Survey of Research Literature for *Impact of class distribution on the detection of slow HTTP DoS attacks using Big Data*

Richard Bosso

I. Introduction

THIS survey is a comprehensive research literature overview of the main issues, techniques, shortcomings, and possible recommended future work for the baseline paper *Impact of class distribution on the detection of slow HTTP DoS attacks using Big Data*, so the content that proceeds from here will be focused on covering the specific domain application and theory that is relevant to the main concerns of this baseline paper [1]. As such, due to the fact that the baseline paper [1] makes what seems to be a unique contribution to this particular domain, there will be several times where the baseline paper will be referenced in this report for the purposes of constructing a full understanding of the unique insights that will be addressed.

II. Background and Challenges

Ever since one of the earliest documented instances of a large-scale Denial of Service (DoS) attack, which took place in 1999 and caused the school computer network of the University of Minnesota to become largely inaccessible for several days, DoS attacks have been well known for their disruptive and damaging capabilities [2]. Slow HTTP DoS attacks, one of many types of DoS attacks, can create problems by overwhelming website applications, which can jeopardize or limit the ability for a website application to deliver whatever service it normally provides to actual users, and many DoS attackers who disrupt such services may sometimes have financial or political motivations in mind [3].

Even though DoS attacks are generally inexpensive for malicious agents that exploit web sources using them, which is part of the reason why they are so prevalent, there have been several occurrences in recent history of DoS attacks either shutting down or negatively impacting the performance of systems that support telecommunications, transportation, public services, and other critical infrastructure [4]. Slow HTTP Denial of Service attacks are uniquely problematic in that they are an example of DoS attack that exploits the HTTP protocol that functions on the application layer of internet-based services [5]. Many different types of application layer DoS attacks have been classified, and they are distinct from more traditional forms of DoS attacks with regard to how the attacks may lead to a meltdown in internet services being provided [6]. Whereas more primitive forms of DoS attacks generally work by trying to overwhelm the bandwidth that is available on the network level [7], application layer DoS attacks can sometimes be more severe than traditional DoS attacks due to their tendency to require a much smaller amount of resources to be consumed, a more narrowed focus on overwhelming only specific parts of an application that are being threatened, and a much higher probability for such DoS attacks to remain undetected [6]. Compared to other types of application layer DoS attacks, one survey recorded by Arbor Networks found that HTTP DoS attacks are among the most common types of application layer DoS attacks, as shown in Figure 1 [8], and a report released by The Cloudflare Blog claims that the amount of quarterly traffic for HTTP DDoS attacks saw an increase of 65% between the second and third quarters of 2023, from roughly 5.4 trillion attack requests in Q2 to roughly 8.9 trillion in Q3 [9].

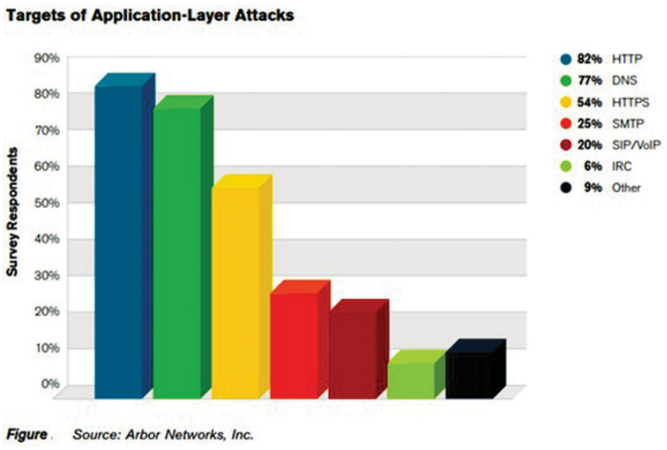

Fig. 1: Most Frequent Types of Application Layer Attacks [8]

Looking at the different varieties of Slow HTTP DoS attacks discussed in the baseline paper [1], the main types focused on were the Slowloris and Slow POST attack types, the algorithms of which are shown in Figure 2 [1]. Slowloris and Slow POST are both often classified as slow-rate attacks, and both of their attack algorithms generally exploit how servers typically handle timeouts when processing and responding to HTTP requests [6]. In comparison with other established methods used for DoS attacks, slow-rate attacks can often be more difficult to differentiate from normal traffic [10], [11], and this difficulty in identifying slow-rate DoS attacks generally means that attempting to mitigate or prevent slow-rate DoS attacks can be equally difficult [12].

