distributed processing, when possible, is desirable to avoid bottlenecks in data processing. The SEE approach is independent of the data collection mode (centralized or distributed). Therefore, the network administrator defines the collection mode based on the computational available resources.

The network administrator defines the network traffic features to collect. The imperative for the approach to operate is that the attack preparation impacts the network traffic features. Attackers perform pre-attack tests [3]. Thus, features such as the number of devices exchanging packets or the number of packets sent or received can change by preparing attacks. In [16], the authors present 40 representative attributes for detecting command and control (C&C) communication. As the C&C communication takes place before the attack, these attributes support the DDoS attack prediction.

The network traffic collected as features must maintain the order of the collection time. The administrator defines the collection time interval. A vector stores the collected network traffic in which each item (index) refers to the collection time interval. For example, the value present in each vector item represents the number of packets received per minute.

The SEE approach calculates the early warning signals to create new features when processing the network traffic collection (Step 2). For example, the approach calculates the kurtosis, skewness, and CV with the number of packets received per minute. Therefore, the SEE creates three new features (kurtosis, skewness, and CV) of the number of packets received and repeats this process for every newly collected data. The network administrator chooses which EWS the approach will apply to each feature. The approach simplifies the interpretation of results, reducing the number of features. This work applies the EWS using the fixed-size sliding window concept to avoid erroneous trends [14].

In Step 3, the K-means algorithm generates notifications of future attacks, using the new features to distinguish the preparation of DDoS attacks. K-means is an unsupervised ML algorithm that distributes the time intervals in a space with the exact dimensions as the new features. The algorithm defines K points that are the centers of the clusters. The value of K is two since the purpose is to separate the attack preparation signals from the regular traffic. The algorithm groups the intervals with the smallest Euclidean distance to each center, forming two groups. The algorithm calculates a new center using the average of all intervals belonging to each grouping. The K-means repeats this process until the centers do not change. K-means does not require labeled data to predict attacks, simplifying the SEE approach adoption in real network environments and enabling zero-day DDoS attack predictions.

Step 4 focuses on the explainability of the results. The approach graphically presents the results, improving their readability. The three-dimensional figures (e.g., Fig. 2(b)) show the network traffic evolving and forming new groups. The three dimensions refer to the new features generated by the approach. The three dimensions refer to the new features generated by the approach. The approach also allows displaying one or two dimensions, rotating the figure axes, and exhibiting numerical results.

IV. Performance Evaluation

This paper evaluates the proposal through four experiments using the datasets CTU-13 [17], CIC-DDoS2019 [18], and IoT-23 [19]. These datasets have labeled the start of DDoS attacks and the bots. The evaluation used the network traffic before the attack started. The evaluation verified the efficiency of the SEE approach in identifying evidence of attack preparation (i.e., before the attacker launches it). The datasets present some actions of attackers, such as bot infection and attack tests.

A. Experiments definition

Experiment 1 uses the traffic from a local network available in the capture 52 of [17]. The capture has 972 seconds, 555 MB, 6,336,398 packets, an Internet Control Message Protocol (ICMP) flood-type attack, and three bots. Researchers have conducted the attack on the second 778 of the capture and combined it with real data. **Experiment 2** applies local network traffic collected in capture 51 of [17]. The capture has 8803 seconds, 41 GB, 46,997,342 packets, ICMP and User Datagram Protocol flood-type attacks, and ten bots. The researchers launched the attacks on the second 5632 and combined the attacks with real data from a university.

Experiment 3 employs network traffic from the CIC-DDoS2019 dataset, with 19 attacks launched by researchers in two days. The dataset has 27 GB of data referring to attacks and real data, 61,407,883 packets. The bots connected to the victim through the Internet. The evaluation of the approach has focused on the first DDoS attack of the first day. The attack began at the 1484th second of the capture.

Experiment 4 employs the IoT-23 dataset, with 23 DDoS attack scenarios in IoT environments. Scenario 17 contains more than one infected and active bot. The scenario has 8.3 GB of data and 109,399,825 packets sent over 24 hours. Researchers started the capture at 06:43:20, and the malware execution was at 11:43:43 on the same day. Thus, the pre-infection traffic capture has legitimate traffic, and the post-infection traffic contains traces of the attack preparation. The documentation has presented an electrical problem at the university. Thus, this work did not identify the effective initiation of DDoS attacks. Therefore, this work hypothesizes that the lack of electricity compromised the attack launching.

