İSTANBUL UNIVERSITY
CERRAHPAŞA

RESEARCH ARTICLE

Electrica 2020; 20(2): 159-167

Detection DDOS Attacks Using Machine Learning Methods

Tuğba Aytaç[1], Muhammed Ali Aydın[2], Abdül Halim Zaim[1]

[1]Department of Computer Engineering İstanbul Commerce University, İstanbul, Turkey
[2]Department of Computer Engineering, İstanbul University-Cerrahpaşa, İstanbul, Turkey

Cite this article as: Aytaç T, Aydın MA, Zaim AH. Detection DDOS Attacks Using Machine Learning Methods. *Electrica,* 2020; 20(2): 159-167.

ABSTRACT

Wishing to communicate each other of people contributes to improve technology and it has made the internet concept an indispensable part of our daily life. Cyber attacks that are from extranets to enterprise network or intranets which are used as personal can cause to pecuniary loss and intangible damages. It is critical to take due precautions for minimizing the losses by early detection of attacks. The aim of this study is analyzing the rate of success in intrusion detection system by using different methods. In this study, CICDDoS2019 data set has been used and DDOS attacks in this data set were compared and the success rates of threat determination were analysed as using Artificial Neural Networks (ANN), Support Vector Machine (SVM), Gaussian Naive Bayes, Multinomial Naive Bayes, Bernoulli Naive Bayes, Logistic Regression, K-nearest neighbor (KNN), Decision Tree (entropy-gini) and Random Forest algorithms. It has been seen that the highest of the success rate is the models which ensures almost 100% success that were made by using K-nearest neighbor, Logistic Regression, Naive Bayes, (Multinomial – Bernoulli algorithms).
Keywords: Machine learning methods, intrusion detection system, CICDDoS2019

Introduction

Internet which is an indispensable factor of our daily life with the improved technology takes a great space in banking, health, many other industries and in our social life. It is foreseen that almost 50 billion objects will be depended on the internet which is a network system until 2020 with ARPANET (Advanced Research Projects Agency Network) which appeared in 1969, ensures communicating the very little devices and provides a basis of internet [8].

Many systems or soft wares such as antivirus and firewall have been used for protecting the enterprise networks from malicious people but these measures can remain incapable to avert the attacks. Because some people who want to lose our reputation or financial gain and work as a team always try to find the weaknesses for detecting the deficits in systems.

It is very important to early detecting the attacks for systems and preventing it. Intrusion Detection Systems (IDS) are software or hardware constituents which have qualification an "alarm" for protecting the information systems toward the attacks from network. IDS can prevent the attempts to entering the systems by detecting the misusing and unauthorized accesses to systems [13].

There are two different methods for IDS design [19]. These two approaches are signature recognition based system which determines with the private characters for every behavior and the system which determines the attacks with examining the abnormal network traffic on networks. The primary aim of these two approaches is to keep definite attacks in quarantine for making the determining of attacks as close to real-time and eliminating the damage which caused by attacks [11].

The aim of this study is to design the establisher system in overachievement rate as earliest as possible with the machine learning methods of DOS attacks. Machine learning methods from Anomaly Based Attack Determiner Systems data set were used in this study and the education had been done in those data sets. It was aimed to find the fastest determination values with the overachievement rate by composing quadruplet, sestet, octuplicate, denary and duodenary data sets. It is important to determine the attack as keeping narrow of attribute values in terms of the performance of IDS.

Corresponding Author:
Tuğba Aytaç

E-mail:
tugba.aytac@istanbulticaret.edu.tr

Received: 15.05.2020

Accepted: 25.05.2020

DOI: 10.5152/electrica.2020.20049

Content of this journal is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Intrusion Detection Systems

Gradually increasing of using internet with improving the information technologies and taking place in a depended network together of systems raise the needs of making provision against the attacks which can come from the outside. Attacks can be identified as being precluded of a system's privacy, integrity or accessibility. Intrusion detection systems are the systems which were designed to recognize the attacks towards the smart systems which are in the same network that are used by corporate firms, companies or governments (computer, tablet, mobile phone, etc.) that can damage the systems in network which can come from internet or local area network, which are composed of various packets and unnecessary traffic density. And it is a security technology which aims to give an answer to those kinds of attacks [10].

Attacks can be determined as examined by two approaches. These two approaches are Anomaly Based Attack Determiner Systems (ABADS) and Signature Based Attack Determiner Systems (SBADS). While ABADS is determining the traffic which has a harmful content as a result of the analysis of network traffic, SBADS makes an examination on the basis of the previous data which were recorded on the system and confirms the attack.

Machine learning methods and studies on IDS

There are many studies about intrusion detection system which are made by machine learning methods which has the property of decision making and takes place in the subassemblies of artificial intelligence. Firstly anomaly based intrusion detection system which also machine learning methods take place in, identify the normal values then decide the incoming data are normal or abnormal and it can make classification.

