DDoS Attacks Detection Method Using Feature Importance and Support Vector Machine

Ahmad Sanmorino[1], Rendra Gustriansyah[2], Juhaini Alie[3]

[1,2]*Faculty of Computer Science, Universitas Indo Global Mandiri, Indonesia*

[3]*Faculty of Economics, Universitas Indo Global Mandiri, Indonesia*

[1]sanmorino@uigm.ac.id, [2]rendra@uigm.ac.id, [3]juhaini@uigm.ac.id

Abstract - In this study, the author wants to prove the combination of feature importance and support vector machine relevant to detecting distributed denial-of-service attacks. A distributed denial-of-service attack is a very dangerous type of attack because it causes enormous losses to the victim server. The study begins with determining network traffic features, followed by collecting datasets. The author uses 1000 randomly selected network traffic datasets for the purposes of feature selection and modeling. In the next stage, feature importance is used to select relevant features as modeling inputs based on support vector machine algorithms. The modeling results were evaluated using a confusion matrix table. Based on the evaluation using the confusion matrix, the score for the recall is 93 percent, precision is 95 percent, and accuracy is 92 percent. The author also compares the proposed method to several other methods. The comparison results show the performance of the proposed method is at a fairly good level in detecting distributed denial-of-service attacks. We realized this result was influenced by many factors, so further studies are needed in the future.

Keywords: Distributed denial-of-service attacks detection method; feature importance; support vector machine

I. INTRODUCTION

Distributed denial-of-service (DDoS) attack is a very dangerous type of attack because it causes enormous losses to the server that is the victim of the attack [1-2]. Since it first appeared, until today's modern era, the types and methods of DDoS attacks have developed very rapidly [3]. Commonly, when an attack method has a known attack pattern, the attacker will try to change, modify, or improve the attack pattern. Pattern modification is usually done in disguise. Attack patterns are made very naturally, such as service requests originating from legitimate users, so that they are not detected as packets or requests originating from zombies, which are controlled by the attacker [4]. In today's modern era, DDoS attacks take advantage of technological advances including artificial intelligence (AI), high-speed internet access, and high-performance computing [5-6]. With very abundant resources, DDoS attacks are carried out massively and become very difficult to detect [7-8].

As DDoS attack methods are constantly evolving, DDoS attack detection methods are also developing very rapidly. The purpose of developing DDoS attack detection methods is to counter DDoS attack methods. Like the DDoS attack method, the DDoS attack detection method also utilizes AI technology. Through this study, the author wants to provide an alternative method to detect DDoS attacks. Machine learning (ML)-based methods, which are part of AI technology, have proven to be quite relevant in detecting DDoS attacks, as evidenced by the results of several studies conducted by Thorat, Parekh, and Mangrulkar [9], Manjula and Neha Mangla [10]. Based on previous related studies, the authors propose the detection of DDoS attacks based on feature importance [11], and the Support Vector Machine (SVM) algorithm [12-13]. The purpose of this study is to prove that the proposed method based on feature importance and SVM can be used to detect DDoS attacks. Deeply, the feature importance is used to select relevant features to detect DDoS attacks. Furthermore, the selected features are used as input for the SVM algorithm. SVM is used to model DDoS attack packets originating from the attacker. As an initial hypothesis, the combination of feature importance and SVM is relevant to distinguish between legitimate packets and packets from attackers. In other words, the proposed method uses feature importance, and SVM can detect DDoS attacks. This study is also a continuation of the previous study the author has done [14-15].

II. METHOD

The author performs a simulation to prove the performance of the proposed method in detecting DDoS attacks. This simulation consists of two major stages, feature selection, and modeling. For the purposes of feature selection and modeling, the author uses 1000

randomly selected network traffic datasets. Generally, the stages in this study are:

1. Define network traffic features
2. Collect datasets based on network traffic features
3. Selecting relevant features using the feature importance approach
4. Modeling using SVM algorithm based on selected features
5. Evaluation of the results of the confusion matrix-based modeling. Outcome: recall, precision, accuracy
6. Comparison of evaluation results with other detection methods.

Determination of the dataset based on the features presented in Table I.