Algorithm 1 Slowloris Connection

```
procedure SLOWLORIS
    for i = 1 to number of connections do
        CONNECT(hostName)
        SEND(GETRequest)
    while Server requests communication do
        header ← random header value
        SEND(header)
```

Algorithm 2 POST Connection

```
procedure POST
    for i = 1 to number of connections do
        CONNECT(hostName)
        CONNECT(identifyPOSTvariable)
        SEND(POSTRequest)
    while content-length header value is not met do
        header ← partial value
        SEND(header)
```

Fig. 2: Algorithms for Slowloris and Slow POST Attacks [1]

One way to identify instances of DoS attacks is to analyze patterns in website interactions, such that slow HTTP DoS attacks can be mitigated or blocked altogether, but this can sometimes prove challenging to implement effectively for many reasons. [13]. There has been interest in using supervised machine learning models for the purpose of predicting instances of DoS attacks, but one of the main problems with this approach is that DoS attacks of any kind are relatively rare events [1]. This often means that labeled DoS attack datasets can be highly imbalanced, which can cause weaker performance for machine learning models [14]. Though the standard definition of class imbalance refers to any dataset where two or more classes don't share equal or similar distributions given the number of instances that constitute the available data being represented, the distinction for whether or not a dataset is highly imbalanced can be defined differently based on whatever ratio of class imbalance may start to introduce unwanted bias into a classification model [15].

III. Current Approaches with Highly Imbalanced DoS Attack Data

To address the problem of significant imbalance impacting the ability for machine learning models to generate accurate predictions for highly imbalanced DoS attack datasets, there have been several proposed methods highlighted in recent literature for this particular domain application. For imbalanced data in general, though it is common for highly-imbalanced data to negatively impact the performance of classification models due to the significant bias towards the majority class that often results from class imbalance, there are a number of different methods that can be used with imbalanced data to help strengthen the performance of whatever classification model is trained with such data [15].

One method for applying supervised models to highly imbalanced DoS datasets, described in the baseline paper for this course project, involved the use of Random Undersampling (RUS) to effectively re-balance the ratio between the majority and minority classes by sampling less of the majority class, with which several different combinations of classification models and sampling ratios were tested [1]. The dataset used for the baseline paper, which contains around 1.89 million samples of data in total and is populated by only a few thousand labeled DoS attacks, can be considered a highly imbalanced dataset since the minority class of slow-rate DoS attacks populates less than 0.01% of the entire dataset [1].

Sample re-balancing methods that change the distribution and numbers of data points for each class, such as the RUS method used by the baseline paper [1], are among the most common methods used when trying to train classification models with heavily imbalanced data [15], and this seems to apply to some other research work which is relevant to this particular domain [16], [17], [18], [19], [20]. At the time when the baseline paper was published, which was in 2019, the authors noted a general lack of published research with regard to the topic of detecting DoS attacks or other related security problems within imbalanced datasets [1], so it is worth noting that some of the papers relevant to this exact problem which will be described here were published after our baseline paper [17], [18], [20]. Regardless of the date of publication, however, they seem to be relevant to the problem to the best of the author's knowledge, and deserve mention here for the purpose of determining the state of insight which this present direction of research can currently provide.

Aside from the RUS methodology described by the baseline paper, some other relevant research is noted there [1], with a paper by Roy et al. [16] being considered one of the more relevant works in the imbalanced DoS data detection domain that the baseline paper was specifically addressing [1]. Published in 2015, though this paper by Roy et al. addresses malware detections for Android OS applications rather than with DoS attack detection specifically [16], the baseline paper nevertheless seems accurate in its appraisal of the Android malware detection data as an imbalanced dataset [16], [1]. The baseline paper does seem to generally find some of the findings from Roy et al. to be useful and worthy of consideration for their specific investigations, particularly noting how Roy et al. addresses how classification performance for machine learning models typically declines as the ratio of sample numbers between 2 classes in a dataset becomes more imbalanced [16], [1]. However, there are some noteworthy differences between the methodologies described in each paper, not the least of which being that Roy et al. measured test model performance with different class ratios, even though RUS was not used to derive these differing ratios in the same way as was done in the baseline paper [16], [1]. Additionally, unlike in the baseline paper, the dataset used is not extremely imbalanced like the one used for the baseline paper, and only the k-Nearest Neighbors classification (kNN) model [21] was tested with these different ratios (rather than with multiple different models, as was investigated by the baseline paper) [16], [1].

Though sampling methods such as RUS and random oversampling (ROS) were addressed by other works of research cited in the baseline paper, which were mostly relevant to

imbalanced data, these generally did not seem to focus on the specific domain of DoS attacks [1]. Beyond related works addressed by the baseline paper [1], there do seem to be other research applied to this domain that seem to be worth mentioning as current approaches to imbalanced DoS attack datasets [17], [18], [19], [20]. To the best of the author's knowledge, the baseline paper does seem to be unique among much of the DoS attack detection research for using binary classification models with such an extremely imbalanced 0.01% minority class, but other notable differences in these research works might point to new directions for inquiry [1], [17], [18], [19], [20].

