Proceedings of the 2023 International Conference on Machine Learning and Automation
DOI: 10.54254/2755-2721/34/20230314

Identifying network connection: Benign vs. DoS Attack - A comparative analysis of binary classifiers

Shuhan Gu

Boston University, 645-665 Commonwealth Ave, Boston, MA 02215, USA

han0705@bu.edu

Abstract. The escalating complexity of cyber-attacks coupled with the increasing sophistication of attackers have created an imperative need for robust and adaptable defense mechanisms to ensure the security of network infrastructure. Among these threats, Denial of Service (DoS) attacks stand out prominently. These attacks focus on inundating systems with high-frequency traffic to exhaust resources and disrupt the availability of services. Consequently, the accurate and timely identification of 'DoS Attacks' is of paramount importance in upholding the integrity and functionality of networks. In this context, the present paper aims to delve into the efficacy of various binary classifiers in effectively distinguishing normal network connections from instances of 'DoS Attacks.' By undertaking this exploration, the study aims to pinpoint the classifiers that exhibit the highest level of effectiveness in tackling this specific task. Ultimately, a comprehensive understanding of which classifiers perform best in discerning these types of cyber threats can significantly contribute to enhancing the overall security posture of network infrastructures.

Keywords: Cyber-Attacks, Denial of Service (DoS) Attacks, Network Defense Mechanisms, Binary Classifiers.

1. Introduction

The ever-growing complexity of cyber-attacks and the sophistication of attackers necessitate robust and adaptive defense mechanisms to safeguard network infrastructure. Denial of Service attacks remain a prominent threat, targeting systems with high-frequency traffic to overwhelm resources and disrupt service availability. Hence, accurate and timely detection of 'DoS Attack' is crucial to maintain the integrity and functionality of networks. This paper aims to explore the capabilities of various binary classifiers in distinguishing normal network connections from 'DoS Attack' and identifying the most effective classifiers for this task.

2. Related works

As the network intrusion problem becomes gradually vital to every other device that has access to the network, researchers categorized deep learning into generative and discriminative types [1], based on which to build the network intrusion protection model. The network intrusion protection model is designed to identify abnormal patterns in both shallow and deep network and host-based systems. The summary of deep learning approaches for network intrusion study for the IoT networks is shown in table 1.

DOI: 10.54254/2755-2721/34/20230314

Table 1. Summary of deep learning approaches for network intrusion study for the IoT networks.

System	Network Model	The Basic Idea	Source
Diro and Chilamkurti	Social internet of things	Deploy the distributed attack detection system at the fog computing layer	[2]
VinayaKumar et al.	The Internet of Things networks of smart cities	Uses a two-tier environment for monitoring DNS logs	[3]
Parra et al.	Internet of things	The CNN is used in an IoT micro-security add-on, while the LSTM is used by the back-end server	[4]
Latif et al.	Industrial internet of things	Uses a model with 1 input layer, 8 hidden layers, and 1 output layer	[5]
Zhou et al.	Industry 4.0	Detecting IoT attacks based a encoder–decoder neural network	[6]
NG and Selva-kumar	Fog computing-enable Internet of things	The computations are performed in the fog nodes	[7]

3. Methodology

3.1. Data selection and processing

In this research endeavor, a pertinent dataset on internet activity sourced from Kaggle has been identified [8], representing real-life traces from the real world. While this dataset encompasses a plethora of diverse internet attacks, the focus of the current investigation shall be dedicated to the analysis of Denial of Service (DoS) attacks. The rationale behind this choice stems from the inherent nature of 'DoS Attack', wherein an extensive influx of packets is unleashed within a condensed time frame.

Given the intricacies and scale of the dataset, prudent consideration has been bestowed upon the computational resources at hand. Consequently, a judicious approach has been adopted, wherein the primary focus rests on employing the initial 5,000 dataset entries for model training. Subsequently, a rigorous testing phase will be conducted utilizing the subsequent 950 entries. This meticulous partitioning ensures the optimization of analytical efficiency and robustness.