The reason of being more preferred of our abnormal based intrusion detection system is the signature based intrusion detection system can be immobilized according to previous recorded values and being lower of the success rate and the determination time. In this part, the machine learning methods which were used in the work and studies about these methods were discussed.

Artificial neural networks

Artificial neural networks which take place in subassemblies of artificial intelligence are based on a smart algorithm which simulate to learning property and reflectiveness of people. It is composed of multilayer or single-layer constructs that created by neural networks method such as neural networks in human brain which ensure learnability and reflectivity. There are 5 parameters that produce artificial neural networks. These parameters are inputs, weights, addition functions, activation function and outputs [3]. The construct of artificial neural networks is seen in Figure 1.

The highest success rate, 97.92 %, was attained in dos attacks (Smurf, Neptune, Back, Teardrop) rl2 and probe attacks by using artificial neural networks KDD'99 data set. It was seen that we can attain true results with the quite low error rate by using test sets and different education thanks to YSA method in study [13].

Murat H. Sazlı and Haluk Tanrıkulu trained DARPA data sets as generating multilayer artificial neural networks with "Neural Network Tools Box" in MATLAB program on their studies. They procured to immobilizing of Dos attacks with the high success rate via well designed attack determination system [15].

The reason of being preferred YSA methods in IDS works is having many advantages such as high categorizing ability of the subject method, making inference for new data from previous learning, completing the imperfect knowledge data and learning new cases. Absence of composing artificial neural networks rules, taking a long time for learning due to making a lot of trying are its disadvantages.

Naive bayes algorithm

Naive Bayes which is a classification algorithm according to data category takes its name from Thomas Bayes (1701 - 7 April 1761). Its success rate is quite high since Naive Bayes algorithm transclude the highest rate value into categorization by calculating the whole probabilities. If the using data have multiple class Multinomial Naïve Bayes, if there is a normal distribution in data Gauss Naïve Bayes, if making forecasts is being wanted dually Bernoulli Naïve Bayes can be preferred. Besides its advantages such as fast resulting, working with data which can show high rate reality and variability, inability for modeling of the relations between variables is its disadvantage [9].

In attack determination system which made via Naïve Bayes algorithm by using KDDCup'99 data set, detecting the attacks system in 1.89 seconds with 95% success rate achieved and it was shown that KNN (K-means clustering algorithm) and YSA methods are better [12].