To select relevant features from the network traffic features shown in Table I, the author uses the feature importance approach [16,17]. Feature importance is the influence that a feature has in predicting the classification results [18]. The greater the feature importance score to get the feature importance score, the entropy value must first be obtained [19,20]. The entropy value is obtained using (1):

$$Entropy(S) = \sum_{i=1}^{C} p_i \, log_2(p_i) \quad (1)$$

Where c is the number of unique classes and pi is the proportion of rows with the output class i. After the entropy value is obtained, then the feature information score is obtained using (2):

$$Feature\_Importance(S, A) = Entropy(S) - \sum_{veValues(A)} \frac{|S_v|}{|S|} Entropy(S_v) \quad (2)$$

Where S is the set of instances, A is the attribute, Sv is the subset of S with A = v, and Values (A) is the set of all possible values of A. The next step is to model the dataset based on the selected features from the previous stage. This modeling aims to determine whether the packet comes from a legitimate user or a packet that comes from an attacker (DDoS attack). For modelling purposes, the author uses a support vector machine (SVM) algorithm, the SVM method was introduced by Cortes and Vapnik in 1995. SVM has many advantages such as being able to work very well for data sets with many attributes and small sample sizes [12-13]. Furthermore, the results of SVM modelling were evaluated using a confusion matrix to obtain recall, precision, and accuracy values [21-22]. Recall, precision, and accuracy scores were obtained using (3-5):

$$Accuracy = \frac{(TP+TN)}{(TP+FP+FN+TN)} \quad (3)$$

Accuracy shows the number of correct predictions of attack detection from the total number of DDoS attacks.

$$Precision = \frac{(TP)}{(TP+FP)} \quad (4)$$

Precision shows the accuracy between the requested data and the prediction results displayed by the model.

$$Recall = \frac{TP}{(TP+FN)} \quad (5)$$

For recall or sensitivity, it shows the success of the model in rediscovering relevant information. The last stage of this study is the comparison of the accuracy scores obtained with the accuracy scores of other detection methods. Based on the results of this comparison, it is known whether the proposed method is relevant enough to detect DDoS attacks.

TABLE I
NETWORK TRAFFIC FEATURES

Code	Feature	Description
f1	Src-Dest-Packets	Number of packets from source to destination
f2	Dest-Src-Packets	Number of packets from destination to source
f3	Src-Packet-Sz	Sum of packet size from source to destination
f4	Dst-Packet-Sz	Sum of packet size from destination to source
f5	Src-Frame	Frame length from source to destination
f6	Dst-Frame	Frame length from destination to source
f7	Src-Num-Fr	Number of frames from source to destination
f8	Dst-Num-Fr	Number of frames from destination to source
f9	Src-IP-Addr	Number of source IP address
f10	Dst-IP-Addr	Number of destination IP address
f11	Source-Ports	Number of source host ports
f12	Desti-Ports	Number of destination host ports

III. RESULTS AND DISCUSSION

Table II shows the results of feature importance-based feature selection. The Src-Dest-Packets feature has the highest score compared to other features. This feature importance score shows the importance of a feature in detecting DDoS attacks. In other words, the higher the score of a feature, the greater its contribution to the DDoS attack detection process.

The number of packets that correctly identified they were not a DDoS attack was 62.64 percent. The number of packets that were incorrectly identified as not being a DDoS attack was 3.30 percent. The number of packets correctly identified as being a DDoS attack was 29.67 percent. The number of packets that were incorrectly identified as being a DDoS attack was 4.40 percent.

Recall, precision, and accuracy of the evaluation results of SVM modeling are shown in Table III.

Based on the results of the feature selection shown in Table II, the author will only take the top 6 features used as variables for the support vector machine modeling. The six selected features are Src-Dest-Packets, Dest-Src-Packets, Src-Packet-Sz, Dst-Packet-Sz, Src-Num-Fr, and Dst-Num-Fr. To get the recall, precision, and accuracy from the modeling results, the authors use a confusion matrix shows in Fig. 1.