Whereas the baseline paper processed the collection of real web traffic data from a college campus network by using Slowloris.py [22] and OWASP Switchblade 4.0 [23] to generate DoS attacks under different network conditions [1], Cieslak et al. [19] processed web traffic data from the campus network of the University of Notre Dame using the SNORT intrusion detection system [24] to label any instances of intrusion (such as DoS attacks), resulting in the Packets and Destinations datasets. Between these two datasets, the Destinations dataset was the most imbalanced dataset in that paper, containing 2106 instances labeled as intrusions and 344,514 instances of normal traffic, such that the minority class made up roughly 0.6% of the entire Notre Dame dataset [19]. Using Repeated Incremental Pruning to Produce Error Reduction (RIPPER) [25] as the classification model, each of the RUS, ROS, Synthetic Minority Over-sampling Technique (SMOTE) [26], and cluster - SMOTE sampling methods were each used to re-balance the class ratios observed with the Notre Dame network intrusion data, with Receiver Operating Characteristic (ROC) Curves [27] being used to evaluate the performance of each of these sampling methods when used with RIPPER [19]. Based on the visualizations of each ROC curve for each sampling method and dataset, Cieslak et al. [19] concluded that SMOTE seemed to have the most optimal performance when used with RIPPER for imbalanced network intrusion data. Interestingly, whereas the baseline paper [1] tested a single sampling method (RUS) with multiple different types of classification models, Cieslak et al. [19] seemed to test a single classification model with multiple different types of sampling methods.

After surveying several different datasets to consider for training and testing an ML-based intrusion detection system, Karatas et al. [17] ultimately used the CSE-CIC-IDS2018 dataset [28] to build several different models using distinct algorithms, including Decision Tree (DT) [29], Random Forest (RF) [30], kNN [21], AdaBoost [31], Gradient Boosting (GB) [31], [32], and Linear Discriminant Analysis (LDA) [33], [34]. The rationale for selecting this dataset (CSE-CIC-IDS2018 is a highly imbalanced and multi-class labeled intrusion traffic dataset [28]), was based on the fact that Karatas et al. noted it to be one of the more recently developed intrusion datasets, which the authors suggested might make it more relevant and ideal for ML-based intrusion detection to generate predictions with modern-day internet traffic [17]. SMOTE [26] was used to adjust the class imbalance for the CSE-CIC-IDS2018 dataset, and for each of the classes of labeled traffic predicted for (Benign (normal traffic), Bot, DoS, Brute Force, Infiltration, and SQL Injection) the use of SMOTE generally saw increases in classification accuracy for each class across all models implemented [17]. Using several different metrics to evaluate the performance measured from each of these models (classification accuracy, precision and recall [35], F1-Measure [36], and training time), AdaBoost and DT using data re-balanced by SMOTE were found to have the best classification performances overall, with DT having one of the quickest training times compared to the other models [17]. Accuracy rates for each class, alongside average accuracy, are shown in Figure 4. As can be seen in Figure 3, out of 4,525,399 total instances in the CSE-CIC-IDS2018 dataset, there were only 53 instances of SQL Injection attacks, making this particular class extremely imbalanced enough to occupy only 0.001 % of the entire dataset [17].

Class Label	Number	Volume (%)
Benign	2,856,035	63.111
Bot	286,191	6.324
Brute Force	513	0.011
DoS	1,289,544	28.497
Infiltration	93,063	2.056
SQL injection	53	0.001
Total	4,525,399	100

Fig. 3: CSE-CIC-IDS2018 Class Distribution [17]

	Accuracy with Sampled Data (%)						
Model	Benign	Bot	DoS	Brute Force	Infilt.	Sql Inj.	Avg. Acc.
ADA	99.56	99.99	99.99	99.99	96.37	100	99.32
DT	99.55	99.99	100	99.99	95.60	96.23	98.56
RF	99.53	99.97	99.99	99.99	92.63	99.99	99.19
KNN	98.07	99.97	99.98	99.85	73.91	100	95.30
GB	98.89	99.96	99.99	99.62	97.83	100	99.38
LDA	86.32	98.40	99.88	51.83	97.82	67.43	83.62

Fig. 4: CSE-CIC-IDS2018 Class Prediction Accuracy Rates for Data Sampled with SMOTE [26], [17]