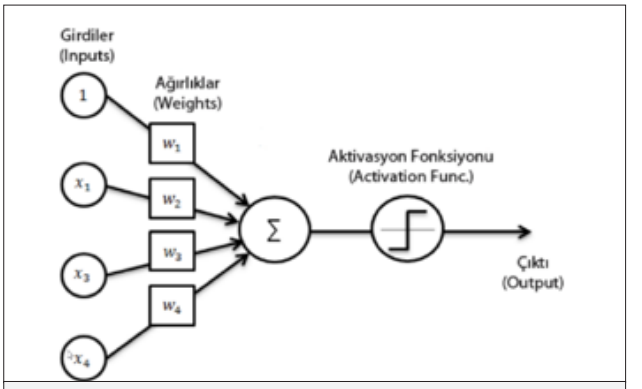


Figure 1. The construct of artificial neural set cell

Table 1. The best attributes and success rates among the results

Property	**Explanation**
Best Values with 4 Property (Success rate: 0,993%)	
Tot Fwd Pkts	Total number of packets in the forward direction
Tot Len Bwd Pkts	Total length of packets in the backward direction
Bwd IAT Mean	Average time between two packets sent backwards
Fwd Seg Size Min	Minimum size observed forward
Best Values with 6 Property (Success rate: 0,994%)	
Bwd Pkt Len Std	Standard deviation of packet lengths in the backward direction
Flow IAT Max	Maximum arrival time of the packets
Pkt Len Min	Minimum length of a stream
Down/Up Ratio	Download and upload rate
Fwd Byts/b Avg	Average number of bytes forwarded
Fwd Seg Size Min	Minimum size observed forward
Best Values with 8 Property (Success rate: 0.973)	
Bwd Pkt Len Max	Maximum length of packets in the backward direction
Flow IAT Std	Standard deviation of arrival times of packets
Flow IAT Min	Minimum arrival time of packets
Fwd IAT Tot	Total time between two forward packets
Bwd IAT Std	Standard deviation of time between two packets sent backwards
Fwd Pkts/s	Number of forward packets per second
Pkt Len Std	Standard deviation of a stream
SYN Flag Cnt	Number of packets containing SYN
Best Value with 10 Property (Success rate: 0.979)	
Fwd Pkt Len Mean	Average length of forward packets
Bwd Pkt Len Min	Minimum length of forward packets
Bwd Pkt Len Mean	Average length of backward packets
Fwd IAT Max	Maximum time between two forward packets
Bwd PSH Flags	Number of active PSH flag in packets moving backwards (0 for UDP)
Fwd Pkts/s	Number of forward packets per second
FIN Flag Cnt	Number of packages containing FIN
SYN Flag Cnt	Number of packages containing SYN
PSH Flag Cnt	Number of packages containing PUSH
Down/Up Ratio	Download and upload rate
Best Values with 12 Property (Success rate: 0,998)	
Bwd Pkt Len Min	Minimum length of back packets
Flow Pkts/s	Number of packets flowing per second
Flow IAT Min	Minimum arrival time of packets
Fwd IAT Tot	Total time between two forward packets
Bwd IAT Std	Standard deviation of time between two packets sent backwards
Fwd URG Flags	Number of active URG flag in packs moving forward (0 for UDP)
Fwd Header Len	Total bytes used for forward header
Bwd Header Len	Total bytes used for backward headers
Bwd Pkts/s	Number of backward packets per second
Subflow Bwd Pkts	Average number of packets in a backward downstream
Fwd Act Data Pkts	Number of packets with at least 1 byte of TCP data carrying capacity
Fwd Seg Size Min	Minimum size observed forward

It was provided to determine the DDOS attacks on Web of Shital K. Ajagekar and Vaishali Jadhav in the range of 79%-99.5% by categorizing with Multinomial NB algorithm and the highest rate success was gained in determining HTTP-flooding attack [4].

K the nearest neighbor algorithm (KNN)

It is an algorithm which calculating the proximity of attribute of the previous k quantity of the new attributes on the phase of the classifying of attributes which data have. By choosing different attributes with NSL-KDD data set, kNN-1, kNN-2, J-48 and Naive Bayes algorithms had been tried. It is seen that the highest success rate obtained from on qualified and original data set PCA 21 with kNN-1, J-48 algorithms [1].

(Decison tree) algorithm

Classifying method decision nodes which made by using decision tree algorithm is composed of cut sheet and axis. Decision nodes or cut sheets occur depending on whether the classifying materialized or not. Attack determination had been done via decision tree algorithm with the 99% high success rate in a study which made by using CICIDS2017 data set. It was seen that Denial of Service (Dos), Spanned Service Rejection (DDOS) and Port Scanning (Port Scan) in data set are seen as abnormal and 78 traffic properties were used to determine it [2].

(Random forest) classifying algorithm

Random forest classifying is a community classifier which produces multi decision tree by using subset of variables and selection education [6]. LGBM, CNN and Random Forest methods which achieved by using CSE-CIC-IDS2018 data set had been tried and it was seen that bi-level hybrid construct which created by random forest model has the highest success with the 0.86 F-score macro avg [5].

Support vector machines (SVM)

Support Vector Machines algorithm is an algorithm which is used for distinguish two classes ideally on the base. Wani and his friends determined DDOS attacks on cloud computing context by using SVM, Random Forest and Naïve Bayes methods on their works in 2019. The most successful result was taken from SVM algorithm with 0.998 F-score by using 9 attributes within data cluster which was created for study [17].

Table 2. Algorithms used for ddos attack detection, success rates and detection times

Algorithm used for training	Success Rate (%)	Detection Time (sn)
Logistic Regrasyon	99,8	788
Gaussian Naive Bayes	98,7	1041
k-nearest neighbor	99,9	1040
Multinomial Naive Bayes	99,1	1041
Bernoulli Naive Bayes	99,8	1042
Decision Tree(entropy)	99,12	1043
Decision Tree(gini)	99,34	1043
Random Forest	98,4	1047
SVM	99,7	1074

Table 3. Algorithms detection times and success rates

Property	Explanation
Tot Bwd Pkts	Total number of packets in the backward direction
Fwd Pkt Len Min	Minimum length of forward packets
Bwd Pkt Len Min	Minimum length of backward packets
Bwd Pkt Len Mean	Average length of backward packets
Flow Byts/s	Number of bytes flowing per second
Flow Pkts/s	Number of packets flowing per second
Flow IAT Std	Standard deviation of arrival times of packets
Bwd IAT Mean	Average time between two packets sent backwards
Fwd Header Len	Total bytes used for forward headers
Pkt Len Std	Standard deviation of a flow
Pkt Len Var	Length variance of a flow
CWE Flag Count	Number of packets containing CWE

Data Set

Many data sets are using in studies which are made with using different algorithms in Intrusion Detection System designs. CICDDoS2019 data set is the latest designed data set which was shared by Canada Cyber Security Institute, was prepared in a proper test context, was designed by having regard to imperfections in previous data sets [16].