The support vector machine classification resulted are 90 percent of packets being correctly not DDoS attacks from all packets that were predicted not DDoS attacks (precision with target = legitimate). The support vector machine classification resulted are 93 percent of packets being correctly detected as DDoS attacks out of all packets predicted to be DDoS attacks (precision with target = DDoS). The support vector machine classification resulted in 87 percent of packets that were

TABLE II
FEATURE IMPORTANCE SCORES

Code	Score
f1	0.34473703
f2	0.26438539
f3	0.15491770
f4	0.05414120
f7	0.04822908
f8	0.04408499
f5	0.03458260
f6	0.02374232
f9	0.02156291
f10	0.00949233
f11	0.00012439
f12	0.00011343

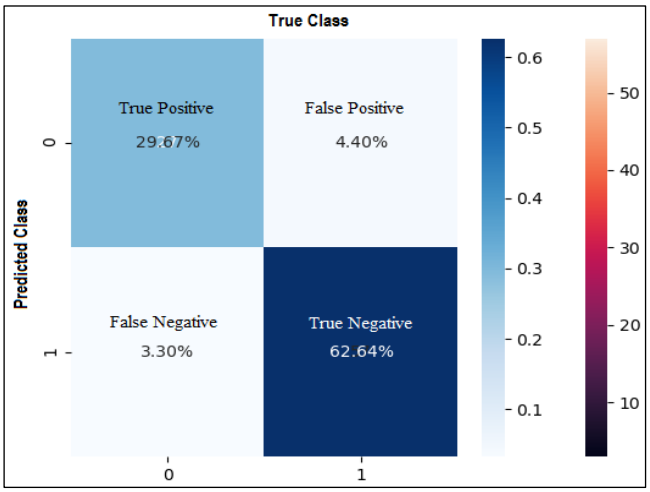

Fig. 1 SVM confusion matrix

TABLE III
RECALL, PRECISSION, AND ACCURACY SCORES

Target	Precision	*Recall*	*f1-Score*
Legitimate	0.90	0.87	0.89
DDoS	0.93	0.95	0.94
Accuracy			0.92

predicted not a DDoS attack compared to the whole packet which was actually not a DDoS attack (recall with target = legitimate). The support vector machine classification results are 95 percent of packets being predicted as DDoS attacks compared to all packets that are actually DDoS attacks (recall with target = DDoS). The support vector machine classification results in an average comparison of recall and precission for packets that are not DDoS attacks of 89 percent. support vector machine classification results in a comparison of the average precision and recall for packets originating from the attacker by 94 percent (f-measure). The support vector machine classification resulted are 92 percent of packets being correctly predicted as DDoS attacks and not DDoS attacks from the total packets. For alternative evaluations besides recall, precision, and accuracy from the confusion matrix table, the receiver operating characteristic (ROC) curve also be derived [23]. The resulting receiver operating characteristic curve is presented in Fig. 2.

The SVM ROC curve with feature importance shows a very high true positive score and a very low false positive score. In the ROC curve, the most important part is the area under the curve (AUC), which is the total area under the ROC curve. The SVM ROC curve has an AUC score of 0.91, so the SVM modelling is proven to correctly predict packets that are DDoS attacks by 91 percent. Based on classification results and continued

with ROC curve measurement, the combination of feature importance and the SVM algorithm is proven to be able to distinguish between legitimate packages and packets from attackers. The results of this test succeeded in providing answers to the initial hypothesis that had been submitted by the author.

The author also compares the evaluation results (recall, precision, and accuracy) obtained with other related studies. The results of the comparison of accuracy scores are shown in Table IV.

Table IV shows a comparison of the accuracy scores of each classification algorithm in the study related to DDoS attack detection. This comparison shows the performance of the detection method proposed is in a fairly good position, with the highest accuracy score. The selection based on feature importance is very influential on the final result of SVM modelling. Irrelevant features will cause bias, which in turn can reduce the accuracy of DDoS attack detection. Based on this evaluation, it is evident that the combination of feature importance and the SVM algorithm is very relevant to be used as a DDoS attack detection method.

IV. CONCLUSION

Based on this study, the combination of feature importance for feature selection and support vector machine for modeling is very relevant used in detecting DDoS attacks. This hypothesis is proven from a confusion matrix-based evaluation with a score for recall of 93 percent, precision of 95 percent, and accuracy of 92 percent. The author also compares the proposed method to several other methods. The comparison results show the performance of the proposed method is at a fairly good level in detecting DDoS attacks. The novelty of this study is the combination of using feature importance for feature selection and SVM to distinguish between legitimate packages and packets from attackers. The contribution of this study is to provide an alternative to detecting DDoS attacks so that they can be implemented, developed, or optimized by other researchers in the future.