The first feature employed in Experiments 1, 2, and 3 was the total number of sent packets, one of the most relevant features in [16]. This work has measured how many packets the network transmitted in each defined time interval to define this feature. The total of Internet Protocol (IP) addresses at the source and destination of the packets represent the other two features that measured how many unique addresses sent or received packets through the source or destination address fields of the packet to define these features. These features were selected because spoofing IP addresses and scanning vulnerable devices were common practices in DDoS attacks. Thus, the total of IP addresses, in sent or received packets, before the attack supports DDoS attack prediction, as the preparation of the attack causes variations on it. Experiment 4 used the largest packet size instead of the total of sent packets because the dataset used in this experiment (IoT-23) has different characteristics. This feature measures the size of the largest packet at each time interval.

Regarding Experiments 1, 2, and 3, the SEE approach has grouped the collected traffic considering one second as the time interval. For Experiment 4, the interval is one minute. Then, the extracted features from the network traffic at each time interval are stored in a dedicated vector. The discrepancy in time intervals for Experiments 1, 2, and 3, differing from Experiment 4, lies in the distinct characteristics of the datasets. For Experiments 1, 2, and 3, the amount of malicious traffic prior to the beginning of the attack would be inexpressive to perform the prediction if the time interval was considerable. More extensive time intervals can also compromise Experiment 1. The dataset used in Experiment 4 has 24 minutes of network traffic. Thus, analyzing minute by minute would make the result analysis more suitable.

The SEE approach execution comprises the estimation of the EWS kurtosis, skewness, and CV using a fixed-sized moving window over the time series of the features to simulate the real application. This work has calculated one EWS for each network traffic feature to improve the explainability of the results. Thus, Experiments 1, 2, and 3 have calculated kurtosis for the total of source IP addresses, skewness for the total of destination IP addresses, and CV for the total of packets. Experiment 4 used the kurtosis of the largest packet, skewness of total destination IPs, and CV total of source IPs. These configurations were made empirically.

The literature is not unanimous about the value of the sliding window size. For example, Bury *et al.* (2020) have used 40% of the dataset. Thus, the size of the sliding window still needs to be investigated. This work has used 5% of the dataset as window size for Experiments 1 and 3 and 10% for Experiments 2 and 4. These values have improved the prediction time of DDoS attacks, using data appropriately.

The evaluation metrics are accuracy, precision, and recall. It was necessary to measure the total number of true positives (TP) and true negatives (TN), the total number of false positives (FP) and false negatives (FN), and the total of observations (N) to calculate these metrics. Accuracy evaluated the system classifications (Eq. 5). However, there were few attack preparation signals because attackers hid their actions. Precision and recall complemented the evaluation. Precision showed the relationship between the observations labeled by the system for a specific type (positive or negative classes) and how many are of the assumed type (Eq. 6). The recall showed the relationship between all expected observations of the specific type and how many observations of that type the system classified correctly (Eq. 7). As the number of samples in the classes varies a lot due to the imbalance of DDoS attack, this work has used the average precision and recall weighted by the number of samples of each class.

$$A = \frac{TP + TN}{N} \quad (5) \qquad P = \frac{TP}{TP + FP} \quad (6) \qquad R = \frac{TP}{TP + FN} \quad (7)$$

B. Results

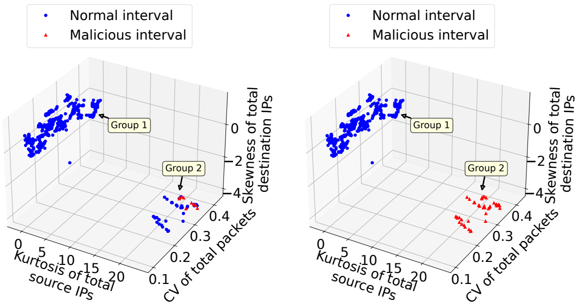
The result of applying the approach using capture 52 in the interval between the beginning of the capture and the second 542 is presented in Fig. 2(a). The SEE approach has identified changes in the behavior of EWS, which led to two groups in the data visualization. Group 1 has only normal time intervals, with no bots sending packets. Group 2 has 48 intervals, where 38 were normal and ten were malicious, where bots communicate. Group 2 began to form at the end of the boot process of bots. All results are available online[1].