Along with good natured and the latest DDOS attacks which are similar to real data (PCAP), CICDDoS2019 also include the result of network traffic analyses which uses CICFlowMeter-V3 that has labeled traffic justified to attack (CSV documents), time stamping, originator and target IPs, originator and target ports, protocols. There are some different DDOS attack kinds such as Port Map, NetBIOS, LDAP, MSSQL, UDP, UDP-Lag, SYN, NTP, DNS and SNMP in this data cluster [16].

Studies that made by using data set

Properties which subtrahend for choosing the best detection property from 80 properties in every DDOS attacks which take place in the first study data set with producing CICDDoS2019 data set had been tested by using Random Forest Regressor. Finding the best properties to determine DDOS attacks with the 11 kinds new data sets in this study (15).

Adhibition

Good natured (benign) values and DDOS attacks that have 83 attributes had been examined with using CICDDoS2019 data set in this study. Since many values in data set such as space, string, port numbers were unavailable, they had been ejected via being subject to preprocessing and had been optimized for trainable with C and C++ programs. Ready data set had been created in such a way as to 77 attributes with 1 label that evaluating if there was an attack or not and 76 attributes which will be subjected to train within 83 attributes and in data set.

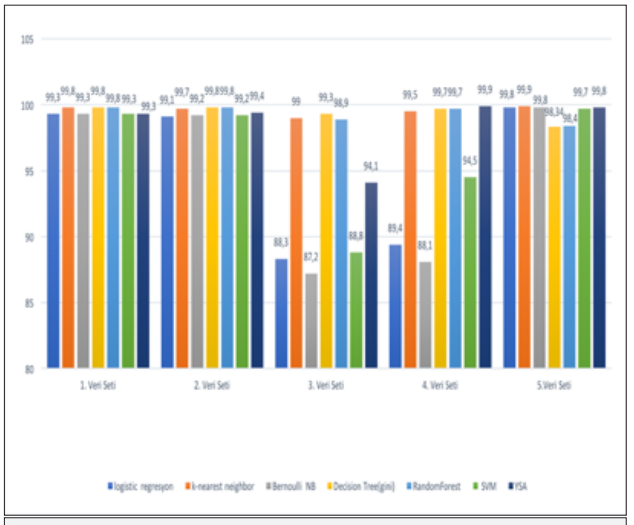


Figure 2. Graph for comparing the accuracy rates of algorithms

There are data which had 3 million housekeeping that belongs to DDOS attack and nondestructive data in Data Set. In total, having attribute values Fifty for each quad, octet, decimal and duodenary data sets which were chosen by Brute Force method, based upon subject data set had been created. Subject attribute values were subject to train firstly by Artificial Neural Network method that created in Pyhon Pycharm program.

When we check the properties and the success rate, determination of DDOS attack at the soonest possible date with the highest success rate had carried out with the values that have 4 quantities property.

With creating 500 thousand data sets which have each of 4, 6, 8, 10 and duodenary property had been trained by Gaussian Naïve Bayes, Multinomial Naive Bayes, Bernoulli Naive Bayes, Logistic Regression, K-nearest neighbor (KNN), Decision Tree (entropy-gini), Random Forest and SVM algorithms. Properties that determined the DDOS attack at the highest rate and in the shortest time as a result of train were shown in Table 2.

In the graphic in Figure 2, the algorithms and datasets with the highest success rate were included at the end of the training

It is seen that the most determinant feature in the detection of DDOS attack is the Fwd_Pkt_Len_Std feature in Figure 1 when the data is analyzed in the data set consisting of four properties and label values, which is the first data.

