A study for DDOS attack classification method

Ahmad Sanmorino  
Faculty of Computer Science, Universitas Indo Global Mandiri, Palembang, Indonesia  
*sanmorino@uigm.ac.id

Abstract. In this study, we discussed three DDoS attack classification methods based on machine learning. The comparison is done to measure the accuracy rate of each machine learning classification method in detecting DDoS attacks. The method of classification that is compared is the decision tree method, naive Bayes and artificial neural network. Based on the comparison of the performance of the classification method, the decision tree method reaches 83.9%, naive Bayes is 76.5% and artificial neural network reaches 84.3%. Based on this comparison, it can be concluded that the DDoS attack classification method using an artificial neural network has the highest accuracy compared to the other two methods.

1. Introduction
Distributed Denial of Service (DDoS) attacks is done to disable the target server. DDoS attacks are usually done in a massive and in a short time. There are several studies and methods that can be used to detect DDoS attacks, including methods based on IP flow [1]. This method uses five statistical features of IP flow. Another method of detection is by matching against attacks by hackers, this method known as matching pursuit algorithm [2]. The use of machine learning for classifying DDoS attacks has also been done by other researchers [3]. In the previous article, we have also proposed a DDoS attack detection method using SOM and pattern of the flow [4]-[5] algorithm. Due to a very large scale of attacks, DDoS attack detection methods can be targeted for a particular environment. As some researchers have done, it is proposing a DDoS attack classification method for cloud computing environment [6]-[8]. The purpose of classification is to distinguish between legitimate packages and packets came from DDoS attacks.

There are several machine learning algorithms such as Support Vector Machines, Decision Trees, Artificial Neural Networks, Genetic Algorithms, k-means, AdaBoost, Apriori, Cluster Analysis, C4.5, k-nearest neighbours, Naïve Bayes, and PageRank. In this study, we only compare the performance of three machine learning algorithms in classifying DDoS attacks. The three comparable algorithms are Decision Tree, Naïve Bayes, and Artificial Neural Network. The selection of these three algorithms is not because it is better than the other algorithm, but rather the similarity of characteristics, so by studying these three algorithms already represent other machine learning algorithms. Through this study is expected to know the most appropriate classification algorithm to detect DDoS attacks.

2. Methodology
The data used in this study is secondary data that has been collected by other researchers. There are many online data banks that provide network traffic that can be directly used. Here is one sample data that can be used for the study of DDoS attack detection. The sample data is still raw or unclassified (Table 1).
The raw network traffic data above consists of five variables ie time(s), IP address of the sender, data flow, number of packages and bytes per packet sent. To be used as a sample, raw network traffic data must be sorted out first based on the pattern of changes that occur on the network. Another alternative that can be used is the use of real traffic data obtained from DDoS attacks simulation. Simulation can be done in peer to peer, one computer as a server, and the other as the attacker. The tools can be used in simulations to perform DDoS attacks such as Slowloris. But to get results that are close to reality required a lot of computer data sources. If this cannot be met, then another alternative that can be used is to use sample data that has been collected by third parties.

The comparison method of machine learning algorithm in classifying DDoS attacks by measuring the performance of each algorithm. The measurement of machine learning algorithm performance is assessed based on predictive accuracy, since usually; the data used are imbalanced, with varying error rates [9]. Machine learning performance measurements range from two thresholds, true positive and true negative, recall and precision [10]. The receiver operating characteristic (ROC) curve shows the value between false negative and false positives in the graphical representation for each possible cut-off. The performance of the machine learning method is determined by four things, true positive \((TP)\), false positive \((FP)\), true negative \((TN)\), and false negative \((FN)\) [11]. In the case of DDoS attack classification, these four values have the following definition, \(TP\) is the number of DDoS packages detected as DDoS packages. \(FP\) is the number of legitimate packages detected as DDoS packages. \(TN\) is the number of legitimate packages that are detected as legitimate packages. \(FN\) is the number of DDoS packages that are detected as legitimate packages. These four values are accurate in classifying DDoS attacks (Eq. 1). Accuracy DDoS attack classification is a measure of machine learning algorithm performance in distinguishing legitimate packets and DDoS packages.

\[
\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \times 100\%
\]

(1)

In addition to accuracy, the alternative of performance measurement of machine learning classification is:

\[
\text{Precision} = \frac{TP}{TP + FP}
\]

(2)

Precision (Eq. 2) is used to determine the rate of accuracy between user expectations and the results given by the method used.
While recall (Eq. 3) is the success rate of the machine learning method in classifying DDoS attacks.