The K-means applied to the results of the SEE approach (Fig. 2(b)) have identified two groups. Group 2 has the most recent intervals (near second 542). Considering Group 2 as malicious, the SEE approach has distinguished DDoS attack preparation signals, and K-means automate attack prediction. Considering the intervals of Group 1 as normal, the proposal correctly classified 447 intervals. Taking the intervals of Group 2 as malicious, the proposal correctly identified ten malicious intervals and incorrectly labeled 38 normal intervals. These results have indicated an accuracy of 92.3%, a weighted mean precision of 98.4%, and a weighted mean recall of 92.32%.

Fig. 3(a) presents the result of the SEE approach execution between seconds 3294 and 3794. Similarly to Experiment 1, the result shows two groups of intervals after the SEE approach execution. However, unlike Experiment 1, both groups have normal traffic intervals, where bots do not transmit data, and malicious intervals, where there is traffic from bots. This occurred because bots were more active near the attack started.

Fig. 3(b) shows K-means results considering the group with the most recent intervals as malicious. K-means clustering

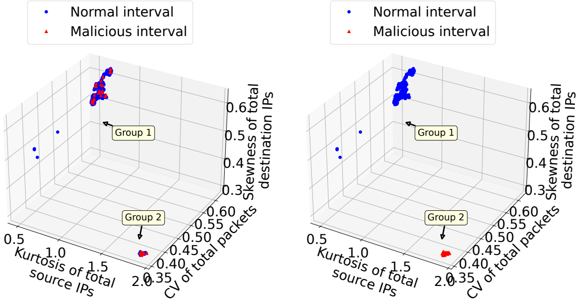
[1] https://github.com/andersonneira/globecom-2023-data



(a) Real labels (b) Proposal prediction

Fig. 2. DDoS attack Prediction in Experiment 1

results have corroborated the existence of two groups. Group 1 has 413 correctly identified normal intervals and 32 malicious intervals wrongly considered normal. Group 2 aggregated ten malicious intervals correctly identified as malicious and 45 intervals erroneously considered malicious. These results have indicated an accuracy of 84.6%, an average precision of 86.54%, and an average recall of 84.60%.

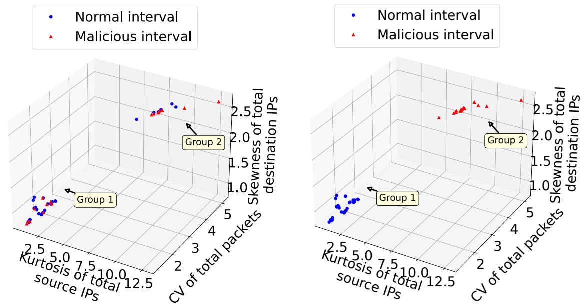


(a) Real labels (b) Proposal prediction

Fig. 3. DDoS attack Prediction in Experiment 2

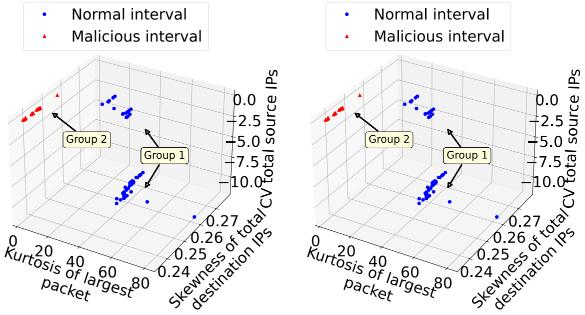
Experiment 3 applied the SEE approach in intervals captured in the dataset up to the second 159 (Fig. 4(a)). The same behavior as in previous experiments is observed. Two groups combine some normal and malicious intervals. Group 2 has a high concentration of malicious intervals and the most recent data (near second 159). The K-means applied to the results (Fig. 4(b)) of the SEE have reinforced the separation of the data. Results considering the most recent group as malicious presented an accuracy of 70.6%, a weighted average precision of 69.48%, and a weighted average recall of 70.69%.