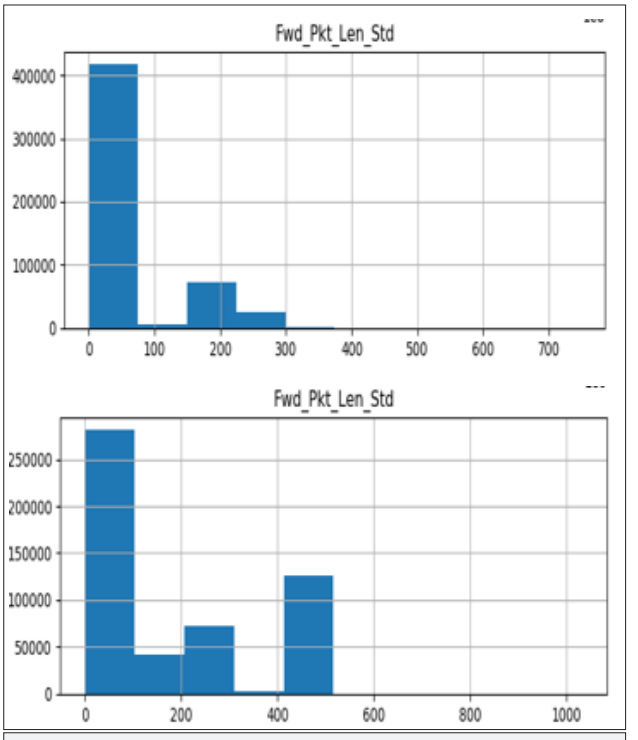


Figure 3. Graph of the best feature in the First Data Set

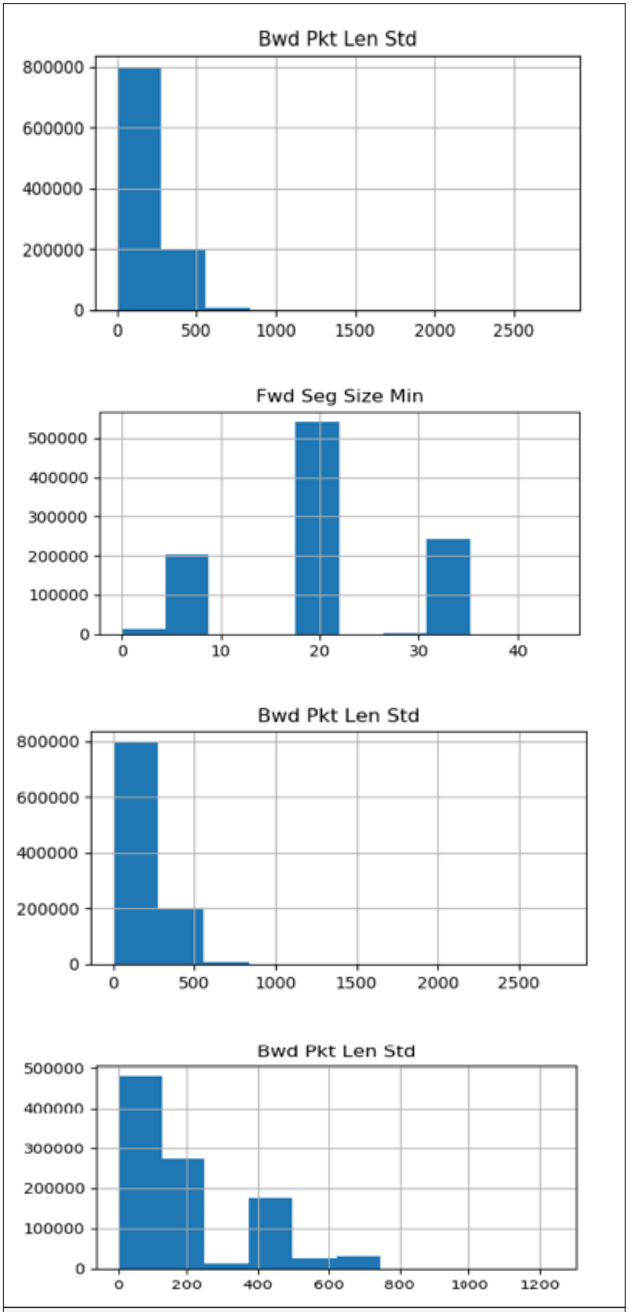


Figure 4. Graph of the best feature in the First Data Set

It is seen that the most determinant features in the detection of DDOS attack are the Fwd Seg Size Min and Bwd Pkt Len Std features in Figure 2 when the data is analyzed.

It is seen that the most determinant features in the detection of DDOS attack are the Bwd Pkt Len Min and CWE Flag Count features in Figure 3 when the data is analyzed.

The most determinant features in the detection of DDOS attack are Bwd Pkt Len Min and Bwd Seg Size Avg in Figure 4 when the data is analyzed.