3.2. Feature selection and engineering

Upon eliminating the row pertaining to other types of attacks and establishing an organized dataset, the focal point of the investigation transitions towards identifying the independent variable, X, that exhibits the strongest correlation with the dependent variable, Y, representing the "ATTACK". Given the inherent characteristics of the Denial of Service (DoS) attack, a judicious selection of eleven distinct variables has been undertaken. The primary objective behind this selection is to construct a comprehensive Correlation Matrix, thereby discerning the variable that most effectively encapsulates fluctuations in the diverse "ATTACK". Through this rigorous analytical process, the study aims to pinpoint the key factors that contribute significantly to the variance in attack classifications, fostering a deeper understanding of the underlying dynamics and providing valuable insights into bolstering cybersecurity measures.

DOI: 10.54254/2755-2721/34/20230314

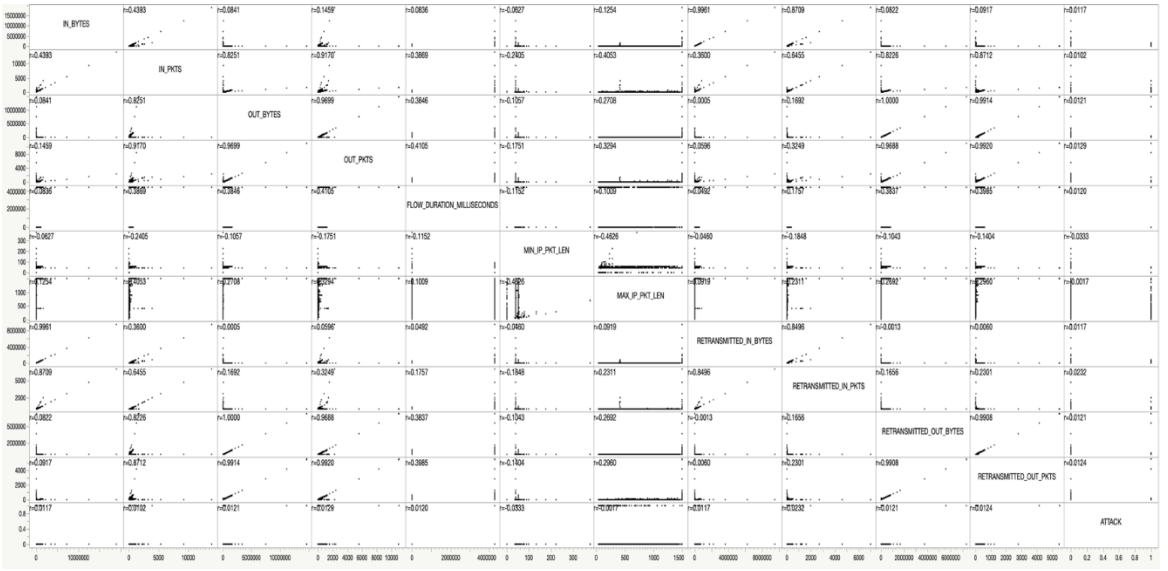

Figure 2. Correlation matrix with eleven distinct variables and “ATTACK”.

The analysis presented in fig. 2 provides valuable insights into the interrelationship among the eleven distinct variables under scrutiny. Upon thorough observation of the correlation patterns, a conspicuous finding emerges, unequivocally indicating that "MIN_IP_PKT_LEN" exhibits the most pronounced correlation among all the variables. To gain a more granular perspective, fig. 3 offers a magnified representation of the correlation matrix, elucidating the finer nuances of the relationships under consideration. Building upon these discerning findings, the forthcoming experiment and research endeavors will revolve around treating "MIN_IP_PKT_LEN" as the independent variable, while the "ATTACK" will be assigned the role of the dependent variable.