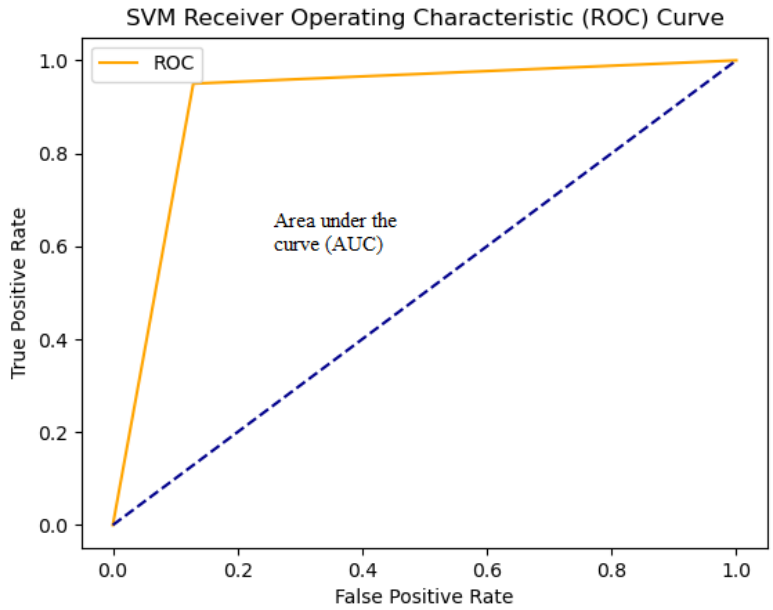

Fig. 2 SVM ROC curve

TABEL IV
ACCURACY COMPARISSON

Feature	Method	Accuracy Score
Src-Dest-Packets, Dest-Src-Packets, Src-Packet-Sz, Dst-Packet-Sz, Src-Num-Fr, and Dst-Num-Fr	SVM only	88%
	Univariate selection + Naive Bayes	86%
	Feature importance + SVM	92%
	Feature importance + Decision Tree	89%

ACKNOWLEDGEMENT

We would like to thank you Universitas Indo Global Mandiri for supporting this study.

REFERENCES

[1] J. Park, M. Mohaisen, D. H. Nyang, and A. Mohaisen, "Assessing the effectiveness of pulsing denial of service attacks under realistic network synchronization assumptions," Comput. Networks, vol. 173, no. December 2019, p. 107146, 2020, doi: 10.1016/j.comnet.2020.107146.

[2] A. Bhardwaj, V. Mangat, and R. Vig, "Effective mitigation against IoTs using super materials for distributed denial of service attacks in cloud computing," Mater. Today Proc., vol. 28, no. xxxx, pp. 1359–1362, 2020, doi: 10.1016/j.matpr.2020.04.800.

[3] Y. Cui et al., "Towards DDoS detection mechanisms in Software-Defined Networking," J. Netw. Comput. Appl., vol. 190, no. March, p. 103156, 2021, doi: 10.1016/j.jnca.2021.103156.

[4] R. Priyadarshini and R. K. Barik, "A deep learning based intelligent framework to mitigate DDoS attack in fog environment," J. King Saud Univ. - Comput. Inf. Sci., vol. 34, no. 3, pp. 825–831, 2022, doi: 10.1016/j.jksuci.2019.04.010.

[5] A. Jaszcz and D. Połap, "AIMM : Artificial Intelligence Merged Methods for flood DDoS attacks detection," J. King Saud Univ. - Comput. Inf. Sci., no. xxxx, 2022, doi: 10.1016/j.jksuci.2022.07.021.

[6] G. C. Amaizu, C. I. Nwakanma, S. Bhardwaj, J. M. Lee, and D. S. Kim, "Composite and efficient DDoS attack detection framework for B5G networks," Comput. Networks, vol. 188, no. December 2020, p. 107871, 2021, doi: 10.1016/j.comnet.2021.107871.

[7] M. A. Lawall, R. A. Shaikh, and S. R. Hassan, "A DDoS Attack Mitigation Framework for IoT Networks using Fog Computing," Procedia Comput. Sci., vol. 182, pp. 13–20, 2021, doi: 10.1016/j.procs.2021.02.003.