\[
\text{Recall} = \frac{TP}{TP + FN}
\]  

(3)

F-measure (Eq. 4) shows the reciprocal relationship between precision and recall. F-Measure is the harmonic mean of recall and precision.

\[
F\text{-measure} = \frac{2 \times \text{precision} \times \text{recall}}{\text{precision} + \text{recall}}
\]  

(4)

F-measure (Eq. 4) shows the reciprocal relationship between precision and recall. F-Measure is the harmonic mean of recall and precision. The best performance comparison of machine learning classification method is Receiver Operating Characteristics (ROC). ROC is a summary of the performance of the calculation of true positive (TP) and false positive (FP). The area under the curve (AUC) is an acceptable performance matrix for the Receiver Operating Characteristic (ROC) curve. On the ROC curve, ROC plots the curve with the x-axis to represent the percentage (%) of the false positive (FP) and plot the curve with the y-axis to represent the percentage (%) of the true positive (TP). The ideal value on the ROC curve is at intervals 0.100 [12].

Next will be explained the machine learning classification method that will be compared.

\[\text{a. Decision Tree}\]

The decision tree is a machine learning classification method that is easy to implement and widely used. One of the factors why a decision tree is widely used because it can handle high dimension data and does not require parameter or domain knowledge [13]. Decision Tree is a structure where each part of a tree represents the attributes that have been tested, each branch is a division of test results, and leaf nodes represent a certain class of groups. The top node level of a Decision Tree is called the root node which is usually in the form of attributes that have the most influence on a particular class. In general, the Decision Tree performs a top-down search strategy for the solution. In the process of classifying uncertain data, attribute values will be tested by tracking the path from the root node to the final node (leaf).

The decision tree is a non-parametric supervision classification method. The following is a simple example of a decision tree that can be used for classification (Figure 1).

\[
\text{Figure 1. Simple Decision Tree for Classification}
\]
b. Naïve Bayes
The probability applied in the Naïve Bayes algorithm is to examine the possible possibility of some indication $S$ with the highest posterior probability distribution, given some observation or prognosis $x$ where there is a dependence relationship between $S$ and $x$, denoted as $P(S \mid x)$, and posterior probability distribution can be calculated as shown in Eq. 5.

$$p(S \mid x) = \frac{p(x \mid S)p(S)}{p(x)} \alpha p(x \mid S)p(S)$$  

The Naïve Bayes model forms a network of interconnected nodes with directed edges and forms directed acyclic graphs [14], used to model dependencies among variables [15].

c. Artificial Neural Network
The definition of an artificial neural network is a computational system as a solution to problems that imitate how neural networks work in the brain. The following is an example of an artificial neural network diagram (Figure 2).

![Artificial Neural Network Diagram](image)

**Figure 2.** Artificial Neural Network for Classification

The artificial neural network consists of three main layers, the input layer, hidden layer and the output layer. In the hidden layer usually has more than one layer. The value problem of each gradient approaching the zero value of each layer when approaching the output layer can be solved by sorting or extracting important features. Then look again at the result, whether still relevant or not.

The method that can be used to compare the performance of machine learning algorithms is the method of cross-validation or cross-evaluation. This test method is often used by researchers to compare the accuracy of machine learning classification methods. Cross-validation is a method of testing that is done repeatedly, usually 0-9 folds. The test was carried out gradually starting from 4-fold ($k$-4), 6-fold ($k$-6), 8-fold ($k$-8), and 10-fold ($k$-10/\text{max}$). The more repetitions of tests performed (10 fold), the better the comparison results obtained.

3. Result and Discussion
Table 2 shows the comparison of the three machine learning methods. The result of the comparison is also obtained from the calculation that has been done by other researchers.
Table 2. Algorithms Performance Comparison

| Performance Metrics     | Decision Tree (%) | Naive Bayes (%) | Artificial Neural Network (%) |
|-------------------------|-------------------|----------------|-----------------------------|
| True Positive (TP)      | 84.0              | 76.6           | 84.5                        |
| False Positive (FP)     | 22.2              | 35.3           | 22.8                        |
| Precision               | 83.9              | 78.9           | 84.6                        |
| Recall                  | 84.0              | 76.6           | 84.5                        |
| F-Measure               | 83.9              | 74.8           | 84.2                        |
| ROC/AUC                 | 84.3              | 81.3           | 86.8                        |

Can be seen based on the comparison of artificial neural network classification method has a better performance metrics value than the other two. With a True Positive (TP) rate of 84.5%, the false positive (FP) rate is only 22.8%, the precision rate is 84.6%, the recall reaches 84.5%, f-measure 84.2%, and ROC area reach 86.8% (Figure 3). The true positive (TP) value is the number of legitimate packages detected as legitimate packages. The higher the true positive rate, the better. While the false positive (FP) value is the number of legitimate packages that are detected as DDoS packages. The lower the false positive rate, the better and vice versa.