The CSE-CIC-IDS2018 dataset [28] and the NSL-KDD dataset [37] were the imbalanced network intrusion dataset benchmarks used by Liu et al. [18]. There are several unique contributions that are relevant to the imbalanced DoS attack dataset domain which are made by Liu et al. [18], and the contributions encompass both the choice of classification models and the sampling methods used. Alongside the several sampling methods that are tested, including RUS, ROS, and SMOTE [26], Liu et al. also proposes a novel sampling method called the Difficult Set Sampling Technique (DSSTE) to re-balance the class ratios in the training data, in a way that Liu et al. suggests may help reflect the natural distribution present in the minority class more accurately [18]. In addition to using several machine learning models like Random Forest (RF) [30], Support Vector Machine (SVM) [38], and XGBoost [39] to generate predictions for these imbalanced network intrusion datasets, Liu et al. [18] also tested several different deep

learning models [40], including Long Short Term Memory (LSTM) [41], AlexNet [42], and Mini-VGGNet [43], [44]. Using classification accuracy, precision, recall [35], and F1-Measure [36] to evaluate the performance of each combination of sampling method and classification model, Liu et al. found that their DSSTE sampling method seemed to outperform every other method on average, and when paired with DSSTE the strongest performing models seemed to be miniVGGNet, AlexNet, and Random Forest [18].

Looking at the work done by Can et al. [20], which used CIC-DDoS 2019 [45] (an imbalanced dataset which consists of multiple different classes of application layer DDoS attacks) for training and testing data, they proposed a deep learning model called DDoSNet, and the overall structure for DDoSNet is shown in Figure 5. With the first layer designed to be a neural network [46] which is used as a feature selection method (which attempts to derive the most significant features from the input data [47]), the second layer of DDoSNet is a fully-connected Multilayer Perceptron (MLP) [48], and when Can et al. compared the performance of DDoSNet with several other classification models it seemed to have the best performance based on different performance metrics [20]. Considering that this work by Can et al. seems unique in this domain for proposing a deep learning model structure specifically for DDoS network detection, it may also be a unique example of how a feature selection methodology might be helpful for the performance of a classification model when using imbalanced data [20].

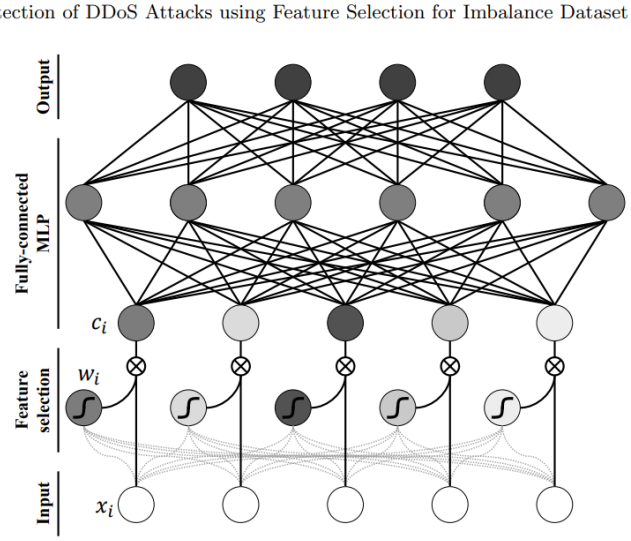

Fig. 5: Basic Structure of Proposed DDoSNet Model [20]

IV. A Critique of Current Approaches

When evaluating the performance of different classification models for highly imbalanced data, a comprehensive understanding of model performance requires a variety of reliable performance evaluation metrics, because merely using classification accuracy for such purposes can be highly misleading for imbalanced data [15]. Since the AUC performance metric can also be misleading if data is highly skewed [49], the fact that different performance metrics can come to different conclusions about model performance for different sampling methods makes the inclusion of different performance metrics even more important when working with imbalanced data [50]. Looking at the performance metrics used by some of the research literature which all focus on imbalanced DoS/network intrusion datasets [1], [17], [18], [19], [20], as discussed in the previous section, though most of these papers primarily used some or all of the metrics for Accuracy, AUC, Recall, Precision, and/or F-Measure, all of these metrics are potentially prone to misuse if their assumptions and biases aren't properly understood [35]. Despite the possible risk of misuse and misunderstandings resulting from the potential limitations inherent to the choice of performance metrics, especially given that sampling methods with imbalanced data are being incorporated with each of these models, almost none of these research papers cited in this survey seem to have made use of other performance metrics such as Kolmogorov-Smirnov Test [51], Geometric Mean [52], or others. One notable exception is a machine learning approach to a DoS attack detection system published by Mihoub et al. [53], where evaluations from Cohen's kappa [54] are included among the performance metrics used in that paper. Otherwise, to the best of the author's knowledge, the use of other performance metrics outside of Accuracy, AUC, Recall, Precision, and F-Measure currently seem relatively sparse in the network intrusion detection domain of research.

