COMPATIVE ANALYSIS OF DEEP LEARNING MODELS FOR DDOS ATTACKS DETECTION

Artur PETROSYAN
Senior Software Developer, "Synopsys", PhD in Electronics
Eduard HARUTYUNYAN
Software Developer, "Krisp", MA student, NPUA, Synopsys
David GALSTYAN
Software Developer, "Frismos", MA student, NPUA, Synopsys

Keywords: DDOS, DFF, CNN, BiLSTM, deep learning

Introduction. Data stored online keeps growing more and more each year, causing a corresponding increase in data value. This, in turn, causes a growing number of threats that come up to target systems containing the data and maliciously access them. The DDoS (Distributed Denial of Service) attack utilizes multiple machines to develop the flooding of packets directed to an aimed machine to create the service disruption on the target computer machine [4].

DDoS attacks are quickly developing in magnitude and complexity in tandem with the rise of new web technologies on the internet [2]. This being the case, many people have conducted extensive studies to determine how this issue can be mitigated by developing specific tools to aid in the endeavor, developing several deep learning techniques, and GPU inventions. This shows that there is promise in developing faster high-performance detection techniques [1].

Scientific novelty. The development of the latest technologies in almost all spheres makes it possible to accelerate the implementation of works, ensuring high efficiency. But at the same time, the digitization of complete information brings with it a number of problems, among which the issue of information security can be singled out. It is impossible today to imagine the work of any branch of the economy without digitalization, but given the dangers and opportunities of many cyber attacks in the world, there is also a need to follow the rules of cyber security, to avoid possible attacks and losses as a result. Therefore, companies face potential cyber threats to their network environment and computer machines that may cause severe effects to their operations, like business downtime, ransom demands, and data breaches from hackers.

The topic is a novelty since it enables the organization to determine key approaches to detecting DDoS attacks and utilize several machine learning techniques. With the development of deep learning methods and powerful GPU hardware, there is significant potential to create devices and techniques to detect DDoS attacks instantly. The discovery of DDoS attacks is important before any reduction approaches can be applied.

About Deep Learning. Deep learning is a field of Computer Science that enables companies to use sophisticated feature embedding techniques to learn from historical data and accurately predict new data with desirable outcomes. This method has been used successfully in many application areas, such as stock market prediction sentiment analysis, text categorization, natural language processing, and so much more [2].

Deep Feed Foward algorithm. Deep feedforward networks, also known as feedforward neural networks or multilayer perceptron's (MLPs)[5]. Their goal is to approximate some function f*. In perceptron where neuron value is 0 or 1, the weighted some are greater than some threshold value. In our case, we will use the sigmoid neuron.

CNN-Bi-LSTM algorithm. A CNN-BiLSTM is a hybrid bidirectional CNN and BiLSTM architecture. It can learn both character-level and word-level features. The CNN component induces character-level features. Each model applies a max-pooling and convolution layer to excerpt a new characteristic vector from the per-character featured vector like the character embeddings and character kind.

Methodology. The dataset used in the study involved is the DDoS Botnet Attack on IoT a71a0b42-4 available at Kaggle. The dataset is large and contains 47 feature columns. So the aim is to create a DDoS attack by aggregating information on packets [3]. The created model then analyzes these packets and classifies each time window into a period where a DDoS attack is underway or not. DDoS attacks take over the management of a large number of computer systems known as a botnet and launch synchronized attacks on the specific system.

*Data Normalization.*Certain components are involved in the pre-processing stage of the normalization of the datasets. The components are' data acquisition, Data pre-processing, Model Classification, Output evaluation. Since we have already acquired the data, the next stage is the pre-processing stage. This stage involves processing the data to make it available for training to minimize overfitting. The first stage of pre-processing is noise filtering; the next stage is filling in missing data values and, lastly, creating classes categorized in the form of reflection and exploitation attacks.

Train models. Train models applied two different deep learning models for our approach. When using Bi-LSTMs to extract information from data, they are preferred due to their ability to keep track of this unique information sequence. This overcomes the limitations of traditional LSTMs and RNNs [3]. This research, using BiLSTMs, uses two hidden layers to predict DDoS attacks based on historical data. The data is credited in a multilayer perceptron when using feed-forward neural networks to obtain corresponding threshold values. The problem of Open Set Recognition (OSR) has severe effects on the detection of DDoS attacks since its technology keeps evolving and cause varying traffic feature. A New BI-LSTM model was recommended for detecting unknown attacks in computer machines.

Analysis. The experiments were performed on the datasets using Python. The results were measured through accuracy and precision for both approaches for the two algorithms. We also passed the datasets through a confusion matrix for both algorithms to test the outcome performance of both on the dataset. It was found that the more iterations on the testing data, the higher the accuracy from each iteration.