Figure 3. Algorithms Performance Comparison

This shows the artificial neural network can be used for DDoS attack classification because of several things: First, a DDoS attack pattern is unpredictable, always changing and has no clear parameters. Second, The more data packets enter, the higher the difference rate. In this case, the other two methods can still handle it, but the right choice is to use the artificial neural network. We do not say that the other two methods are not good, but for the case of DDoS attack classification based on the comparison results (table 2), the artificial neural network method is the best in accuracy.

4. Conclusion
Based on the comparison of machine learning algorithm performance that has been discussed, can be seen artificial neural network has the best accuracy rate, compared with two other methods. The accuracy rate of the artificial neural network algorithm reached 84.3%. So it can be concluded for the classification case of DDoS attacks, the use of an artificial neural network method is the right choice. But we recognize that there are other external factors and maybe something amiss that may have contributed, so more in-depth research and testing is needed to get better results.
References

[1] Y. Feng, R. Guo, D. Wang, and B. Zhang, “Research on the Active DDoS Filtering Algorithm Based on IP Flow,” in 2009 Fifth International Conference on Natural Computation, IEEE, pp. 628–632, 2009.

[2] D. Erhan, E. Anarım, G. K. Kurt, “DDoS attack detection using matching pursuit algorithm,” 2016 24th Signal Processing and Communication Application Conference (SIU), 2016.

[3] M. S. Hoyos, G. A. Isaza, J. I. Vélez, O. L. Castillo, “Distributed Denial of Service (DDoS) Attacks Detection Using Machine Learning Prototype,” In: Omatu S. et al. (eds) Distributed Computing and Artificial Intelligence, 13th International Conference. Advances in Intelligent Systems and Computing. Springer, vol 474, 2016.

[4] Sanmorino, S. Yazid, "DDoS Attack detection method and mitigation using pattern of the flow," IEEE International Conference of Information and Communication Technology, 2013.

[5] Sanmorino, R. Gustriansyah, "An alternative solution to handle ddos attacks," Journal of Theoretical and Applied Information Technology, Vol. 96, No. 3, 2018.

[6] R. Kumar, S. P. Lal, A. Sharma, “Detecting Denial of Service Attacks in the Cloud, Dependable, Autonomic and Secure Computing,” 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress, IEEE, 2016.

[7] B. B. Gupta, O. P. Badve, “Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment,” Neural Comput Appl, Springer, pp. 1-28, 2016.

[8] K. Borisenko, A. Smirnov, E. Novikova, A. Shorov, “DDoS Attacks Detection in Cloud Computing Using Data Mining Techniques,” Industrial Conference on Data Mining ICDM 2016: Advances in Data Mining. Applications and Theoretical Aspects pp 197-211, 2016.

[9] N. V. Chawla, K. W. Bowyer, L. O. Hall and W. P. Kegelmeyer, "SMOTE: Synthetic Minority Over-sampling Technique," Journal of Artificial Intelligence Research, p. 321–357, 2002.

[10] Chao, A. Liaw and L. Breiman, "Using random forests to learn imbalanced data," University of California, Berkeley, 2004.

[11] S. Deepa and V. Bharathi, "Textural Feature Extraction and Classification of Mammogram Images using CCCM and PNN," IOSR Journal of Computer Engineering (IOSR-JCE), vol. 10, no. 6, pp. 07-13, June 2013.

[12] N. V. Chawla, K. W. Bowyer, L. O. Hall and W. P. Kegelmeyer, "SMOTE: Synthetic Minority Over-sampling Technique," Journal of Artificial Intelligence Research, p. 321–357, 2002.

[13] M. E. Anbarasi, Anupriya and N. C. S. N. Iyengar, "Enhanced prediction of heart disease with feature subset selection using genetic algorithm," International Journal of Engineering Science and Technology, vol. 2, no. 10, pp. 5370-5376., 2010.

[14] K. Aftarczuk, "Evaluation of selected data mining algorithms implemented in Medical Decision Support Systems," Blekinge Institute of Technology School of Engineering, Blekinge, 2007.

[15] S. Floyd, "Data Mining Techniques for Prognosis in Pancreatic Cancer," 2007.