IJERMT

International Journal of Engineering Research & Management Technology

ISSN: 2348-4039

Volume 9, Issue-6 November-December- 2022

Email: editor@ijermt.org www.ijermt.org

NETWORK PERFORMANCE IMPROVEMENT BY DDOS ATTACK DETECTION USING MACHINE LEARNING

Parula,

Research Scholar, School of Technology and Computer Science,

Glocal University Saharanpur (U. P.)

Dr. Aaruni Goel,

Research Supervisor School of Technology and Computer Science,

Glocal University Saharanpur

ABSTRACT

DDoS assaults are a serious problem for businesses that have integrated their technology into public networks since they enable numerous attackers to access data or provide services to big businesses or nations. As a result of the Distributed Denial of Service (DDoS) assaults, which overwhelm the company's servers with erroneous requests while denying genuine users' requests, rendered services become unavailable for an indefinite amount of time, resulting in financial losses. The purpose of this paper is to demonstrate the process of detecting prototype DDoS attacks using Support Vector Machines (SVM), a supervised learning model that captures network traffic, filters HTTP headers, normalises the data based on operational variables, such as rate of false positives, rate of false negatives, and rate of classification, and then sends the data to the appropriate training and testing sets. Different machine learning models, including Navies Bayes, SVM, and suggested approaches based on Navies Bayes, are constructed with the chosen attributes for effective DDoS attack detection. Finally, the results of our experiments demonstrate that Fuzzy c-means clustering provides a higher level of attack detection accuracy.

Keywords: Navies Bayes , Support Vector Machines , Machine Learning , DDOS Attack Detection

INTRODUCTION

A DDoS attack entails sending tens of thousands or even hundreds of thousands of requests per second to a server from various locations or IP addresses; the term "Distributor" refers to the fact that these requests are sent from hundreds of thousands of infected machines (commonly referred to as "zombies") that are controlled by "botnets" simultaneously, i.e. SYN Flood and Smurf attacks, which combine bandwidth, memory usage, and target processing; Information security and pattern recognition research have both successfully applied machine learning with SVM to various categorization, prediction, and regression processes. Since the generation of the model is based on a statistical model that changes its behaviour in accordance with the input parameters defined and is based on a training rule that necessitates human interaction, the application of techniques with an SVM supervised model has significant advantages over rule-based techniques. In the prototype evaluation, it was discovered that the correct classification rate of normal or abnormal requests in the training phase is directly related to standardization a. This essay explains: The relevant work in section 2 and the contextual reference. The proposed model for the creation and use of a machine learning prototype is shown in Section 3. Some results are obvious in section 4, and in the final section, section 5, the conclusions are stated.

DDOS ATTACKS AND DETECTION METHODOLOGIES

Although cloud services are becoming more and more popular, assuring the security and accessibility of data, resources, and services is still a research problem. DDoS attacks are a significant security concern and a broad area of continuing academic interest. They are not a new threat. This section reviews intrusion detection methodologies and protection tactics as well as various DDoS intend and launch techniques that may be used to carry out or support DDoS attacks.

A. DDoS Attack

1) DDoS Intention and Methods of Launch DoS attacks are attempts to prevent authorised users from accessing a certain network resource. To comprehend the kinds of DDoS attacks we face, it helps to grasp the Open Systems Interconnection Model (OSI model).DDoS attacks target particular layers of a network connection (attacks on the application layer target layer 7, while attacks on the protocol layer target layers 3 and 4). It was reported that the first DDoS attack had occurred [30].

There are now two basic ways to start DDoS assaults on the Internet. The first is a vulnerability attack when packets with errors are sent to the recipient. In the second technique, an attacker tries to accomplish either or both of the following:

