Ilkogretim Online - Elementary Education Online, 2021; Vol 20 (Issue 5): pp. 7894-7899
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.05.894

Ddos Attack Prediction Using Voting Classifer

Varun Sharma , Research Scholar: Department of Computer Science, Desh Bhagat University, Mandi Gobindgarh, India

Dr. R.K. Bathla , Professor: Department of Computer Science, Desh Bhagat University, Mandi Gobindgarh, India

E-mail**:** rajav20@yahool.com, prof.bathla@gmail.com

Abstract

DDOS attack causes the distortion in performance of wireless sensor network. Sensor energy decays quickly by the applications of the DDOS attack. Distribute denial of service causes the performance delays by deadlock. Deadlock causes the resource block and hence no process or client can access the resources over the network. This paper proposed an ensemble of algorithms to detect DDOS attack with high classification accuracy. For the detection process, we will use KNN, naïve bayes and support vector machine. The ensemble of algorithm known as voting classifier is proposed that takes all the algorithms and produce the result according to effective properties of each ensembled algorithm. This result of the ensemble-based approach in terms of classification accuracy is 99% which is significantly higher as compared to individual approaches.

Keywords: DDOS, KNN, Naïve Bayes, SVM

I. Introduction

DDOS attack is perhaps one of the most critical issues that hamper the performance of the wireless sensor network. Not only WSN but it also has devastating effects on cloud-based environment as well. In this work primary area of concern is wireless sensor network. The effect of DDOS on WSN are listed as under

- DDOS attack causes the deadlock in resource access and hence both time and cost increases in the availability of resources.
- Service provider in this competitive world will be many. DDOS attack could cause the distortion in reliability of service provider.
- Energy decays could lead to decrease in lifetime of the network.
- Packet drop ratio also increase due to deadlock caused by DDOS

Nodes causing DDOS attack ensures multiple packets to be transmitted over small period. These packets are generally more as compared to bandwidth of the media used. This causes congestion and ultimately traffic jam on network. This means resource requests are not transmitted to the destination nodes and denial in service requests as discussed in [1][2].

Technology advancements allows easy detection of DDOS, but techniques used generally does not have that much classification accuracy. The algorithms that are followed in this work have good classification rates, but as large datasets are deployed, classification accuracy decays. These algorithms are discussed within [3][4].

Rest of the paper are discussed as under. Section ii gives the insights into KNN, Naïve bayes, SVM and linear regression. section iii presents the proposed methodology. Section iv gives the result and performance analysis. Section v gives the conclusion. Last section gives the references.

ii. Algorithms for DDOS detection

algorithm considered for evaluation are discussed along with results obtained. The dataset derived from the UCI machine learning website corresponding to the DDOS attack. The link for the same is UCI Machine Learning Repository: Dishonest Internet users Dataset Data Set. The attributes of the dataset are describe in table 1

Table 1: Attributes within dataset

Attribute	Description
Eij	It indicates i^{th} node interaction with j^{th} node
EIDs	Entity identification
CT	Counting trust
CU	Counting untrust entities
LT	It indicates last time interaction of entity
TC	Transaction Context
TS	Trust score that must be high in case entity is not attacker

Since all the attributes within the dataset cannot be used for prediction so only following attributes are considered for DDOS attack prediction.

Table 2: relevant attributes

Attribute	Description
CT	Counting trust
CU	Counting untrust entities
LT	It indicates last time interaction of entity
TC	Transaction Context
TS	Trust score that must be high in case entity is not attacker

The relevant attributes first applied to predict DDOS through KNN approach. This approach is described as under

A. KNN

This mechanism is a nearest neighbor approach used to form the clusters of values that fall within threshold limit[5][6]. Threshold limit is specified with K. Checking packet transmission is critical phase within KNN. This is accomplished with the help of trust score. The algorithm used for KNN for abnormal pattern detection and DDOS prediction is given as under

KNN(Dataset)

- Input dataset
- Input value of K
- Initialize z=0
- For i=1:n
  If $\sqrt{(x - x_i)^2 + (y - y_i)^2}$<K then
  Gr[z]=i
  Else
  z=z+1
  End of if
  End of for
- For i=0:z
  If(TS>score(Gz[i])) then
  Predict DDOS
  End of if
  End of for
- Output classification accuracy

When applied to the dataset, good result in terms of classification accuracy was generated. 87% classification accuracy indicates room for improvement.