Though it is true that the baseline paper [1] tested the effectiveness of multiple different classification models with a highly imbalanced slow HTTP DoS Attack dataset, applying models such as Naive Bayes [55], [56], Multilayer Perceptron [48], Random Forest [30], Support Vector Machine [38], k-Nearest Neighbors (kNN) [21], C4.5 Decision Tree [57], RIPPER [25], and Logistic Regression [58] to a level of class imbalance that seems to be uniquely extreme when compared to most other examples in this particular domain application, the lack of deep learning models used here is worth addressing. Though some of the papers discussed in this survey do include deep learning models in their arsenal of model testing for this domain of research [53], [20], [18], the inclusion of deep learning models for the network intrusion domain is not unanimous in the present literature [1], [17], [19], [16], and nearly all of the papers in the network intrusion domain (to the best of the author's knowledge) that do incorporate deep learning models generally seem to be papers that were published between 2020 and the present day [53], [20], [18]. Despite the massive interest that deep learning models have attracted in recent years, extensive surveys have shown a lack of emphasis on analyzing how deep learning models perform with imbalanced data in general [59]. As such, this may suggest that deep learning models should have more consistent inclusion within the domain of network intrusion detection, given how network attack traffic data is often highly imbalanced data [1], [28], [45], [37].

Though there were some papers in this domain that did record the time taken for each model to complete all required steps for training and testing [17], [53], [60], there were other papers that chose not to record training times [16], [18],

[19], [20]. Different machine learning models can sometimes have very different run-times from other models given the same hardware [17], so similarly performing models can not always be assumed to have similar run-times. For any practitioner in the field of network intrusion detection who wishes to determine the best potential models to use with large amounts of network traffic data, the computational efficiency of different models might be useful information to have for the purpose of keeping servicing costs as low as possible [61].

Liu et al. [18] and Cieslak et al. [19] were the only authors in this whole survey who each tested multiple different sampling methods in each of their papers [1], [16], [17], [53], [60]. Liu et al. were especially unique for having included their own novel sampling method called DSSTE with the other sampling methods [18]. Even the analysis of multiple sampling methods by Cieslak et al.[19], however, was limited by having only a single classification model to test with each sampling method. When experimentally testing for optimal combinations of sampling methods with classification models, though it is common for any sampling method to cause some improvement in classification performance, it is possible for different classification models to have optimal sampling methods that are also different from one another [50], so it is often more descriptive to test several sampling methods for different model conditions since any single sampling method is not always going to be the best method to use [15]. By this logic, some of the current research for this domain may be limited by a lack of comprehensiveness when testing sampling methods, as may be indicated by some papers that focus on only one sampling method in their testing procedures [1], [16], [17], [53], [60].

Beyond the domain context of using supervised learning models to generate predictions for imbalanced DoS attack and network intrusion datasets [1], some brief mention should be made of unsupervised learning methods [62], which refers to any classification models that don't make use of prescribed class labeling during model training. The main motivation for applying unsupervised learning methods to the problem of network intrusion detection has largely to do with the practical limitations of designing network intrusion detection to recognize only previously known types of network attacks, since this can run the risk of having supervised learning models that are incapable of detecting new kinds of network attacks, given overall network traffic that is also changing as time passes [63], [64]. In theory, a network intrusion system based on reliable unsupervised learning would be capable of screening out newer, previously unknown types of DoS attacks, given real-time network traffic that is also constantly changing [65]. Though there has been some research on the topic of applying unsupervised learning models for anomaly detection using imbalanced network intrusion data, the current coverage on this topic seems limited compared to supervised learning models, and problems with unsupervised classification accuracy have been noted with regard to high false positive rates [66], [65], [64].

V. Conclusion

There has been significant interest in developing network intrusion detection systems that can catch instances of intrusive network traffic, especially for difficult to detect network attacks such as Slow HTTP DoS attacks. Machine learning models are one possible methodology to consider for implementing network intrusion detection systems, but the relatively extreme rarity of network attacks means that a lot of real-world network traffic will generally have to be labeled as extremely imbalanced data. In general, data with extreme class imbalance can degrade the performance of machine learning models due to majority class bias, and network traffic is no exception to this general problem.

For this literature overview, we have examined many of the current techniques used to improve the classification performance of machine learning models used with highly imbalanced network intrusion data. Sampling methods, which are used to change the ratio of classes present in a sample of data, are shown to be a common supplement to classification models working with network intrusion data, and in nearly all instances sampling methods like RUS, ROS, SMOTE, and even the novel method DSSTE proposed by Liu et al. [18] have all been shown to improve the performance of classification models that generate predictions for network intrusion data (regardless of whether the network intrusion data is generated by the researchers themselves using network attacks experimentally injected into normal traffic using programmed scripts, or based on publicly available network traffic datasets).

Using highly imbalanced network intrusion data, a wide range of commonly used machine learning models were tested for their classification performance. Across the different research works surveyed, promising classification performance was noted with several different traditional machine learning models and deep learning models. The novel DDoSNet, designed by Can et al. [20] specifically for DDoS attack detection when given imbalanced DDoS network attack data, showed what seemed to be stronger performance compared to the other models tested by them, which was partially attributed to the use of a feature selection layer built into the design of the model.