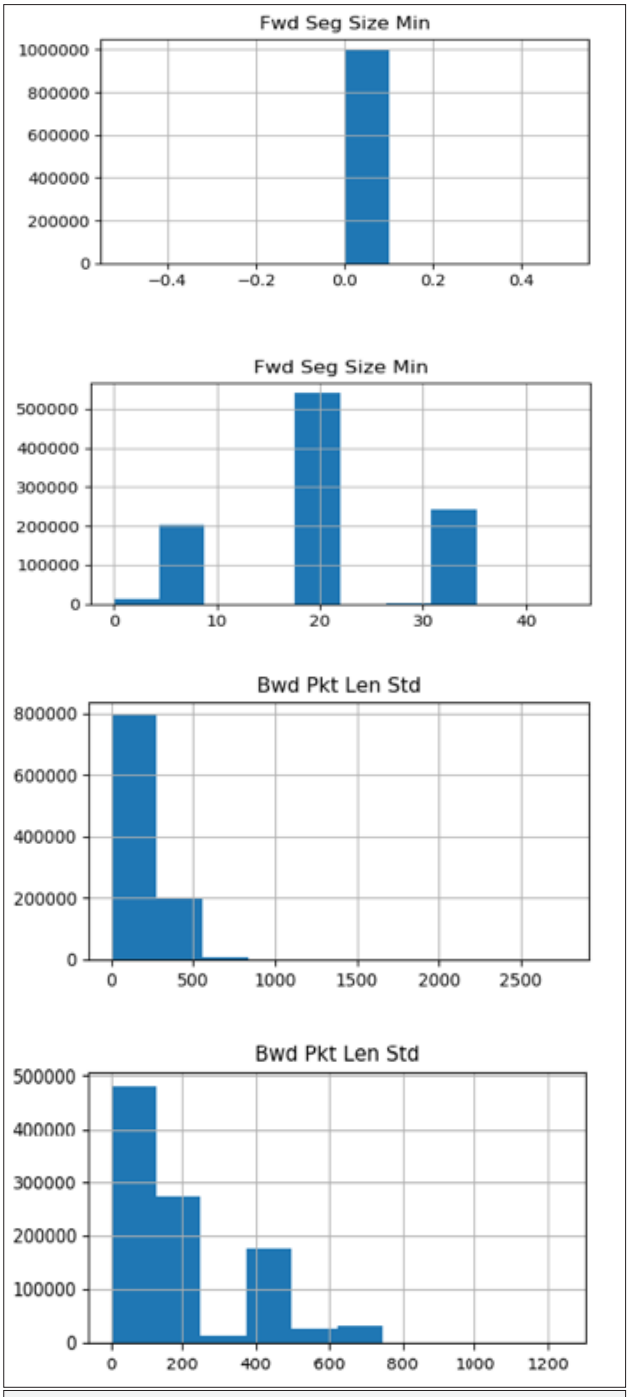


Figure 5. Graph of the best features in the third Data Set

The most determinant features in the detection of DDOS attack are Bwd Pkt Len Min and Bwd Seg Size Min feature in Figure 5 when the data is analyzed.

Conclusion

Data sets which have different 4, 6, 8, 10 and 12 properties and were taken fifty each quantity from every category in total by using Brute Force method for finding the best proper-

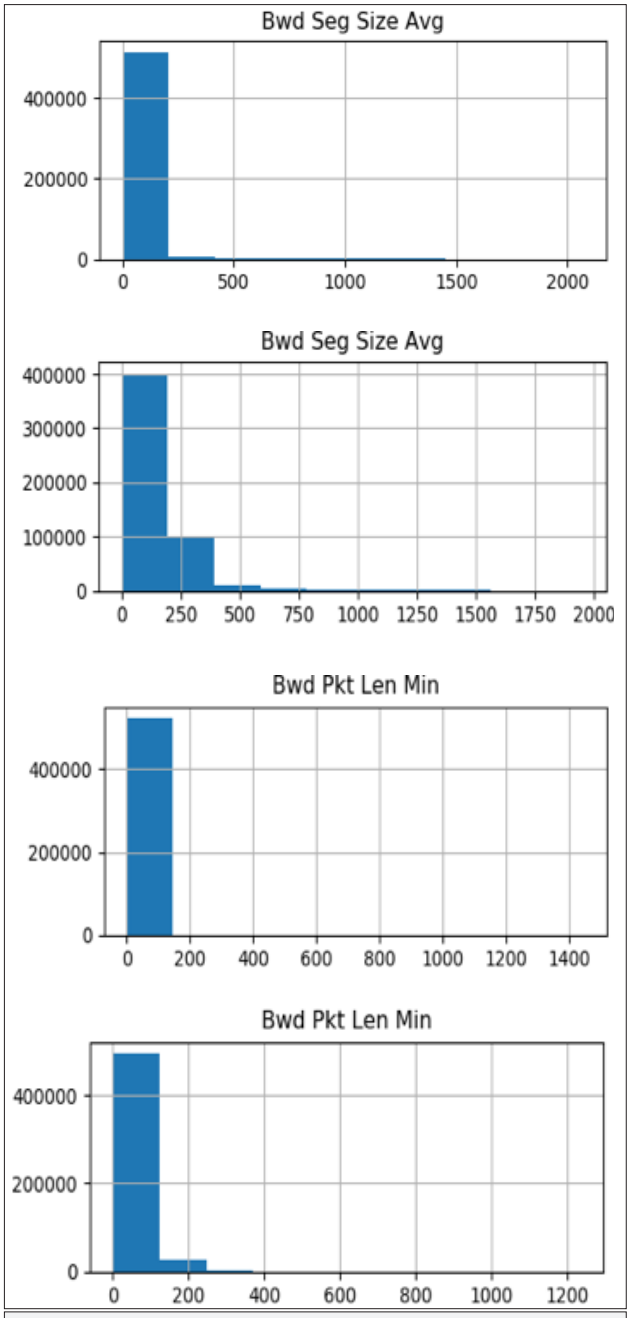


Figure 6. Chart of the best features in the fourth Data Set

ties in determining of attack types by using the best current data set CICDDoS2019.

