IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Detection of DDOS Attack Using Decision Tree Classifier

[1] Sankara Narayanan S, [2] Vigneshmani S, [3] Pal Jesveen E, [4] Mrs.Brundha P

[1]Student, [2] Student, [3] Student, [4] Assistant Professor
[1] Computer Science and Engineering,
[1] Francis Xavier Engineering College, Tirunelveli – Tamil Nadu – India

***Abstract* — SDN architecture uses programmatic control so it is flexible but the design vulnerability makes it easy for Distributed Denial of Service (DDoS) attacks to occur. These attacks which include TCP, UDP, SYN, ICMP and DHCP flooding result in network disruptions that disrupt service availability for entire networks. This research develops a machine learning detection model that evaluates and categorizes DDoS attacks within SDN systems. Decision Tree Classifier served as the main algorithm because its accuracy rate surpassed those of Gaussian Naive Bayes and Support Vector Machine (SVM). Forward Feature Selection served as a tool to select the key features in the dataset which improved model operational effectiveness. The model training used these selected features which delivered better prediction results after testing. The study proves that Decision Tree classification makes effective DDoS pattern detection possible which serves as foundational knowledge for developing hybrid models that achieve better accuracy and fewer false negative results.**

Keywords*— *SDN, DDoS detection, Decision Tree Classifier, Machine Learning, Feature Selection, Network Security.

INTRODUCTION

The network management revolution comes from Software Defined Networking (SDN) because it delivers programming capabilities along with unified administration and adaptive system modification. The separation of control and data planes in SDN creates specific vulnerabilities which allow Distributed Denial of Service (DDoS) attacks to penetrate the system. The flooding attacks against services use TCP, UDP and SYN, ICMP and DHCP which result in service disruption along with network availability compromise. Standard security tools find it challenging to develop swift and precise solutions against developing threats. Machine learning now receives extensive attention because researchers demonstrate through evidence that it can identify and stop Distributed Denial of Service attacks in intelligent ways. A DDoS detection system based on Decision Tree Classifier operates in SDN environments where feature selection techniques optimize the detection process.

Modern networks require Software Defined Networking (SDN) adoption as an answer to the rising complexity because this system separates control from data planes to achieve better network programmability and agility. The centralized architecture of SDN systems makes them exposed to Distributed Denial of Service (DDoS) attacks that jeopardize continuous network operation. Machine learning technology presents effective methods which can detect and categorize such attacks immediately. The examination under this project demonstrates how Decision Tree Classifier operating with Forward Feature Selection detects various DDoS attacks in SDN networks effectively. The investigation confirmed Decision Tree provides the highest accuracy rates when compared with SVM and Gaussian Naive Bayes models in this implementation environment.

The forwarding functions of networks can be decoupled from intelligent control mechanisms through Software Defined Networking (SDN) which originates from the need for evolving modern network demands. The benefits of this architecture for better management come with specific weaknesses which make the networks particularly prone to Distributed Denial of Service (DDoS) attacks. Network resources become overwhelmed by these attacks to the extent that they disable services available to genuine network users. Our study addresses this problem using machine learning technologies which detect and stop DDoS attacks toward SDN infrastructure. Our project focuses on the Decision Tree Classifier because it provides both accuracy and interpretability in its results. The modified model with Forward Feature Selection operates with higher efficiency which makes it appropriate for actual network protection deployments.

Software Defined Networking (SDN) architecture enables administrators to gain essential benefits from network flexibility and automated operations as well as

centralized control management. The design of controller-plane separation within SDN platforms creates security risks that let Distributed Denial of Service (DDoS) attacks develop. The central controller becomes a target for attacks which results in the complete network shutdown. The authors use machine learning methods for detecting these attacks within their study. The Decision Tree Classifier reaches high accuracy rates when trained with traffic data features selection. SDN DDoS detection benefits tremendously from Decision Tree algorithms based on the results of comparison with SVM and Gaussian Naive Bayes classifiers.

The rise in Software Defined Networking (SDN) implementations makes network security harder to achieve because SDN presents architectural weaknesses. The design where control functions operate separately from data functions in SDN networking creates conditions that enhance Distributed Denial of Service (DDoS) attack susceptibility. The research develops a machine learning model for detecting and suppressing Distributed Denial of Service threats from network traffic information. According to testing results the Decision Tree Classifier showed outstanding performance because it achieved maximum accuracy during detection operations. Forward Selection featured in the procedure to enhance model prediction ability through feature selection. The presented research helps develop secure SDN domains through modern intelligent systems for threat detection.