Partly based on criticisms given for the more pressing limitations of these current approaches to network intrusion data, several recommendations can be made for future work. These methods should be applied to as many other network intrusion datasets as possible, perhaps with a variety of different levels of class imbalance, and the number of different machine learning models tested should be expanded to include deep learning models that have yet to be considered in the current research surrounding network intrusion detection. To develop a clearer idea of how these different models can actually perform given different datasets, future works should investigate how multiple different sampling methods may perform with an array of different classification models, and a larger range of different performance metrics should be calculated for future work to develop a more comprehensive understanding of how these models perform given highly imbalanced data. For any researchers who are interested to take training time into

account, particularly when considering how models may be applied to large amounts of real traffic data, it might be ideal for future works to also record training times for different classification models given different sampling methods and datasets. Similar to how DDoSNet [20] and DSSTE [18] were novel methods proposed for the specific application of working with heavily imbalanced DDoS attack/network intrusion data, future work should also develop more comparative testing regiments that also include any methods that are either novel or recently developed by other works. Additionally, given that Can et al. found the performance of DDoSNet to be significantly improved when feature selection was incorporated into the model design [20], this might lend some justification for future works to also consider investigating how different feature selection methods might also help influence the overall performance of models working with network intrusion data.

For any researchers who may also want to consider investigating how unsupervised models might perform given imbalanced network intrusion data, incorporating unsupervised models into studies that also examine the performance of supervised models might also prove interesting for developing new methodologies which might prove useful for network intrusion detection.

REFERENCES

[1] C. L. Calvert and T. M. Khoshgoftaar, "Impact of class distribution on the detection of slow http dos attacks using big data," *Journal of Big Data*, vol. 6, no. 1, pp. 1–18, 2019.

[2] "Radware's ddos handbook: The ultimate guide to everything you need to know about ddos attacks," https://www.radware.com/ddoshandbook-lpc-6442456170/, 2015.

[3] C. Wueest, "The continued rise of ddos attacks," *White Paper: Security Response, Symantec Corporation*, 2014.

[4] R. Sommese, K. Claffy, R. van Rijswijk-Deij, A. Chattopadhyay, A. Dainotti, A. Sperotto, and M. Jonker, "Investigating the impact of ddos attacks on dns infrastructure," in *Proceedings of the 22nd ACM Internet Measurement Conference*, 2022, pp. 51–64.

[5] V. Durcekova, L. Schwartz, and N. Shahmehri, "Sophisticated denial of service attacks aimed at application layer," in *2012 ELEKTRO*. IEEE, 2012, pp. 55–60.

[6] G. Mantas, N. Stakhanova, H. Gonzalez, H. H. Jazi, and A. A. Ghorbani, "Application-layer denial of service attacks: taxonomy and survey," *International Journal of Information and Computer Security*, vol. 7, no. 2-4, pp. 216–239, 2015.

[7] S. Ranjan, R. Swaminathan, M. Uysal, and E. W. Knightly, "Ddos-resilient scheduling to counter application layer attacks under imperfect detection." in *INFOCOM*. Citeseer, 2006, pp. 1–14.

[8] G. Kumar, "Denial of service attacks–an updated perspective," *Systems science & control engineering*, vol. 4, no. 1, pp. 285–294, 2016.

[9] J. P. Omer Yoachimik, "Ddos threat report for 2023 q3," 2023.

[10] A. Kuzmanovic and E. W. Knightly, "Low-rate tcp-targeted denial of service attacks: the shrew vs. the mice and elephants," in *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, 2003, pp. 75–86.

[11] O. Yevsieieva and S. M. Helalat, "Analysis of the impact of the slow http dos and ddos attacks on the cloud environment," in *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*. IEEE, 2017, pp. 519–523.

[12] J. A. Perez-Diaz, I. A. Valdovinos, K.-K. R. Choo, and D. Zhu, "A flexible sdn-based architecture for identifying and mitigating low-rate ddos attacks using machine learning," *IEEE Access*, vol. 8, pp. 155 859–155 872, 2020.

[13] N. Agrawal and S. Tapaswi, "Defense mechanisms against ddos attacks in a cloud computing environment: State-of-the-art and research challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3769–3795, 2019.

[14] T. Hasanin, T. M. Khoshgoftaar, J. L. Leevy, and R. A. Bauder, "Investigating class rarity in big data," *Journal of Big Data*, vol. 7, no. 1, pp. 1–17, 2020.

[15] J. L. Leevy, T. M. Khoshgoftaar, R. A. Bauder, and N. Seliya, "A survey on addressing high-class imbalance in big data," *Journal of Big Data*, vol. 5, no. 1, pp. 1–30, 2018.