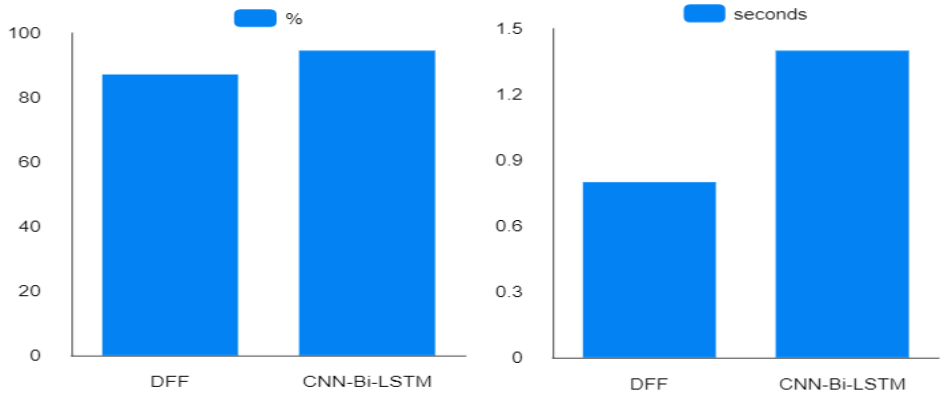

Figure 1. Graphical representations

Outcome 1. Using the CNN-Bi-LSTM with a filter size of 9 * 9 and a filter count of 18, we notice that this model performs 94.6% accuracy. The confusion matrix used in this algorithm classified normal and attack categories with a rate of 0.95 for all outcomes.

Outcome 2. With the second algorithm used, with the training of a batch of 100 trees, the model accuracy was 87.2%. The result for both the confusion and evaluation matrix performed by this algorithm showed a false positive rate of 0.007 and a false negative rate of 0.003.

Graphical Representation. Below are graphical representations of both density plots and confusion matrix performed on the dataset. The graphs created were further compared against each other. From the graphs, it shows that the performance was close.

Conclusion. With the increase of data on the internet and the rise of threats to internet threats, DDoS attacks have become rampant. Traditional intrusion detection systems can only work with small amounts of data. This necessitated using improved methods to handle large amounts of data. These two algorithms were able to achieve that. In terms of accuracy, it was found that CNN-Bi-LSTM achieved a high mean percentage accuracy in testing and training data (94.6%) with detecting the time of 1.4 seconds. feedforward neural networks, performed faster than the other one (0.8 seconds) but loses in the accuracy (87.2%). Also, the feedforward neural network had a faster clocked time than the hybrid network. With an increased rate of data on the internet, new opportunities for threats to aim sensitive data have raised several security challenges like malicious intrusions. Throughout the paper, the application of a machine learning algorithm for the issue of DDoS attack detection has been explained; hence further should be done to improve on detection of cyber-crime. The deep learning model is a valuable choice for the classifications of DDoS attack packets in the perspective of problem detection accuracy.

References

[1] Awan, M. J., Farooq, U., Babar, H. M. A., Yasin, A., Nobanee, H., Hussain, M., ... & Zain, A. M. (2021). Real-time DDoS attack detection system using big data approach. *Sustainability*, *13*(19), 10743. https://doi.org/10.3390/su131910743
[2] Gadze, J.D.; Bamfo-Asante, A.A.; Agyemang, J.O.; Nunoo-Mensah, H.; Opare, K.A.-B. An Investigation into the Application of Deep Learning in the Detection and Mitigation of DDOS Attack on SDN Controllers. Technologies 2021, 9, 14. [CrossRef] https://doi.org/10.3390/technologies9010014
[3] Khuphiran, P., Leelaprute, P., Uthayopas, P., Ichikawa, K., & Watanakeesuntorn, W. (2018, November). Performance comparison of machine learning models for ddos attacks detection. In 2018 22nd International Computer Science and Engineering Conference (ICSEC) (pp. 1-4). IEEE. https://doi.org/10.1109/ICSEC.2018.8712757
[4] Sambangi, S. (2020). A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Regression, 63, 51. https://doi.org/10.3390/proceedings2020063051
[5] Shieh, C. S., Lin, W. W., Nguyen, T. T., Chen, C. H., Horng, M. F., & Miu, D. (2021). Detection of Unknown DDoS Attacks with Deep Learning and Gaussian Mixture Model. *Applied Sciences*, *11*(11), 5213. https://doi.org/10.3390/app11115213

Artur PETROSYAN, Eduard HARUTYUNYAN, David GALSTYAN
Compative analysis of Deep Learning Models for DDOS Attacks Detection
Keywords: DDOS, DFF, CNN, BiLSTM, deep learning

Recently, Distributed Denial of Service(DDOS) attacks have been on the rise and come in very many forms costing many technology firms a lot of time and money. In this study, deep learning models were compared in terms of performance, to solve the problem of detecting these attacks. The first step to mitigating DDOS attacks is by first identifying them, which serves as a toll order. This report used two deep learning models: the Deep Feed Forward (DFF) algorithm and a hybrid containing a CNN with BiLSTM (bidirectional long short-term memory). To compare these algorithms, the "DDoS Botnet Attack on IoT a71a0b42-4" dataset available on Kaggle was chosen. The dataset was undergone various evaluations to find out the performance metrics between the two algorithms. From the simulations conducted, DFF was found to have an accuracy of 87.2% with detecting the time of 0.8 seconds, while the CNN-Bi-LSTM was found to have an accuracy of 94.6% with detecting the time of 1.4 seconds.