DISTRIBUTED DENIAL OF SERVICE ATTACKS DETECTION SYSTEM BY MACHINE LEARNING BASED ON DIMENSIONALITY REDUCTION

Sara Abdalelah Abbas , Mahdi S. Almhanna
College of Information Technology, University of Babylon, Babil, Iraq
saraabd900@gmail.com

Abstract. Data mining algorithms have essential methods and rules that can contribute in detecting and preventing various types of network attacks. These methods are utilized with the intrusion detection systems that can be designed and developed preserve the information in organizations from damage. Specifically, the data mining technique allows users to effectively distinguish between normal and malicious traffic with good accuracy.

In this paper, a methodology for revealing and detecting (DDOS) network attack was suggested using DM algorithms. The utilized methodology is divided especially into four parts, each part has its own rules, as the following: First one is the pre-processing which consists of three sub-steps: (i) encoding, (ii) log2, and (iii) PCA. Encoding is used by converting the original nominal packets into numeric features. Standardization of data was performed using logarithmic algorithm. Finally the PCA technique is applied eight times for several different features to reduce the dimensions of the dataset. The second stage is an anomaly detection model, (RF) algorithm is implemented for the extraction of data patterns while classification the types of the given features in training step, (NB) algorithm was also used in classifying the data to compare the results of its classification with the results of using the classifier (RF). In the third stage, the outcomes were tested by implementing the already trained datasets. In the fourth stage, the proposed system performance evaluation metrics were collected such as the rates of accuracy, false alarm, detection precision, and F.measure.

MIX dataset were utilized to train and test the proposed model which resulted from merging two datasets (PORTMAP+LDAP), which are used from the CICDDOS2019 datasets, each consisting of several types of attack packets, and benign packets.

Several metrics were utilized in the evaluation of the proposed system. The best outcomes were obtained for detection by using the log2 algorithm and PCA technique in the preprocessing step and using (RF) classifier to classify the dataset. the accuracy when using MIX dataset was 99.9764%, the detection rate was 100%, false alarm rate ≈ 0, and the F.measure was 99.9% when PCA = 25.

KEYWORDS. DDoS, PCA, Random Forest (RF), Nave Bayes (NB) , Portmap, LDAP, MIX.

1. Introduction
The (DDoS) assault is an example of the most significant difficulties confronting the Internet society now. These strikes are created with worker machines known as (slaves) who are a portion of the botnet unit that acts on the instructions of the original machine (master machines) whose object is to reduce the network and server sources like bandwidth and storage so that its settings grow unavailable to the genuine parties[1].

These attacks can be utilized in the layers of the network, transport, and application layers employing various rules and protocols such as (HTTP, UDP, and TCP)[2]. DDoS assault impacts the data integrity resulting in losing data and in wrong or misrepresented information. Consequently, wasting the part of security standards like confidentiality, Integrity, and Availability (CIA) which produce great abuse in the industry of the foundation such as missing the confidence of their customers [3].

Network security plays an essential act with financial institutions to defend their data from undesirable jeopardizing. Numerous works have been suggested and developed an Intrusion Detection System (IDS) to examine, identify, and stop hateful actions like network attacks (DDoS). IDS is divided into couple central sections: (i) Misuse Intrusion Detection (MIS) and (ii) Anomaly-Intrusion Detection (AID), the former is
built from obvious attack action worked with model matching, which can be applied later as signature-based for attack event. However, the latter formed from the continuous cycle of traditional practice action forms of network traffic. In common, IDS is able to be classified with various data mining algorithms to recognize the unique entrance or crimes happening to the traffic of the network to guard inner networks [2]. Moreover, IDS is categorized into two sections:

1.1. Host Intrusion Detection (HID). in a class, the implementation in an entire workstation or for the devices of the network, these methods are utilized to block DDoS strikes on a chosen device or targeted network, but it doesn’t hold the director a complete network [4].