[16] S. Roy, J. DeLoach, Y. Li, N. Herndon, D. Caragea, X. Ou, V. P. Ranganath, H. Li, and N. Guevara, "Experimental study with real-world data for android app security analysis using machine learning," in *Proceedings of the 31st Annual Computer Security Applications Conference*, 2015, pp. 81–90.

[17] G. Karatas, O. Demir, and O. K. Sahingoz, "Increasing the performance of machine learning-based idss on an imbalanced and up-to-date dataset," *IEEE access*, vol. 8, pp. 32 150–32 162, 2020.

[18] L. Liu, P. Wang, J. Lin, and L. Liu, "Intrusion detection of imbalanced network traffic based on machine learning and deep learning," *Ieee Access*, vol. 9, pp. 7550–7563, 2020.

[19] D. A. Cieslak, N. V. Chawla, and A. Striegel, "Combating imbalance in network intrusion datasets." in *GrC*, 2006, pp. 732–737.

[20] D.-C. Can, H.-Q. Le, and Q.-T. Ha, "Detection of distributed denial of service attacks using automatic feature selection with enhancement for imbalance dataset," in *Intelligent Information and Database Systems: 13th Asian Conference, ACIIDS 2021, Phuket, Thailand, April 7–10, 2021, Proceedings 13*. Springer, 2021, pp. 386–398.

[21] E. Fix and J. L. Hodges, "Discriminatory analysis: Nonparametric discrimination: Small sample performance," 1952.

[22] G. Yaltirakli, "Slowloris," *github.com*, 2015. [Online]. Available: https://github.com/gkbrk/slowloris

[23] "OWASP Switchblade." [Online]. Available: https://www.owasp.org/

[24] Sourcefire, *Snort Users Manual: The Snort Project*, 2005.

[25] W. W. Cohen, "Fast effective rule induction," in *Machine learning proceedings 1995*. Elsevier, 1995, pp. 115–123.

[26] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, "Smote: synthetic minority over-sampling technique," *Journal of artificial intelligence research*, vol. 16, pp. 321–357, 2002.

[27] J. A. Hanley and B. J. McNeil, "The meaning and use of the area under a receiver operating characteristic (roc) curve." *Radiology*, vol. 143, no. 1, pp. 29–36, 1982.

[28] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization." *ICISSp*, vol. 1, pp. 108–116, 2018.

[29] N. Frosst and G. Hinton, "Distilling a neural network into a soft decision tree," *arXiv preprint arXiv:1711.09784*, 2017.

[30] L. Breiman, "Random forests," *Machine learning*, vol. 45, pp. 5–32, 2001.

[31] Y. Freund and R. E. Schapire, "A decision-theoretic generalization of on-line learning and an application to boosting," *Journal of computer and system sciences*, vol. 55, no. 1, pp. 119–139, 1997.

[32] G. Ke, Q. Meng, T. Finley, T. Wang, W. Chen, W. Ma, Q. Ye, and T.-Y. Liu, "Lightgbm: A highly efficient gradient boosting decision tree," *Advances in neural information processing systems*, vol. 30, 2017.

[33] R. A. Fisher, "The use of multiple measurements in taxonomic problems," *Annals of eugenics*, vol. 7, no. 2, pp. 179–188, 1936.

[34] L. Wu, C. Shen, and A. Van Den Hengel, "Deep linear discriminant analysis on fisher networks: A hybrid architecture for person re-identification," *Pattern Recognition*, vol. 65, pp. 238–250, 2017.

[35] M. Sokolova and G. Lapalme, "A systematic analysis of performance measures for classification tasks," *Information processing & management*, vol. 45, no. 4, pp. 427–437, 2009.

[36] D. M. Powers, "Evaluation: from precision, recall and f-measure to roc, informedness, markedness and correlation," *arXiv preprint arXiv:2010.16061*, 2020.

[37] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the kdd cup 99 data set," in *2009 IEEE symposium on computational intelligence for security and defense applications*. Ieee, 2009, pp. 1–6.

[38] C. Cortes and V. Vapnik, "Support-vector networks," *Machine learning*, vol. 20, pp. 273–297, 1995.

[39] T. Chen and C. Guestrin, "Xgboost: A scalable tree boosting system," in *Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining*, 2016, pp. 785–794.

[40] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *nature*, vol. 521, no. 7553, pp. 436–444, 2015.

[41] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

[42] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," *Advances in neural information processing systems*, vol. 25, 2012.

[43] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," *arXiv preprint arXiv:1409.1556*, 2014.