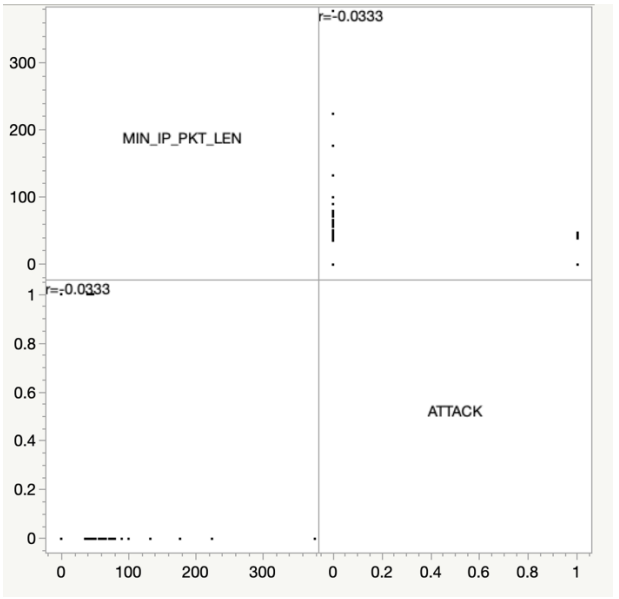

Figure 3. Correlation matrix with “MIN_IP_PKT_LEN” and “ATTACK”.

3.3. Model selection and description

In the pursuit of effectively addressing binary classification challenges, my research undertook a comprehensive evaluation of various classification methodologies. The central task involved discerning

DOI: 10.54254/2755-2721/34/20230314

between two distinct classes within the dataset. To tackle this, three prominent classifiers were explored: the Logistic Regression Binary Classifier, Gaussian Naive Bayes classifier [9][10] and K-Nearest Neighbors (KNN) classifier. The classification problem aimed to assign data points to one of two categories, demanding models with predictive accuracy. The Logistic Regression Binary Classifier leveraged statistical principles to model the relationship between predictor variables and class probabilities, enabling precise classification. The Gaussian Naive Bayes classifier assumed a normal distribution of features within each class, employing Bayesian probabilities to make informed predictions. On the other hand, the KNN classifier utilized proximity-based classification, assigning data points to the majority class among their k-nearest neighbors. This research encompassed a diverse spectrum of techniques, ranging from probabilistic modeling to distance-based categorization, fostering an encompassing comparison of their effectiveness in binary classification scenarios.

3.3.1. Logistic regression binary classifier. In the Logistic Regression model, I assume that I have N Bernoulli measurements of N individual "MIN_IP_PKT_LEN". I donate this measurement as l_i for $i \in \{0, \cdots, N\}$. I assume that each l_i is sampled independently from a Bernoulli distribution such that:

$$l_i \sim Bernoulli(1-p) \tag{1}$$

where p denotes the probability derived from applying the logistic function to the entirety of data points. To be more specific, I model p as following:

$$p = \frac{1}{1+e^{-k(t-t_0)}} \tag{2}$$

where t is the value of each data points. Since I do not directly observe k and t_0, and thus I need to assign reasonable priors to them. Due to the advantageous conjugate relationship that exists between the Exponential distribution and the Logistic distribution, I can sample k from Exponential distribution. As for t_0, adopting a customary and fundamental approach, the initial presumption often involves considering the normal distribution and the parameters of which have been adjusted by experiment tryouts to get the mean of 40 and standard deviation of 100.

$$k \sim Exponential(1) \tag{3}$$

$$t_0 \sim Normal(40,100) \tag{4}$$

3.3.2. Gaussian naive bayes classifier. As for the naive Bayesian approach, using the same training dataset, I assume that I have N measurements of the "MIN_IP_PKT_LEN" and I denote every individual measurement as g_i for $i \in \{0, \cdots, N\}$. For each of the N measurements:

$$g_i \sim Normal(\mu, \sigma)$$

Within this methodology, both μ and σ have two values, switching back and forth, based on specific data points. Employing two distinct Normal distributions, the former with parameters of mean 20 and standard deviation 20 to signify a 'DoS Attack', and the latter with mean 52 and standard deviation 2 to represent 'Benign Attack', their values shaped through experimental exploration and this approach provides a structured framework to unravel potential outcomes.