1.2. Network Intrusion Detection (NID). a system is executed as a safety procedure within a preserved network, and it is utilized to expose and analyze the entire traffic of the network with all its devices [4].

2. Related works

Many researchers have produced IDS to expose the DDoS attacks using data mining techniques. The most related works are:

- **In 2016, M. Alkasassbeh et al. [5]**, the researcher collected a new dataset that comprises twenty-seven characteristics and five groups. The dataset was designated for various kinds of network attacks that targeted two network layers (application and network). The utilized algorithms are (MLP, Naïve Bayes NB, and Random Forest RF) that implemented to classify the distributed denial of service attacks DDoS such as HTTP-Flood, SIDDDOS, Smurf, and UDP-Flood. confusion matrix is used to calculate the performance of the models. The accuracy rate 98.63% for MLP, 98.02% RF, and 96.91% NB, the highest accuracy rate goes to MLP classifier.

- **In 2019, V. Sharma et al. [6]**, Machine learning algorithm, Support Vector Machine, NB and RF were applied on the dataset that generated by Snort haven incharacteristics and four groups, the classification is made with machine learning algorithms implementing WEKA software, The confusion matrix used for evaluation, The overall accuracy gives 99.7% for Support Vector Machine, 97.6% for Random Forest, and 98.0% for Naïve Bayes, Since it is the highest performance model of SVM, it can be used for intrusion detection systems.

- **In 2019, T. A. Tuan et al. [7]**, The researchers in this proposed system used multiple classifiers to detect Botnet DDoS attacks, by using machine learning algorithms, The SVM, ANN, NB, DT, and USML (K-means, and X-means) were implemented with UNBS-NB15 and KDD99 database. Unsupervised learning algorithm gives best outcomes between DDoS attacks and normal traffic, the obtained Acc was 94.78% which is the highest accuracy when applying this algorithm to UNBS-NB 15 dataset, and 98.08% when applied to KDD99 dataset.

- **In 2017, W. Bhaya and M. Ebadymanaa [8]**, The researchers used a combination of unsupervised data mining techniques as IDS, they utilized collection of adatasets (CAIDA2008, CAIDA2007 and DARPA2000). a methodology of this work implements entropy by windowing on incoming packets, with DM algorithms using (CURE) with clustering model to expose the attack of (DDoS). A results indicate of the proposed system (4) of the (5) discovered stages, more of 99% accuracy, 96.29% detection rate, 0% FAR.

- **In 2012, A. A. K. Hari Om [9]**, The researcher introduced a hybrid intrusion detection system that combines k-Means, and two classifiers: K-nearest and NBto detect anomaly. given system picks essential characteristics and excludes the irredundant characteristics based on entropy characteristic choice. It was applied on KDD-99 dataset; the system discovered interruptions more organized them into 4 classes: Denial of Service (DoS), (U2R), probe, and (R2L). Moreover, it decreased wrong flow.

- **In 2018, A. A. A. and M. K. Ibrahim [10]**, In this work (HIDS) was used to detect DDoS attacks, relying on the (CICIDS 2017) dataset, this dataset contains benign and DDoS attack network flows. To classify the attacks, four classifications were used: Random Forest, C5.0, Naïve-Bayes, and SVM. Depending on the confusion matrix, (RF) was obtained with the highest accuracy = 86.80%, (C5.0)
= 86.45%, and the Precision for both = 99%, but FAR for (RF) = 0.050%, (C5.0) = 0.046% and highest FAR for(SVM) = 75%.

3. CICDDoS2019 Taxonomy/Reflection-based and Exploitation-based DDoS attacks:
The CICDDoS2019 dataset overall consists of 500 63112 instances, including 56863 of benign, and 50006249 DDoS attacks instance[35]. New CICDDoS2019 attacks are implemented using TCP/UDP within the first layer which is the application layer, these attacks are categorized into two categories:

3.1. Reflection-based. in this attack victim encounter difficulty distinguishing between legitimate users and attackers, because attackers hide behind legitimate agents and use them in the attack, such as Internet devices, to become reflector servers (bots) to send attack traffic (such as HTTP requests) to the victim. These attacks are taking by implementing either (TCP) or (UDP) protocol or a combination of both.