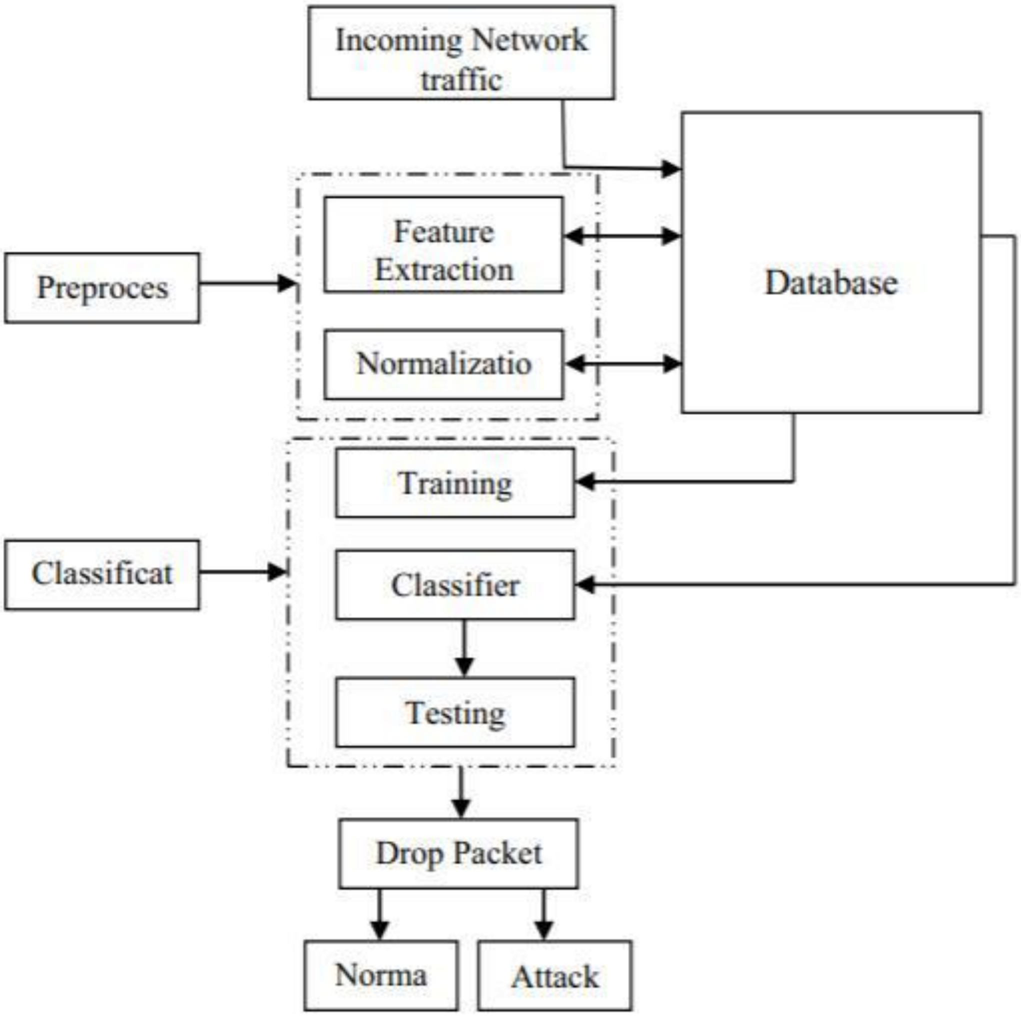

Figure 2: Existing model (Sumathi, S., & Karthikeyan, N. (2020)

Disrupt a legitimate users connectivity by exhausting bandwidth, router processing capacity or network resources.

These are essentially network/transport-level flooding attacks . (i.e., flooding attacks)

• Disrupt legitimate users services by exhausting the server resources (e.g., sockets, CPU, memory, disk/database bandwidth, and I/O bandwidth) These essentially include application-level flooding attacks.

2) The attacker's incentives: DDoS attackers are usually motivated by various justifications. Analyzing the attackers incentives help to stop and respond to these attacks .

- Economical/Financial gain: A major concern of corporations generally performed by frustrated individuals, possibly with lower technical skills.
- Intellectual Challenge: The attacks are usually young hacking enthusiasts who want to show off their capabilities to experiment and learn how to launch various attacks.
- Cyber warfare: This category of Attackers are usually politically motivated to attack a wide range of critical sections of another country.

Machine Learning Methodologies We briefly detail the various machine learning algorithms used in the suggested framework in this section.

The Naive Bayes is a straightforward probabilistic classifier [13]. It is predicated on the idea that a variable's impact on a particular class is unaffected by the values of other variables. The term "class conditional independence" refers to this presumption.

SVM Support Vector Machines are the most prevalent and well-liked approach for machine learning tasks in classification and regression. This method provides a series of training examples, each of which is designated as falling into one of two categories. The Support Vector Machines approach is then used to create a model that can forecast whether a new example belongs to one category or another.