$$M_1 = 20 \ (with\ probability\ p) \tag{6}$$

$$\Sigma_1 = 20 \ (with\ probability\ p) \tag{7}$$

$$\mu_2 = 52 \ (with\ probability\ 1-p) \tag{8}$$

$$\sigma_2 = 2 \ (with\ probability\ 1-p) \tag{9}$$

Here, the variable p assumes a pivotal role, serving as a key determinant for each distinct data point's affiliation with a specific Normal distribution. Through a meticulous process, p is generated for every

DOI: 10.54254/2755-2721/34/20230314

alternative data point, allowing for an informed assessment of the likelihood that a given data point aligns more closely with one of the two Normal distributions.

$$p \sim Bernoulli(p_{prior}) \tag{10}$$

Naturally, p isn't directly observable initially. So, to begin, I make an educated guess about the probability and call it p_{prior}.This guess comes from a Uniform distribution ranging between 0 and 1, reflecting our neutral stance, for each of the data points.

$$p_{prior} \sim \text{Uniform}(0,1) \tag{11}$$

3.3.3. K-Nearest Neighbors (KNN) classifier. K-Nearest Neighbors (KNN) is a simple yet versatile machine learning algorithm used for classification and regression tasks. It operates on the principle of proximity, where it classifies or predicts a data point's label or value based on the majority or weighted average of its k nearest neighbors in the feature space. In the case of classification, KNN assigns a class label to a new data point by considering the labels of its neighboring data points. The value of k determines the number of neighbors taken into account, influencing the algorithm's bias-variance trade-off. In our case:

$$k = 3 \tag{12}$$

KNN doesn't require prior training and can handle both numerical and categorical data, making it easy to implement and interpret. However, its performance can be affected by the choice of distance metric, the value of k, and data dimensionality. Regularization techniques, distance weighting, and dimensionality reduction methods are often employed to enhance KNN's effectiveness and mitigate potential limitations.

4. Results and discussion

Our research reveals the comparative effectiveness of different binary classifiers in distinguishing 'Benign Attack' from 'DoS Attack'. Drawing insights from the Receiver Operating Characteristic (ROC) curves, meticulously presented for each individual classifier, as well as the quantification of the area beneath these curves, a discernible pattern emerges. Specifically, it becomes evident that both the Logistic Regression classifier and the Gaussian Naive Bayes classifier exhibit a congruent level of accuracy, as discerned from their nearly overlapping ROC curves and analogous area values. This alignment in accuracy underscores the consistency of these two classifiers in their predictive capacity. In contrast, a marginal departure from this similarity is discerned with the K-Nearest Neighbors (KNN) classifier. It is noteworthy that the KNN classifier exhibits a slightly diminished level of accuracy compared to its counterparts, as suggested by its ROC curve being subtly displaced from the convergence point of the others.

On the other hand, when we consider the effectiveness of the Logistic Regression classifier versus the Gaussian Naive Bayes classifier, it's worth noting that as discussed earlier, the Gaussian Naive Bayes classifier tends to show greater deviation from the true value as the sample size increases. In this context, the Logistic Regression classifier appears to outperform the Gaussian Naive Bayes classifier. This indicates that when dealing with this specific problem and dataset in question, the Logistic Regression classifier offers more consistent and accurate results.

5. Limitations

The primary limitation faced in this study is related to the dataset itself. Within this dataset, there is a significant issue with the distribution of instances labeled as 'DoS Attack'. These 'DoS Attack' entries are heavily skewed towards a relatively small proportion, which poses a challenge for the model's ability to predict them accurately. The lack of sufficient representative data for this specific attack category makes it difficult for the model to predict 'DoS Attack' reliably, thus hindering the achievement of dependable and robust predictions.