3.2. Exploitation-based. on the DDoS attacks:TCP attacks can contain SYN flood while the UDP ones has UDP flood and UDPLag[11][12]. Fig.1. explains the taxonomy of DDOS Attack.

4. Methodology
Flood attacks include sending useless packets in huge amounts to the other machine which is known as (the victim machine) to end the ways of the links are communicated and lead to general network congestion. In DDoS type of attack, the difficulty is how to model/estimate the traffic of the chosen network; that is the traffic of any network have two characteristics(linear and burst), a proposed generic intrusion which is presented as a system for detection model which is illustrated into Figure.3.

The proposed model aims to create network-traffic classification types which are: (i) normal packets and (ii) attacker packets. The proposed system consists of four stages: (i) Preprocessing, detection model, (ii) classification stage, and (iii) performance evaluation stage.

1. The first stage is the pre-processing; In this step, a (MIX) dataset that produced by combine two datasets (Portmap, and LDAP) from (CICDDOS2019) datasets, is used as inputs to the proposed NIDS. the dataset attacks are numbered, by converting the values of symbolic features like: (the IPs of the source and destinations, the ID of the flow, the protocol used by the network, and the

Figure 1. DDoS Attack taxonomy[11].
ports) plus 80 numeric shape data features ranging from 1 to N, Table.1 views features of (CICDDoS2019) [11].

Table.1. Features of (CICDDoS2019) [11].

| Unnamed | Flow ID | Source IP | Source Port | Destination IP | Destination Port | Protocol | Time stamp | Flow Duration | Total Bwd Packet |
|---------|---------|-----------|-------------|----------------|------------------|----------|------------|--------------|------------------|
| Total Backward Packets | Total Length of Fwd Packet | Total Length of Bwd Packets | Fwd Packet Length | Fwd Packet Length Mean | Fwd Port | Bwd Packet Length | Bwd Packet Length Mean | Bwd Packet |
| Bwd Packet Length Std | Flow Bytes | Flow Packets/ s | Flow IAT Std | Flow IAT Mean | Flow IAT Min | Flow IAT Total | Flow IAT Mean |
| Fwd IAT Std | Fwd IAT Max | Fwd IAT Min | Bwd IAT Total | Bwd IAT Mean | Bwd IAT Min | Bwd IAT Std |
| Fwd URG Flags | Bwd URG Flags | Bwd Header Length | Bwd Header Length | Bwd Packet Length | Bwd Packet Length Std |
| Packet Length Variance | FIN Flag Count | STN Flag Count | RST Flag Count | PSH Flag Count | PSH Flag Count |
| Down/Up Ratio | Average Packet Size | Avg Fwd Segments (Size) | Avg Bwd Segments (Size) | Fwd Header Length | Fwd Avg Bytes/Bulk |
| Bwd Avg Bulk Rate | Subflow Fwd Packets | Subflow Fwd Bytes | Subflow Bwd Packets | Subflow Bwd Bytes | Inst Win_bytes_forward | Acct_win_bytes_backward | Acct_win_bytes_backward |
| Active Std | Active Max | Active Min | Idle Mean | Idle Std | Idle Max | Idle Min | Similar HTTP | Inbound | Label |

There are two steps: (i) Encode-step which is found to enhance the outcomes of the system and to accelerate the normalization step and (ii) Data must be standardized before training the classifier. And all parameters must have close values to obtain a fair comparison. To overcome the large spacing in values, through implementing log2 equations to break the (z) values of the features. log2 applies to all values in the MIX dataset used except for the two values (0,1), where:

\[
\begin{align*}
(z \geq 2) & \quad z = f \log_2 (z + 1) \\
& \quad \text{(1)}
\end{align*}
\]