Every data set had been trained by using YSA, Gaussian Naive Bayes, Multinomial Naive Bayes, Bernoulli Naive Bayes, Logistic Regression, K-nearest neighbor (KNN), Decision Tree (entropy-gini), Random Forest and SVM algorithms. The highest success rate of data sets which were used for training and test obtained by using K-nearest neighbor, Logistic Regression, Naive Bayes, (Multinomial - Bernoulli) algorithms.

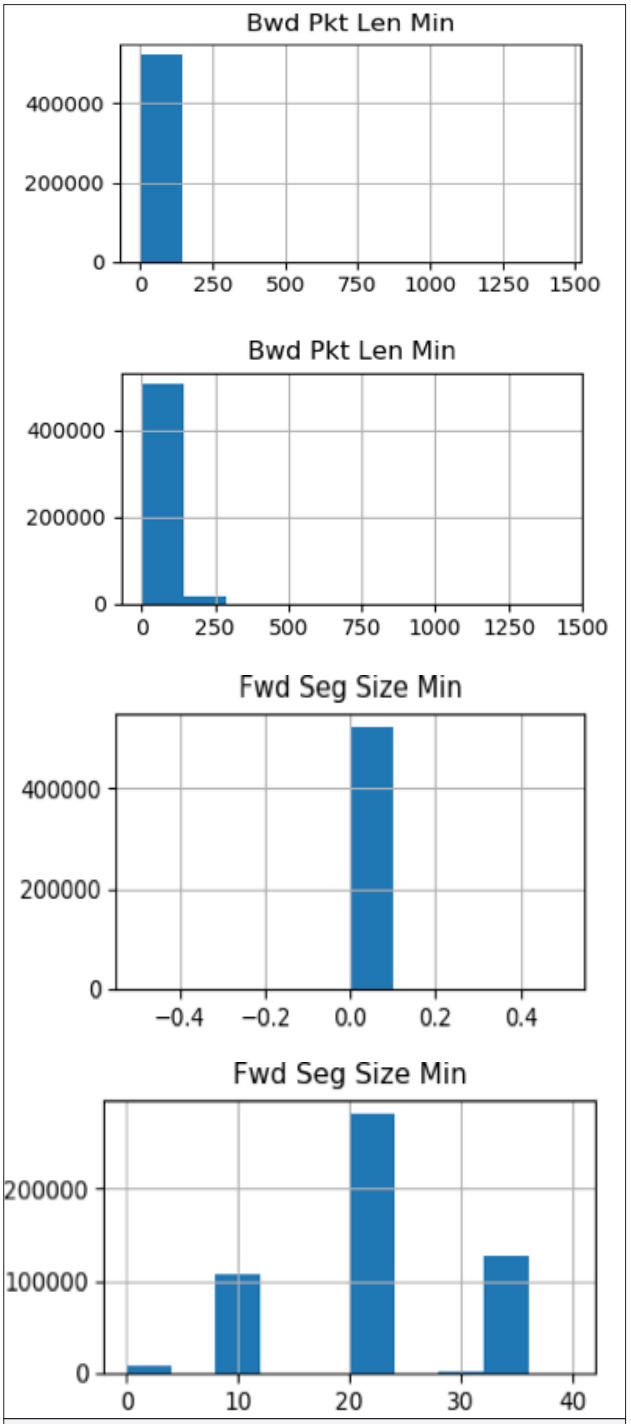


Figure 7. Graph of the best features in the fifth Data Set

When we consider the training and test period, attack determination was done by high rate as 99.7% attack with SVM algorithm and it was identified that its performance is the best.

By analyzing 5 data sets from which have the highest accuracy rate in data that have been trained with different algorithms, it was seen that Fwd Pkt Len Std, Fwd Seg Size Min,

Bwd Pkt Len Std, Bwd Pkt Len Min, CWE Flag Count, Bwd Seg Size Avg, Bwd Seg Size Min properties were the most distinct values for determination of DDOS attacks.

Peer-review: Externally peer-reviewed.

Conflict of Interest: The authors has no conflicts of interest to declare.

Financial Disclosure: The authors declared that the study has received no financial support.