Attacking system and Internet resources via a Distributed Denial of Service (DDoS) attack is a straightforward and reliable technique. Along with insect viruses, the side effect has a significant negative impact on real networks. Because DDoS attacks are becoming more frequent, there have been numerous studies done on detection mechanisms. The defence capacity of the current protection systems is solely restricted to a set of DDoS attacks. The detection of DDoS attacks is one of many uses for data mining techniques. The study that follows describes the extraction of a feature set from two independent Internet traffic datasets. These are the Smart and Secure Environment (SSE) Network's (public-domain) traffic and CAIDA Dataset. The traffic metrics that alter unexpectedly during different forms of DDoS attacks are explored. The twenty-three features are gathered, ranked using Information Gain and the Chi-Square statistic, which reduces the twenty-three features to eight. Each attribute used in this study is calculated once every second. Because these classes are clearly split into attack and normal behaviour, a variety of machine learning techniques can be used for detection. The strategy under consideration is to develop the classifier utilising different machine learning algorithms, such as SVM, K-NN, and Naive Bayesian, while utilising the feature selection method previously stated. In this stage of the study, the effectiveness of the chosen set of machine learning algorithms in identifying DDoS attacks is evaluated. The receiver operating characteristic (ROC) curve and F-measure serve as performance indicators. A crucial Training

Each dataset's data is given to pre-processing and feature extraction throughout the training phase. At this stage, classes are assigned to trained features once they have been trained for each unique piece of dataset data. This algorithm has two classes: normal and DDoS assault.

Testing When performing testing, test samples are supplied into a DNN classifier, which then uses training features to categorise the test instance into class j. Correct classification of the provided class by the classifier will improve the process's output. If the DNN classifier's decision is not final, the cost-minimization algorithm technique is used to get the conclusion.

One of the classifiers in the machine learning approach, proposed approaches based on the Bayesian algorithm classify the data by assigning a class label to each instance of the problem [10, 11], where the class label is taken from the dataset. The main presumption is that each feature operates independently of the others. Class conditional independence is the premise under consideration. A modest amount of training data is needed to classify the attack. It is based on the Bayesian probabilistic model provided below:

$$p(C|S_0, S_1, \ldots.., S_n) = \frac{p(C).p(S_0, S_1, \ldots.., S_n|C)}{p(C|S_0, S_1, \ldots.., S_n)}$$

WhereC is the class of dataset, S0, S1,…,Sn is the set of features in the dataset, and p() is a probability function Our proposed methods bsed on naive Bayes classifier emerged out to be the best classifier for detecting DDoS attacks. most of the authors have considered approaches and also suggested that naïve Bayes approach will give better accuracy. So, naive Bayes, procedure in data mining were experimented and also compared to the accuracy and error. The 10-fold cross-validation was employed in the experimentation.

RESULTS

Method Used	Correct Classification %	Detection Time (in seconds)

Naive Bayesian	96.2	0.52
SVM	93.4	0.23
KNN	92.6	0.25
proposed methods	98.7	0.21

Table 1. Classification results

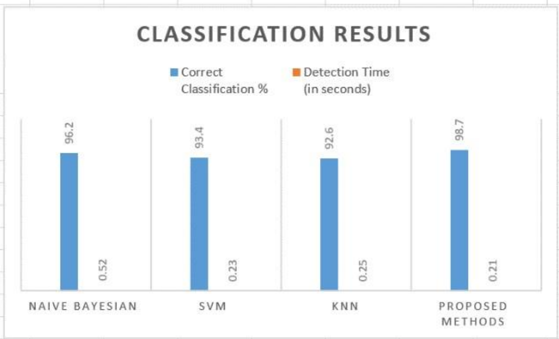

Figure 2: Classification results

CONCLUSION

The created model has an appropriate percentage of classification at the time of the evaluation of the prototype in a production setting with real information because it is based on the training process and machine learning tuning using the standard data set. The measures chosen for the intrusion detection issue, such as false positive and false negative rates, rate classification, and ROC curves, enable benchmark comparisons with other models. Since the generation of the model is based on a statistical model that changes its behaviour in response to the input parameters defined in the training, the application of techniques with supervised training, such as SVM models, has significant advantages over the technique based on rules. In contrast, the application of rules-based techniques necessitates human interaction. A better classification rate for normal and anomalous requests was discovered in the prototype evaluation's training phase. This improvement is directly related to standardization and proper input parameter selection, allowing output variables to be generated with the lowest possible percentage of misclassification, generating reliability in the generated model, and detecting these behaviours.