(iii) Dimensional reduction using (PCA), MIX dataset used in the proposed model is converted from high dimensions (HD) to low dimensions (LD) by using the PCA algorithm to reduce the dimensions without any loss in the data features by applying a series of steps outlined in equations(2),(3),(4), and Fig.2. as this algorithm is applied after performing a log2 step to MIX dataset over eight different feature reductions (40,35,30,25,20,15,10,5).

\[
\begin{align*}
Y &= \frac{1}{D} \sum_{i=1}^{D} x_i \\
& \quad \text{(2)}
\end{align*}
\]

\[
\begin{align*}
\text{EGV} &= \frac{1}{D-1} X^T \cdot X \cdot 1 \\
& \quad \text{(3)}
\end{align*}
\]

\[
\begin{align*}
\text{EGV} \cdot S^{-1} \cdot \text{EGV} \cdot S \cdot 1 &= N \\
& \quad \text{(4)}
\end{align*}
\]
2. The second stage is the detection model; the RF classifier is applied in this step to the dataset resulting from the feature reduction step. And applying NB classifier too for results Comparison.

3. The third stage is the classification stage, by testing data with trained pattern information, and classifying them into normal or Multi types of attacks.

4. The fourth stage is the performance evaluation stage using the confusion matrix. The proposed system used a (MIX)dataset that produced by combine two datasets (Portmap, and LDAP) from (CICDDOS2019) datasets, is used as inputs to the proposed NIDS. (CICDDOS2019) datasets with very large network flows, (CICDDOS2019) consists of two (CSV) files, each file contains a different number of datasets, the first file contains 13 datasets, the second file consists of seven datasets, each of which contains different types of serious attacks and the (BENIGN).
5. Performance Measures
The proposed system is evaluated using a confusion matrix in Table 2, [14] [15][16][17][18]. The four metrics are calculated (TP, TN, FP, and FN) for testing; The True Detection Rate(Recall), False Alarm Rate, F. Measure, and Positive Predictive Rate(Precision) are also calculated. The best performance of the system classifier should be with high accuracy, high detection rate, less false alarm rate, and high F. Measure rate.

**Table 2. Confusion Matrix**

| Actual | Predicted |
|--------|-----------|
| Normal | Normal    | Attack   |
| Attack | FN        | TP       |

Detection rate $= \frac{TP}{TP+FN}$ ... (5)

False alarm $= \frac{FP}{FP+TN}$ ... (6)
Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \quad \ldots (7)

Positive Predictive Rate = \frac{TP}{TP + FP} \quad \ldots (8)

F.Measure = \frac{2(Precision \times \text{Recall})}{\text{Precision} + \text{Recall}} \quad \ldots (9)

6. Experimental Analyses

The objective of this paper is to take into consideration the security manners by designing a network intrusion detection system with high accuracy high detection rate. by building a training and testing model, the training was conducted on 70% of the MIX dataset, and the testing on 30% of the dataset. detected three types of attacks (PORTMAP, LDAP, NetBios) After applying preprocessing steps such as; (encoding), (standardization), and (PCA) technique on MIX dataset for obtaining reduced features, then applying the (RF) and (NB) algorithm. The confusion matrix was used to evaluate the proposed system, Tables.3..4. gives the obtained final results of the performance evaluation of the classifier inside the testing stage. achieved the highest accuracy (99.9764 %) when using RF classifier, and data was reduced to (25) features , and then achieved accuracy(95.5469 %)when using NB classifier, and data was reduced to (25) features.