B. Naïve bayes approach

In this approach mining base NB approach was applied on the dataset. The approach yield bit better result as compared to KNN approach. The NB approach to detect DDOS is popular classification mechanism that helps to classify the data based upon the conditional probability. It is based on bayes theorem and used class levels as feature vectors. This mechanism is used for predicting text classification and sentiment analysis[7][8]. In addition, it is also useful in multi class predictions. With this approach, it is possible to calculate the posterior probability P(c(x)) using the previous probability values P(c). The probability of predictor class also termed as likelihood denoted by P(x|c) is calculated as

$$P(c|x) = (P(x|c) * P(c))/P(x)$$

The result of this approach is better in terms of classification accuracy. This classification accuracy is improved by 3% and actual magnitude of accuracy obtained is 90%.

C. SVM

Support vector machine is one of the most important approach used to detect DDOS attack. The DDOS attack detection in this approach is based upon the hyperplane's formation. Dataset used for DDOS detection is 2 dimensional[9]. Using SVM we can expand 2-dimensional dataset into 3-dimensional space. Formed vectors are generally denoted with named alphabet. The magnitude for n-dimensional vector in SVM is denoted as under

$$||x|| = \sqrt{x_1^2 + x_2^2 \pm - - - - - \mp x_n^2}$$

Different vectors will form different hyperplanes. Every hyperplane will be assigned different weight. The obtained vector magnitude values will be compared against the hyperplane threshold value. Matched hyperplane magnitude value gives attacker or non attacker nodes. The classification accuracy of this approach appears to be 95%.

iii. Proposed methodology

the proposed methodology combines the best possible features from the different approaches including SVM, KNN and Naïve bayes to produce ensemble algorithm. The algorithm for the same is given as under

Voting_Ensemble

```
from sklearn.ensemble import VotingClassifier
models =
[('RF',RandomForestClassifier()),('gnb',GaussianNB()),('knn',KNeighborsClassifier()),('lr',L
ogisticRegression(solver='lbfgs', max_iter=1000)),('svm',svm.SVC())]
ensemble = VotingClassifier(estimators=models)
ensemble.fit(Xtrain,ytrain)
y_pred=ensemble.predict(Xtest)
print(y_pred)
```

iv. Performance analysis and Results

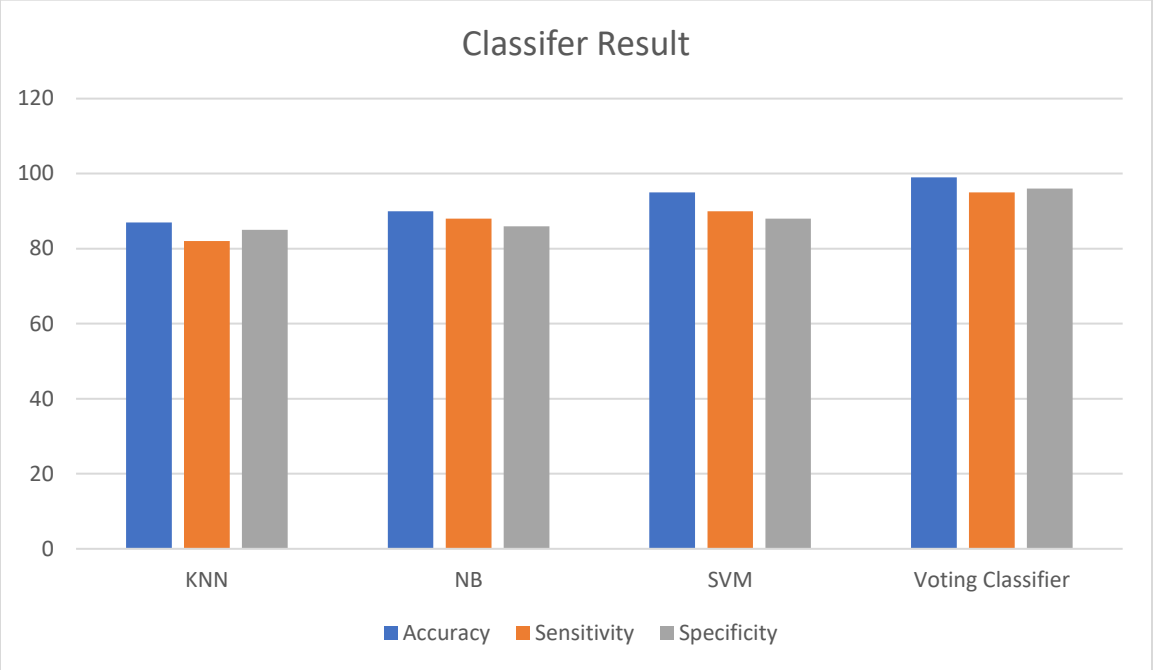
The results of the proposed mechanism using voting classifier is much better as compared to KNN, SVM and naïve bayes. The result of the voting classifier is expressed in terms of classification accuracy, specificity, and sensitivity. Table 3 shows the result in terms of classification accuracy., specificity and sensitivity