LITERATURE SURVEY

[1] The study implements min-max scaling and SMOTE on the CICIDS 2017 data before applying LASSO for feature selection. Scientists trained different ML models by implementing XGBoost, LGBM, CatBoost, Random Forest and Decision Tree algorithms with their optimized parameters. The research demonstrates that LGBM produces the best results among models because it achieved a 99.77% accuracy rate in detecting DDoS attacks for financial system security.

[2] The research based its evaluations on nine ML models with a deep learning model demonstrating 99% attack detection results but approximately 70% precision in identifying attack types. The implementation of time-based features alone brought substantial reductions to training time while maintaining the same level of accuracy performance standards which makes this detection method ideal for real-time applications. Research shows that analyzing time-related features can create valuable improvements for detecting and classifying DDoS attacks in modern network systems.

[3] The XRC system utilizes the capabilities of XGBoost and regression classifiers for accurate detection and forecasting of different cyber threats. The sigmoidal activation function as an addition to the model delivers better performance and lower error rates. The hybrid model delivers experimental results which substantially reduce training and testing errors thus creating a dependable system for current cybersecurity threat monitoring and classification purposes.

[4] Based on present network conditions the proposed framework determines which algorithm from Naive Bayes, Decision Tree (Entropy and Gini) and Random Forest to execute through fuzzy logic selection. The system achieves better detection accuracy with optimal performance-slowdown trade-offs by uniting these system components. Laboratory tests confirm that Fuzzy logic-based algorithm selection enhances both system performance and timeliness in live-time DDoS alerting operation.

METHODOLOGY

The project starts with gathering network traffic data with standard patterns and DDoS attack signatures that need preprocessing for analysis. The data consists of different DDoS attack varieties including TCP flooding, UDP flooding and SYN flooding, ICMP flooding and DHCP flooding. The dataset contains instances which receive the necessary labels needed for supervised learning methods. Forward Feature Selection method is used to find key features which maximize model accuracy at minimum computational time. The selection process identifies unimportant attributes which allows the machine learning models to receive training only on essential features.

The dataset is divided for training and testing purposes after choosing features. Gaussian Naive Bayes alongside Support Vector Machine (SVM) and Decision Tree Classifier conduct evaluations using the chosen data for training purposes. The Decision Tree Classifier shows the highest effectiveness as a model based on evaluations using accuracy measures alongside precision and recall and F1-score metrics. The Decision Tree model generates flowchart structures that learn data rules to identify between normal and malicious traffic. The Decision Tree achieves better accuracy performance and interpretability capabilities which makes it an excellent choice for real-time DDoS detection within SDN environments.

Additional evaluation of model performance included a confusion matrix comparison together with classification report analysis. The tests demonstrated that Decision Tree Classifier succeeded in detecting multiple DDoS attack types at a superior true positive rate and reduced false negative rate than Gaussian Naive Bayes and SVM. Network security applications benefit from using the Decision Tree because of its transparent decision-making process and ability to analyze non-linear relationships. The practical deployment of SDN real-time environments happens easily through this classifier due to its simple training procedure and flexible scalability capabilities. Knowledge obtained from this methodology can act as a basis of updates in the future, for example in the integration of hybrid models or ensemble learning methods in order to improve detection accuracy and robustness.

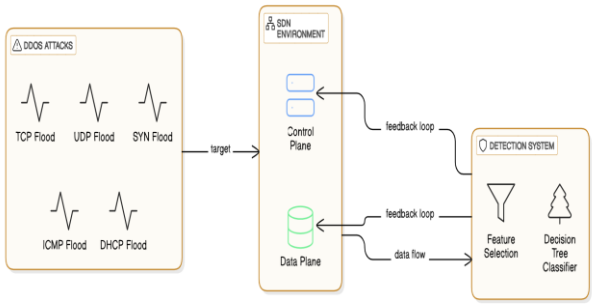

Fig.1. Architecture Diagram

EXISTING SYSTEM

Traditional security mechanisms or fixed-rule intrusion detection are typical in the current systems for DDoS detection in Software Defined Networking (SDN) environments. These methods have difficulty in keeping up with the changing or complex nature of modern DDoS attacks, especially within SDN, where the control and data plane separation brings additional risks. Attacks such as TCP, UDP, SYN, and ICMP flooding can rather easily post significant stress on the central controller, to incidents of failures of service drops and directions network. Moreover, traditional static rule-based systems have no ability to detect emerging attack patterns or various DDoS categories.