Experiment 4 analyzed the SEE approach until minute 321 of the capture. The result of Fig. 5(a) refers to the 60 minutes before and 20 minutes after malware execution. The analysis used 20 minutes to reinforce that the proposed approach can quickly identify attack preparation signals, even considering a scenario with more normal traffic. The result of K-means has shown the existence of two groups. Group 1 has the oldest and just normal intervals. Group 2 has malicious and newest intervals (near minute 321). Remarkably, K-means have divided the two groups ideally. Thus, all metrics reach 100%. The solution predicted the DDoS attack 20 minutes after malware execution in an IoT network.



(a) Real labels (b) Proposal prediction

Fig. 4. DDoS attack Prediction in Experiment 3



(a) Real labels (b) Proposal prediction

Fig. 5. DDoS attack Prediction in Experiment 4

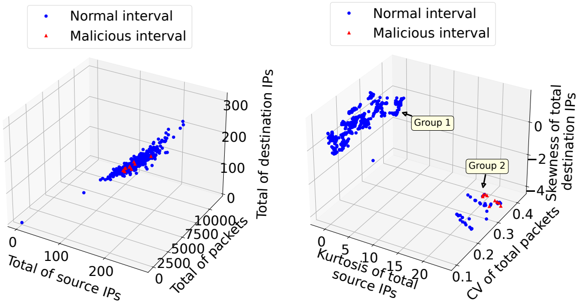
C. Discussion

In Experiment 1, the proposal predicted the DDoS attack 3 minutes and 56 seconds before the attack started. Thus, the SEE approach published a notification when identifying the formation of a new cluster with different characteristics from the previous cluster. This notification occurred 3 minutes and 56 seconds before the attackers launched their attacks. This result is relevant because the dataset has 16 minutes. The SEE approach obtained these results 15 seconds after the start of the infection. Experiment 2 also presented relevant results, as the proposal predicted the attack in a scenario with huge network traffic. The approach identified signals of attack preparation 30 minutes before its start and 19 minutes after infection.

Experiment 3 showed inferior results compared to the previous ones. However, the SEE approach identified the same behavior in all experiments. The results have indicated two interval groups, where one group was mainly composed of data intervals where the bots do not act. The other contained intervals with the bots acting. Even if the division of groups was not as accurate as in the others, the proposal predicted the DDoS attack 22 minutes before its launch.

Experiment 4 achieved 100% accuracy in predicting a DDoS attack. The high accuracy occurred because malware execution impacted network traffic. The new network traffic behavior induced changes in EWS, generating the new malicious cluster (Fig. 5). Although it was not possible to measure how long before the onset of the attack the prediction occurred, Experiment 4 was an excellent example of how important the prediction of the attack is. The prediction on the IoT dataset would occur just 20 minutes after the malware started. Therefore, the proposal has maximized the time to deal with DDoS attacks. Finally, the proposed approach obtained all results without prior attack knowledge and in scenarios with more normal data than malicious data. This made the proposed solution predict zero-day DDoS attacks in an unbalanced scenario.

The SEE approach results were compared to the original data. In Fig. 6(a), attackers have hidden their behavior in normal network traffic. Thus, K-means applied to the original data did not identify attack preparation. In comparison, the SEE approach has separated the set of intervals with bot-originated packets from most seconds without malicious traffic (Fig. 6(b)). Therefore, the new features created by the proposal provide the prediction of DDoS attacks. The same occurred in the other experiments. Thus, the results presented in this work demonstrate the distinction of the proposal.



(a) Data without the approach

(b) Data with the approach

Fig. 6. Comparison of the approach with the original data in Experiment 1

The SEE approach has evolved the literature in three ways. First, it has increased the prediction time. In [9], the prediction of the DDoS attack on CTU-13 capture 51 occurred 5 minutes and 41 seconds in advance, while the SEE approach predicted the attack 30 minutes earlier. The prediction time at [10] was 3 minutes and 22 seconds, while this work predicted the attack at 3 minutes and 56 seconds. Furthermore, the SEE approach achieved the results without supervised ML, unlike [10]. This simplifies the use of the proposal in real environments, enabling the prediction of zero-day DDoS attacks. Finally, the explainability of the results was a substantial evolution in the literature. The formations of new groups (graphically represented) indicate a different behavior than usual.