References

1. Ü. Çavuşoğlu, S. Kaçar, "Anormal Trafik Tespiti için Veri Madenciliği Algoritmalarının Performans Analizi", Akademik Platform Mühendislik ve Fen Bilimleri Dergisi, vol. 7, no. 2, pp. 205-216, 2019.
2. S. Özekes, E. N. Karakoç, "Makine Öğrenmesi Yöntemleriyle Anormal Ağ Trafiğinin Tespit Edilmesi", Düzce Üniversitesi Bilim ve Teknoloji Dergisi, vol. 7, no. 1, pp. 566-576, 2019.
3. E. Öztemel, "Yapay Sinir Ağları", Papatya Yayıncılık, İstanbul, Turkey, 2006.
4. S. K. Ajagekar, V. Jadhav, "Study on Web DDOS Attacks Detection Using Multinomial Classifier" International Conference on Computational Intelligence and Computing Research (ICCIC), 2016, pp. 1-5.
5. R. Atay, D. E. Odabaş, M. K. Pehlivanoğlu, "İki Seviyeli Hibrit Makine Öğrenmesi Yöntemi ile Saldırı Tespiti", Gazi Mühendislik Bilimleri Dergisi, vol. 5, no. 3, pp. 258-272, 2019.
6. M. Belgiu, L. Draguţ, "Random Forest in Remote Sensing: A Review of Applications and Future Direction", ISPRS Journal of Photogrammetry and Remote Sensing, vol. 114, pp. 24-31, 2016.
7. Canadian Institute for Cybersecurity, DDoS Evaluation Dataset (CICDDoS2019), 2019. Available: https://www.unb.ca/cic/datasets/ddos-2019.html
8. D. Evans, "The Internet of Things How the Next Evolution of the Internet Is Changing Everything", CISCO, 2011.
9. E. Hatipoğlu, "Machine Learning — Classification — Naive Bayes — Part 11", Medium, 2018. Available: https://medium.com/@ekrem.hatipoglu/machine-learning-classification-naive-bayes-part-11-4a10cd3452b4
10. İTUBİDB, "Saldırı Tespit Sistemleri", 2013. Available: https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/sald%C4%B1r%C4%B1-tespit-sistemleri
11. R. Kraur, M. Singh, "Efficient Hybrid Technique for Detecting Zero-Day Polymorphic", In 2014 IEEE International Advance Computing Conference, 2014.
12. IACC, IEEE, pp. 95-100.
13. M. Panda, P. M. Ranjan, "Network Insrusipn Detection Using Naive Bayes". International Journal of Computer Science and Network Security, vol. 7, no. 12, pp. 258-263, 2007.
14. Ş. Sağıroğlu, E. N. Yolaçan, U. Yavanoğlu, "Zeki Saldırı Tespit Sistemi Tasarımı ve Gerçekleştirilmesi", Journal of the Faculty of Engineering & Architecture of Gazi University, vol. 26, no. 2, pp. 325-340, 2011.
15. I. Sharafaldin, A. H. Lashkari, S. Hakak, A. A. Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy", 2019 International Carnahan Conference on Security Technology (ICCST), Chennai: IEEE, 2019, pp. 1-8).
16. H. Tanrıkulu, M. H. Sazlı, "Saldırı Tespit Sistemlerinde Yapay Sinir Ağlarının Kullanılması", 2007.
17. UNB, "DDoS Evaluation Dataset (CICDDoS2019)", 2019. Available: https://www.unb.ca/cic/datasets/ddos-2019.html
18. A. R. Wani, Q. P. Rana, U. Saxena, N. Pandey, "Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques", 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai: IEEE, pp. 870-875, 2019.
19. M. M. Zulkernine, "A Neural Network Based System for Intrusion Detection and Classification of Attacks", Natural Sciences and Eng Research Council of Canada (NSERC) Reports, 148-04, 2004.



Tuğba Aytaç received her Bachelor's Degree in 2016 from Süleyman Demirel University Department of Electronic and Communication Engineering. She studies for master degree in cyber security from İstanbul Commerce University Institute of Science. She works in the private sector as IT auditor



Muhammed Ali Aydın received his B.S degree in 2001, M.S degree in Computer Engineering in 2005 from İstanbul Technical University and he holds a doctorate in the same discipline from İstanbul University, received in 2009. Dr. Aydın is currently working as an Assistant Professor in Department of Computer Engineering of İstanbul University - Cerrahpaşa. His main research interests involve computer networks, cryptography and cyber security.



Abdül Halim Zaim Computer Engineering at the Faculty of Engineering at İstanbul University and the Director of the Center for Information Technology Application and Research at İstanbul Commerce University. Abdul Halim Zaim served as Vice Rector and Vice President of Academic Evaluation Commission at İstanbul Commerce University. He received his MS degree in Computer Engineering from Boğaziçi University in 1996 and his PhD in Electrical and Computer Engineering from North Carolina State University (NCSU) in 2001.