Table. 3. Performance evaluation of the detection model in which the MIX dataset and the Random Forest classifier were used.
Table 4. Performance evaluation of the detection model in which the MIX dataset and the Naïve Bayes classifier were used.

| No. of features | Type of Attacks orBenIGN | DR (TPR) | FAR (FPR) | Precision (PPR) | F-Measure | accuracy |
|-----------------|--------------------------|----------|-----------|------------------|-----------|----------|
| 5               | BENIGN                   | 0.000    | 0.000     | 0.021            | 0.021     | 93.937 % |
|                 | LDAP                     | 0.955    | 0.010     | 0.998            | 0.976     |          |
|                 | NetBIOS                  | 0.012    | 0.001     | 0.090            | 0.021     |          |
|                 | BENIGN                   | 0.994    | 0.030     | 0.133            | 0.235     |          |
|                 | PORTMAP                  | 0.934    | 0.034     | 0.857            | 0.894     |          |
| 10              | BENIGN                   | 0.000    | 0.000     | 0.021            | 0.024     | 93.3786 %|
|                 | LDAP                     | 0.950    | 0.004     | 0.999            | 0.974     |          |
|                 | NetBIOS                  | 0.043    | 0.018     | 0.025            | 0.031     |          |
|                 | BENIGN                   | 0.999    | 0.038     | 0.108            | 0.195     |          |
|                 | PORTMAP                  | 0.926    | 0.012     | 0.943            | 0.934     |          |
| 15              | BENIGN                   | 0.000    | 0.000     | 0.019            | 0.023     | 94.4661 %|
|                 | LDAP                     | 0.951    | 0.000     | 1.000            | 0.975     |          |
|                 | NetBIOS                  | 0.057    | 0.020     | 0.029            | 0.039     |          |
|                 | BENIGN                   | 1.000    | 0.009     | 0.346            | 0.514     |          |
|                 | PORTMAP                  | 0.982    | 0.032     | 0.869            | 0.922     |          |
| 20              | BENIGN                   | 0.000    | 0.000     | 0.000            | 0.022     | 95.5377 %|
|                 | LDAP                     | 0.951    | 0.008     | 0.998            | 0.974     |          |
|                 | NetBIOS                  | 0.984    | 0.000     | 0.957            | 0.971     |          |
|                 | BENIGN                   | 1.000    | 0.007     | 0.396            | 0.567     |          |
|                 | PORTMAP                  | 0.984    | 0.043     | 0.832            | 0.901     |          |
7. Performance and comparison proposed model

The results of other researchers are shown in Table.5.[2]. Highest accuracy is obtained from random forest and ID3 Classifiers; these results are obtained based on the criteria of three evaluation types with Precision score, Recall score, and F1 score respectively.

Table 5. The obtained results [2].
8. Conclusion

1. Flexibility of coding when utilizing a large datasets such as (MIX) by converting data type from nominal to numerical.

2. The computational complexity has been reduced by applying log2 algorithm; it has proven its efficiency by standardizing the data, as it produced convergent data values after they were spaced.

3. Reducing dataset dimensionality by implementing the technique of principal components analyses that led to reducing the complexity of the computational time as well as speeds-up classification and numerical stability. The dimensions of the datasets were reduced to eight times with different numbers of features to ensure a fair comparison.

4. Converting the related variables into a smaller number of unrelated compounds, as the dataset has a relation between the dependent and independent variables, where there are fewer variables in the independent variables comparing to the dependent variables which are meant to be reduced to lessen the degree of information rate.

5. The experimental results MIX dataset showed that the proposed system detects multiple types of attacks, and achieved excellent results for very large network data efficiently when implementing RF classifier.

6. The highest accuracy reached (99%) with false alarms rate that reached (≈ 0) using the RF detection model. While in NB classifier, the results were relatively good, but the values varied according to the percentage of data dimensions reduction. Both classifiers gave promising results in terms of accuracy for detection and computational efficiency.

References

[1] K. J. S. and T. De, “An Approach of DDOS Attack Detection Using Classifier,” Springer India, 2015, doi: DOI 10.1007/978-81-322-2550-8_41.

[2] S. H. and A. A. G. Iman Sharafaldin, Arash Habibi Lashkari, “Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy,” Can. Inst. Cybersecurity (CIC), Fac. Comput. Sci., 2019.

[3] M. E. M. and Wesam S. Bhaya, “Review clustering mechanisms of distributed denial of service attacks,” J. Comput. Sci., doi: 10.3844/jcssp.