V. Conclusion

Detecting DDoS attacks is not enough to prevent damage caused by them. It is necessary to anticipate their signals to offer more response time to administrators to act against them. This work introduced SEE, an unsupervised approach to predict DDoS attacks. The SEE approach is composed of 4 steps. The first one defines the network traffic collection without using packet payload. Therefore, user privacy is preserved. The approach processes network traffic to create new features using early warning signals (EWS). The approach uses the new features allied with unsupervised ML to identify DDoS attacks preparation and predict them. The SEE approach presents the results graphically. The performance evaluation comprises four experiments, considering IoT, local networks, and access networks that connect the victim and the attackers. The results showed that the SEE approach predicts attacks up to 30 minutes before the attack effectively starts, with a maximum accuracy of 100%. The solution creates new representative features to distinguish normal from attack preparation traffic. The prediction occurred when the unsupervised ML clustered the data and attested the existence of two different groups. Future works will focus on testing other unsupervised ML algorithms, automatic feature engineering and selection, and evaluating the prediction quality using cohesion, separation, and silhouette coefficient metrics.

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] Netscout, "Findings from 2nd half 2022. [(accessed: April 2023)]," Netscout, 2023. [Online]. Available: www.netscout.com/threatreport/global-highlights

[3] A. N. Jaber, M. F. Zolkipli, M. A. Majid, and S. Anwar, "Methods for preventing distributed denial of service attacks in cloud computing," *ASL*, vol. 23, no. 6, pp. 5282–5285, 2017.

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

[5] A. A. Santos, M. Nogueira, and J. M. F. Moura, "A stochastic adaptive model to explore mobile botnet dynamics," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 753–756, 2017.

[6] M. Scheffer, *Critical Transitions in Nature and Society*. PUP, 2009.

[7] D. Proverbio, F. Kemp, S. Magni, and J. Gonçalves, "Performance of early warning signals for disease re-emergence: A case study on COVID-19 data," *PLOS C B*, vol. 18, no. 3, p. e1009958, 2022.

[8] G. Takimoto, "Early warning signals of demographic regime shifts in invading populations," *PE*, vol. 51, no. 3, pp. 419–426, 2009.

[9] B. Rahal, A. Santos, and M. Nogueira, "A distributed architecture for DDoS prediction and bot detection," *IEEE Acce.*, vol. 8, pp. 1–17, 2020.

[10] 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.

[11] N. Boers and M. Rypdal, "Critical slowing down suggests that the western Greenland Ice Sheet is close to a tipping point," *PNAS*, vol. 118, no. 21, 2021.

[12] H. Salemi, H. Rostami, S. Talatian-Azad, and M. R. Khosravi, "Leaesn: Predicting DDoS attack in healthcare systems based on lyapunov exponent analysis and echo state neural networks," *MTA*, vol. -, no. -, pp. 1–22, 2021.

[13] 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.

[14] T. M. Bury, C. T. Bauch, and M. Anand, "Detecting and distinguishing tipping points using spectral early warning signals," *J. R. Soc.*, vol. 17, no. 170, 2020.

[15] A. G. Bedeian and K. W. Mossholder, "On the use of the coefficient of variation as a measure of diversity," *ORM*, vol. 3, no. 3, p. 13, 2000.

[16] Y. Feng, H. Akiyama, L. Lu, and K. Sakurai, "Feature selection for machine learning-based early detection of distributed cyber attacks," in *DASC*. Greece: IEEE, 2018, pp. 173–180.

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

[18] 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.

[19] S. Garcia, A. Parmisano, and M. J. Erquiaga, "IoT-23: A labeled dataset with malicious and benign IoT network traffic [(accessed: April 2023)]," Zenodo, 2020. [Online]. Available: https://zenodo.org/record/4743746