[8] P. Harikrishna and A. Amuthan, "Rival-Model Penalized Self-Organizing Map enforced DDoS attack prevention mechanism for software defined network-based cloud computing environment," J. Parallel Distrib. Comput., vol. 154, pp. 142–152, 2021, doi: 10.1016/j.jpdc.2021.03.005.

[9] O. Thorat, N. Parekh, and R. Mangrulkar, "TaxoDaCML: Taxonomy based Divide and Conquer using machine learning approach for DDoS attack classification," Int. J. Inf. Manag. Data Insights, vol. 1, no. 2, p. 100048, 2021, doi: 10.1016/j.jjimei.2021.100048.

[10] H. T. Manjula and Neha Mangla, "An approach to on-stream DDoS blitz detection using machine learning algorithms," Mater. Today Proc., no. xxxx, 2022, doi: 10.1016/j.matpr.2021.07.280.

[11] C. M. Scavuzzo et al., "Feature importance: Opening a soil-transmitted helminth machine learning model via SHAP," Infect. Dis. Model., vol. 7, no. 1, pp. 262–276, 2022, doi: 10.1016/j.idm.2022.01.004.

[12] I. Zoppis, G. Mauri, and R. Dondi, Kernel methods: Support vector machines, vol. 1–3. Elsevier Ltd., 2018. doi: 10.1016/B978-0-12-809633-8.20342-7.

[13] L. Hong, Z. Chen, Y. Wang, M. Shahidehpour, and M. Wu, "A novel SVM-based decision framework considering feature distribution for Power Transformer Fault Diagnosis ☆" Energy Reports, vol. 8, pp. 9392–9401, 2022, doi: 10.1016/j.egyr.2022.07.062.

[14] A. Sanmorino, "A study for DDOS attack classification method," J. Phys. Conf. Ser., vol. 1175, no. 1, 2019, doi: 10.1088/1742-6596/1175/1/012025.

[15] A. Sanmorino and S. Yazid, "DDoS Attack detection method and mitigation using pattern of the flow," 2013. doi: 10.1109/ICoICT.2013.6574541.

[16] A. Wibowo, S. Rasyid, C. Pratama, L. Sophia, D. P. Sahara, and S. Tri, "Geodesy and Geodynamics Anomaly detection on displacement rates and deformation pattern features using tree-based algorithm in Japan and Indonesia," Geod. Geodyn., no. August, pp. 1–13, 2022, doi: 10.1016/j.geog.2022.07.003.

[17] A. V. Phan, P. N. Chau, M. Le Nguyen, and L. T. Bui, "Automatically classifying source code using tree-based approaches," Data Knowl. Eng., vol. 114, no. July, pp. 12–25, 2018, doi: 10.1016/j.datak.2017.07.003.

[18] X. Zhu, C. Ying, J. Wang, J. Li, X. Lai, and G. Wang, "Ensemble of ML-KNN for classification algorithm recommendation," Knowledge-Based Syst., vol. 221, p. 106933, 2021, doi: 10.1016/j.knosys.2021.106933.

[19] L. Yang, F. Wei, and E. Chen, "Developing an assessment index for collection-user suitability: Application of information entropy in library science," J. Acad. Librariansh., vol. 48, no. 1, p. 102477, 2022, doi: 10.1016/j.acalib.2021.102477.

[20] M. Wibral and V. Priesemann, Information Theoretical Approaches, vol. 1. Elsevier Inc., 2015. doi: 10.1016/B978-0-12-397025-1.00338-9.

[21] J. Xu, Y. Zhang, and D. Miao, "Three-way confusion matrix for classification: A measure driven view," Inf. Sci. (Ny)., vol. 507, pp. 772–794, 2020, doi: 10.1016/j.ins.2019.06.064.

[22] S. Wang, H. Lu, A. Khan, F. Hajati, M. Khushi, and S. Uddin, "A machine learning software tool for multiclass classification," Softw. Impacts, vol. 13, no. July, p. 100383, 2022, doi: 10.1016/j.simpa.2022.100383.

[23] T. Duong, "Non-parametric smoothed estimation of multivariate cumulative distribution and survival functions, and receiver operating characteristic curves," J. Korean Stat. Soc., vol. 45, no. 1, pp. 33–50, 2016, doi: 10.1016/j.jkss.2015.06.002.