REFERENCES

[1].Wani, A. R., Rana, Q. P., Saxena, U., & Pandey, N. (2019). Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques. 2019 Amity International Conference on Artificial Intelligence (AICAI). doi:10.1109/aicai.2019.8701238

[2]. WU ZHIJUN , XU QING , WANG JINGJIE , YUE MENG (2020) Low-Rate DDoS Attack Detection Based on Factorization Machine in Software Defined Network, Digital Object Identifier 10.1109/ACCESS.2020.2967478, VOLUME 8, 2020

[3].Yadav, S., & Subramanian, S. (2016). *Detection of Application Layer DDoS attack by feature learning using Stacked Auto Encoder. 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT).* doi:10.1109/icctict.2016.7514608

[4].Bakker, J. N., Ng, B., & Seah, W. K. G. (2018). Can Machine Learning Techniques Be Effectively Used in Real Networks against DDoS Attacks? 2018 27th International Conference on Computer Communication and Networks (ICCCN). doi:10.1109/icccn.2018.8487445

[5]. Khuphiran, P., Leelaprute, P., Uthayopas, P., Ichikawa, K., & Watanakeesuntorn, W. (2018). *Performance Comparison of Machine Learning Models for DDoS Attacks Detection. 2018 22nd International Computer Science and Engineering Conference (ICSEC).* doi:10.1109/icsec.2018.8712757

[6].Yuan, X., Li, C., & Li, X. (2017). *DeepDefense: Identifying DDoS Attack via Deep Learning. 2017 IEEE International Conference on Smart Computing (SMARTCOMP).* doi:10.1109/smartcomp.2017.7946998

[7].Subbulakshmi, T., BalaKrishnan, K., Shalinie, S. M., AnandKumar, D., GanapathiSubramanian, V., & Kannathal, K. (2011). *Detection of DDoS attacks using Enhanced Support Vector Machines with real time generated dataset. 2011 Third International Conference on Advanced Computing.* doi:10.1109/icoac.2011.6165212

[8]. Hoyos Ll, M. S., Isaza E, G. A., Vélez, J. I., & Castillo O, L. (2016). *Distributed Denial of Service (DDoS) Attacks Detection Using Machine Learning Prototype. Advances in Intelligent Systems and Computing, 33–41.* doi:10.1007/978-3-319-40162-1_4

[9]. Suresh, M., & Anitha, R. (2011). *Evaluating Machine Learning Algorithms for Detecting DDoS Attacks. Communications in Computer and Information Science, 441–452.* doi:10.1007/978-3-642-22540-6_42

[10]. Rajawat A.S., Upadhyay P., Upadhyay A. (2021) Novel Deep Learning Model for Uncertainty Prediction in Mobile Computing. In: Arai K., Kapoor S., Bhatia R. (eds) Intelligent Systems and Applications. IntelliSys 2020. Advances in Intelligent Systems and Computing, vol 1250. Springer, Cham. https://doi.org/10.1007/978-3-030-55180-3_49

[11]. Narasimha Mallikarjunan, K., Bhuvaneshwaran, A., Sundarakantham, K., & Mercy Shalinie, S. (2018). *DDAM: Detecting DDoS Attacks Using Machine Learning Approach. Advances in Intelligent Systems and Computing, 261–273.* doi:10.1007/978-981-13-1132-1_21

[12]. Abid, K.: An efficient intrusion detection using J48 decision tree in KDDCUP99 dataset. Int. J. Emerging Technol. Adv. Eng. 6(2), (2016)

[13]. Sumathi, S., & Karthikeyan, N. (2020). *Detection of distributed denial of service using deep learning neural network. Journal of Ambient Intelligence and Humanized Computing.* doi:10.1007/s12652-020-02144-2

[14]. A. Singh Rajawat and S. Jain, "Fusion Deep Learning Based on Back Propagation Neural Network for Personalization," 2nd International Conference on Data, Engineering and Applications (IDEA), Bhopal, India, 2020, pp. 1-7, doi: 10.1109/IDEA49133.2020.9170693.