[44] A. Ismail, S. A. Ahmad, A. C. Soh, K. Hassan, and H. H. Harith, "Improving convolutional neural network (cnn) architecture (minivggnet) with batch normalization and learning rate decay factor for image classification," *International Journal of Integrated Engineering*, vol. 11, no. 4, 2019.
[45] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (ddos) attack dataset and taxonomy," in *2019 International Carnahan Conference on Security Technology (ICCST)*. IEEE, 2019, pp. 1–8.
[46] J. J. Hopfield, "Neural networks and physical systems with emergent collective computational abilities." *Proceedings of the national academy of sciences*, vol. 79, no. 8, pp. 2554–2558, 1982.
[47] A. Verikas and M. Bacauskiene, "Feature selection with neural networks," *Pattern recognition letters*, vol. 23, no. 11, pp. 1323–1335, 2002.
[48] F. Rosenblatt, "The perceptron: a probabilistic model for information storage and organization in the brain." *Psychological review*, vol. 65, no. 6, p. 386, 1958.
[49] L. A. Jeni, J. F. Cohn, and F. De La Torre, "Facing imbalanced data–recommendations for the use of performance metrics," in *2013 Humaine association conference on affective computing and intelligent interaction*. IEEE, 2013, pp. 245–251.
[50] J. Van Hulse, T. M. Khoshgoftaar, and A. Napolitano, "Experimental perspectives on learning from imbalanced data," in *Proceedings of the 24th international conference on Machine learning*, 2007, pp. 935–942.
[51] F. J. Massey Jr, "The kolmogorov-smirnov test for goodness of fit," *Journal of the American statistical Association*, vol. 46, no. 253, pp. 68–78, 1951.
[52] N. Seliya, T. M. Khoshgoftaar, and J. Van Hulse, "A study on the relationships of classifier performance metrics," in *2009 21st IEEE international conference on tools with artificial intelligence*. IEEE, 2009, pp. 59–66.
[53] A. Mihoub, O. B. Fredj, O. Cheikhrouhou, A. Derhab, and M. Krichen, "Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques," *Computers & Electrical Engineering*, vol. 98, p. 107716, 2022.
[54] J. Cohen, "A coefficient of agreement for nominal scales," *Educational and psychological measurement*, vol. 20, no. 1, pp. 37–46, 1960.
[55] T. Bayes, "Lii. an essay towards solving a problem in the doctrine of chances. by the late rev. mr. bayes, frs communicated by mr. price, in a letter to john canton, amfr s," *Philosophical transactions of the Royal Society of London*, no. 53, pp. 370–418, 1763.
[56] I. Rish *et al.*, "An empirical study of the naive bayes classifier," in *IJCAI 2001 workshop on empirical methods in artificial intelligence*, vol. 3, no. 22, 2001, pp. 41–46.
[57] S. L. Salzberg, "C4. 5: Programs for machine learning by j. ross quinlan. morgan kaufmann publishers, inc., 1993," 1994.
[58] D. R. Cox, "The regression analysis of binary sequences," *Journal of the Royal Statistical Society Series B: Statistical Methodology*, vol. 20, no. 2, pp. 215–232, 1958.
[59] J. M. Johnson and T. M. Khoshgoftaar, "Survey on deep learning with class imbalance," *Journal of Big Data*, vol. 6, no. 1, pp. 1–54, 2019.
[60] J. G. Almaraz-Rivera, J. A. Perez-Diaz, and J. A. Cantoral-Ceballos, "Transport and application layer ddos attacks detection to iot devices by using machine learning and deep learning models," *Sensors*, vol. 22, no. 9, p. 3367, 2022.
[61] A. B. de Neira, B. Kantarci, and M. Nogueira, "Distributed denial of service attack prediction: Challenges, open issues and opportunities," *Computer Networks*, vol. 222, p. 109553, 2023.
[62] M. Usama, J. Qadir, A. Raza, H. Arif, K.-L. A. Yau, Y. Elkhatib, A. Hussain, and A. Al-Fuqaha, "Unsupervised machine learning for networking: Techniques, applications and research challenges," *IEEE access*, vol. 7, pp. 65 579–65 615, 2019.
[63] J. Mazel, "Unsupervised network anomaly detection," Ph.D. dissertation, INSA de Toulouse, 2011.
[64] P. Casas, J. Mazel, and P. Owezarski, "Unsupervised network intrusion detection systems: Detecting the unknown without knowledge," *Computer Communications*, vol. 35, no. 7, pp. 772–783, 2012.
[65] C. Bellas, G. Kougka, A. Naskos, A. Gounaris, A. Vakali, C. Xenakis, and A. Papadopoulos, "Facilitating dos attack detection using unsupervised anomaly detection," in *Proceedings of the 34th International Conference on Scientific and Statistical Database Management*, 2022, pp. 1–4.
[66] I. Syarif, A. Prugel-Bennett, and G. Wills, "Unsupervised clustering approach for network anomaly detection," in *Networked Digital Technologies: 4th International Conference, NDT 2012, Dubai, UAE, April 24-26, 2012. Proceedings, Part I 4*. Springer, 2012, pp. 135–145.