DOI: 10.54254/2755-2721/34/20230314

Specifically, the dataset includes only 150 entries that are classified as 'DoS Attack'. This limited sample size makes it complex to train the model to effectively understand and differentiate the intricacies of 'DoS Attack' patterns. This constraint becomes even more apparent when using the Gaussian Naive Bayes classifier. As previously mentioned, the model's predictive accuracy noticeably decreases when dealing with an expanded dataset containing 5,000 samples. This significant drop in predictive accuracy highlights the model's vulnerability to changes in sample size, emphasizing the intricate relationship between data scarcity, classifier performance, and model generalization.

An additional limitation relating to this study involves computational abilities. The subset of 5,000 samples employed for analysis represents a substantially reduced version of the original dataset, which encompasses an extensive compilation of over 2,000,000 samples. This reduction in dataset size is necessitated by computational limitations, as the computational demands associated with processing the entire dataset transcend the available resources. However, it is worth acknowledging that the introduction of the entire dataset, the whole 2,000,000 samples, has the potential to yield more comprehensive results, which is needed for further research.

References

[1] Mohamed Amine Ferrag Leandros Maglaras, Helge Jan- icke et al. (2019). “Deep Learning Techniques for Cyber Security Intrusion Detection : A Detailed Anal- ysis.” In: 6th International Symposium for ICS and SCADA Cyber Security Research 2019 (ICS-CSR).

[2] Diro, Abebe Abeshu and Naveen Chilamkurti (2018). “Distributed attack detection scheme using deep learning approach for Internet of Things”. In: Fu- ture Generation Computer Systems 82, pp. 761–768. issn: 0167-739X. doi: https://doi.org/10. 1016/j.future.2017.08.043. url: https:// www.sciencedirect.com/science/article/pii/ S0167739X17308488.

[3] Vinayakumar, R. et al. (2020). “A Visualized Botnet Detection System Based Deep Learning for the In- ternet of Things Networks of Smart Cities”. In: IEEE Transactions on Industry Applications 56.4, pp. 4436– 4456. doi: 10.1109/TIA.2020.2971952.

[4] De La Torre Parra, Gonzalo et al. (2020). “Detecting Internet of Things attacks using distributed deep learning”. In: Journal of Network and Computer Ap- plications 163, p. 102662. issn: 1084-8045. doi: https://doi.org/10.1016/j.jnca.2020.102662.

[5] Latif, Shahid et al. (2020). “A Novel Attack Detection Scheme for the Industrial Internet of Things Using a Lightweight Random Neural Network”. In: IEEE Access 8, pp. 89337–89350. doi: 10.1109/ACCESS. 2020.2994079.

[6] Zhou, Xiaokang et al. (2021). “Variational LSTM En- hanced Anomaly Detection for Industrial Big Data”. In: IEEE Transactions on Industrial Informatics 17.5, pp. 3469–3477. doi: 10.1109/TII.2020.3022432.

[7] N.G., Bhuvaneswari Amma and Selvakumar S. (2020). “Anomaly detection framework for Internet of things traffic using vector convolutional deep learning ap- proach in fog environment”. In: Future Generation Computer Systems 113, pp. 255–265. issn: 0167- 739X. doi: https://doi.org/10.1016/j.future. 2020.07.020. url: https://www.sciencedirect. com/science/article/pii/S0167739X19316954.

[8] Srinath, Sankuri (Updated on 2023 July). NFF-UNSW- NB15. url: https://www.kaggle.com/datasets/ sankurisrinath/nf-unsw-nb15-v2csv.

[9] Davidson-Pilon, Cameron (2015). Bayesian Methods for Hackers: Probabilistic Programming and Bayesian Inference. Addison-Wesley Professional.

[10] Martin, Osvaldo (2018). Bayesian Analysis with Python: Introduction to statistical modeling and probabilistic programming using PyMC3 and ArviZ. Packt Publishing.