Table 3: Result in terms of accuracy , sensitivity and specificity

Classifier	Accuracy	Sensitivity	Specificity
KNN	87	82	85
NB	90	88	86
SVM	95	90	88
Voting Classifier	99	95	96

Plot for the table 3 is given in figure 1

Figure 1: Result in terms of classification accuracy, specificity and sensitivity



From figure 1 it is concluded that classification accuracy is improved significantly by the application of voting classifier.

v. Conclusion

The distributed denial of service attack must be identified at early stage to eliminate the devastating effect on the WSN medium. The existing approach including KNN, SVM and naïve bayes approach produce sufficient classification accuracy in the detection of DDOS attack but still room for improvement is present. The voting classifier deriving the properties from KNN, SVM and naïve bayes and then generates a voting classifier. The classifier that is best possible in terms of classification accuracy is further tuned to produce best accuracy values in terms of DDOS prediction. Voting classifier predicts the DDOS attack with 99% classification accuracy.

vi. References

[1] Y. Gu, K. Li, Z. Guo, and Y. Wang, "Semi-Supervised K-Means DDoS Detection Method Using Hybrid Feature Selection Algorithm," IEEE Access, vol. 7, pp. 64351–64365, 2019, doi: 10.1109/ACCESS.2019.2917532.

[2] H. D. Rajendra Patel, "Protocol specific Multi Threaded Network Intrustion Detection System(PM-NIDS) for DOS/DDOS Attack Detection in Cloud," IEEE, no. 1, pp. 430–439, 2018.

[3] A. Praseed and P. Santhi Thilagam, "DDoS attacks at the application layer: Challenges

and research perspectives for safeguarding web applications," IEEE Communications Surveys and Tutorials, vol. 21, no. 1. Institute of Electrical and Electronics Engineers Inc., pp. 661–685, Jan. 01, 2019, doi: 10.1109/COMST.2018.2870658.

[4] S. T. Zargar, J. Joshi, and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," IEEE Commun. Surv. Tutorials, vol. 15, no. 4, pp. 2046–2069, 2013, doi: 10.1109/SURV.2013.031413.00127.

[5] S. Dong and M. Sarem, "DDoS Attack Detection Method Based on Improved KNN with the Degree of DDoS Attack in Software-Defined Networks," IEEE Access, vol. 8, pp. 5039–5048, 2020, doi: 10.1109/ACCESS.2019.2963077.

[6] M. Aamir and S. M. A. Zaidi, "Clustering based semi-supervised machine learning for DDoS attack classification," J. King Saud Univ. - Comput. Inf. Sci., Feb. 2019, doi: 10.1016/j.jksuci.2019.02.003.

[7] K. J. Singh and T. De, "MLP-GA based algorithm to detect application layer DDoS attack," J. Inf. Secur. Appl., vol. 36, pp. 145–153, Oct. 2017, doi: 10.1016/j.jisa.2017.09.004.

[8] L. Barki, A. Shidling, N. Meti, D. G. Narayan, and M. M. Mulla, "Detection of distributed denial of service attacks in software defined networks," 2016 Int. Conf. Adv. Comput. Commun. Informatics, pp. 2576–2581, 2016, doi: 10.1109/ICACCI.2016.7732445.

[9] J. Ye, X. Cheng, J. Zhu, L. Feng, and L. Song, "A DDoS Attack Detection Method Based on SVM in Software Defined Network," Secur. Commun. Networks, vol. 2018, Apr. 2018, doi: 10.1155/2018/9804061.