[4] M. S. Talha ALI Khan, Muhammad Kamran Asif, and Talha Ahmed Taj, “Network Intrusion Detection and its strategic importance,” researchgate, doi: 10.1109/BEIAC.2013.6560100.

[5] M. Alkasassbeh, G. Al-Naymat, A. B.A, and M. Almseidin, “Detecting Distributed Denial of Service Attacks Using Data Mining Techniques,” Int. J. Adv. Comput. Sci. Appl., vol. 7, no. 1, pp.
436–445, 2016, doi: 10.14569/ijacsa.2016.070159.

[6] V. Sharma, V. Verma, and A. Sharma, “Detection of DDoS Attacks Using Machine Learning in Cloud Computing,” *Commun. Comput. Inf. Sci.*, vol. 1076, pp. 260–273, 2019, doi: 10.1007/978-981-15-0111-1_24.

[7] T. A. Tuan, H. V. Long, L. H. Son, R. Kumar, I. Priyadarshini, and N. T. K. Son, “Performance evaluation of Botnet DDoS attack detection using machine learning,” *Evol. Intell.*, 2019, doi: 10.1007/s12065-019-00310-w.

[8] W. Bhaya and M. Ebadymanaa, “DDoS attack detection approach using an efficient cluster analysis in large data scale,” *2017 Annu. Conf. New Trends Inf. Commun. Technol. Appl. NTICT 2017*, no. March, pp. 168–173, 2017, doi: 10.1109/NTICT.2017.7976110.

[9] A. A. K. Hari Om, “A Hybrid System for Reducing the False Alarm Rate of Anomaly Intrusion Detection System,” *IEEE*, 2012.

[10] A. A. A. and M. K. Ibrahim, “EVALUATION OF DDOS ATTACKS DETECTION IN A CICIDS2017 DATASET BASED ON CLASSIFICATION ALGORITHMS,” *Iraqi J. Inf. Commun. Technol.*, vol. 1, no. 3, 2018.

[11] Canadian Institute for Cybersecurity, *DDoS evaluation dataset (CICDDoS2019)*, 2019. [Online]. Available: https://www.unb.ca/cic/datasets/ddos-2019.html (visited on 17/01/2020).

[12] A. J. S. Nour Moustafa, “The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set,” *Inf. Secur. J.*, 2016, doi: 10.1080/19393555.2015.1125974.

[13] M. K. Ibraheem, I. M. A. Al-Khafaji, and S. A. Dheyab, “NETWORK INTRUSION DETECTION USING DEEP LEARNING BASED ON DIMENSIONALITY REDUCTION,” *ausrevisa*, pp. 168–174, 2019, doi: 10.4206/aus.2019.n26.2.23/.

[14] A. J. S. Moustafa, Nour, “The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set,” *Inf. Secur. J. A Glob. Perspect. J.* homepage http://www.tandfonline.com/loi/uiss20, vol. 25, NOS. 1, pp. 18–31, 2016, doi: 10.1080/19393555.2015.1125974.

[15] T. H. H. Manish R. Joshi, “A Review of Network Traffic Analysis and Prediction Techniques,” *Sch. Comput. Sci. North Maharashtra Univ. Jalgaon (M.S) India*.

[16] S. K. S. Preeti Aggarwal, “Analysis of KDD Dataset Attributes - Class wise For Intrusion Detection,” *Procedia Comput. Sci.*, pp. 842 – 851, 2015, doi: 10.1016/j.procs.2015.07.490.

[17] C.-Y. Chih-Fong Tsai, “A triangle area based nearest neighbors approach to intrusion detection,” *Pattern Recognit.*, pp. 222–229, 2010, doi: 10.1016/j.patcog.2009.05.017.
[18] HOW TO PROTECT YOUR VPS HOSTING FROM DDOS ATTACKS? [Online]. Available: https://tuchacloud.com/how-to-protect-your-vps-hosting-from-ddos-attacks// (visited on 2/01/2020).