In recent years, machine learning methods became popular as fair-share and scalable options. But most of these existing methods done with the generic algorithm without using optimized algorithms lead to less accuracy and more false negatives. Furthermore, some models do not have xml (feature selection) enabling inclusion-renunciation complexity and longer training time. The existing scenario demands for more effective, correct and acute models capable of identifying and labeling the DDoS assaults in the SDN network in real time. This project achieves this by combination of Decision Tree Classifier along with Forward Feature Selection to enhance detection accuracy and employ economic usage of resources.

V. PROPOSED SYSTEM

A machine-learning based system operates in Software Defined Networking environments to detect DDoS attacks while performing classification functions. The Decision Tree Classifier stands as the main component of the system because of its superior detection accuracy and explainable operation. The system starts its process by gathering network traffic data that contains normal operations as well as multiple types of DDoS attack traffic. The Forward Feature Selection method performs feature selection to pick essential attributes from the dataset thus the system maintains enhanced computational efficiency while reaching higher model performance. The Decision Tree model receives training through the selected features which enables it to recognize the behavioral patterns of malicious and benign traffic.

The proposed system utilizes its training to examine incoming traffic data in real-time or batch mode to provide classifications of normal traffic or specific HTTP DDoS attack categories including TCP flood and UDP flood and SYN flood. Performance monitoring methods which combine accuracy, precision and recall measures enable the system to monitor new traffic patterns and adjust accordingly. The machine learning-based system surpasses rule-based methods through its ability to create comprehensive conclusions about new traffic types plus swift perception of fresh attack patterns. The system will gain additional reliability through hybrid or ensemble model development in its future iterations to create a scalable intelligent solution for SDN security enhancement.

VI. IMPLEMENTATION

Data Collection and Preprocessing

The first step involves obtaining a dataset containing DDoS traffic data together with normal traffic data. The available dataset contains diverse DDoS attack types including TCP flooding attacks with additional UDP flooding attacks as well as SYN flooding attacks and ICMP flooding attacks and DHCP flooding attacks. After data collection sweeps the data undergoes cleaning steps that include value completion for missing data and outlier correction and standardization across features. The encoding process handles categorical features because it improves model learning efficiency. At the same time normalization techniques standardize numerical features.

Feature Selection using Forward Feature Selection

Model accuracy receives enhancement and computational load decreases through the implementation of Forward Feature Selection. Forward Feature Selection begins its operation with an empty set of features which then incorporates one significant feature during each step to enhance model performance. The method selects DDoS-relevant features that play a crucial role in detection while removing unimportant attributes present in the dataset.

Model Selection and Training

For evaluation purposes three machine learning models namely Gaussian Naive Bayes, Support Vector Machine (SVM), and Decision Tree Classifier have been chosen. The training process of these models occurs with data from the filtered dataset. Special attention is dedicated to Decision Tree Classifier because it handles complex boundaries and gives interpretable results. The trainable models receive dataset with known labels to extract traffic behavior patterns during the training process.

Model Testing and Evaluation

The testing stage utilizes different data from the training data through a separate test set after training completes. The performance assessment utilizes accuracy as well as precision and recall and F1-score. Analysis of each

model's effectiveness depends on using both confusion matrices and classification reports. The Decision Tree Classifier demonstrated both the best accuracy performance and a superior balance between detection results and false positive occurrences which makes it optimal for this problem.

System Integration and Simulation

The Decision Tree Classifier becomes part of a simulated SDN environment once we select its most successful model. During real-time operations the system keeps tracking incoming network traffic while conducting immediate classification tasks. The system uses prediction results for malicious traffic detection and enables administrators to execute blocking IP addressing and traffic redirection as necessary security measures. The test simulation provides different network environments for evaluating the model's operation.

Comparative Results and Future Scope

A comparison between all three methods determines that Decision Tree Classifier presents optimal performance results. The SDN system demonstrates high effectiveness combined with precision and its ability to scale for DDoS detection applications. The system will benefit from future developments because multiple classifiers can be added into a hybrid learning model which enhances system reliability through lower false-negative rates. The implementation can be extended by developing a real-time deployment framework for an active SDN controller environment.

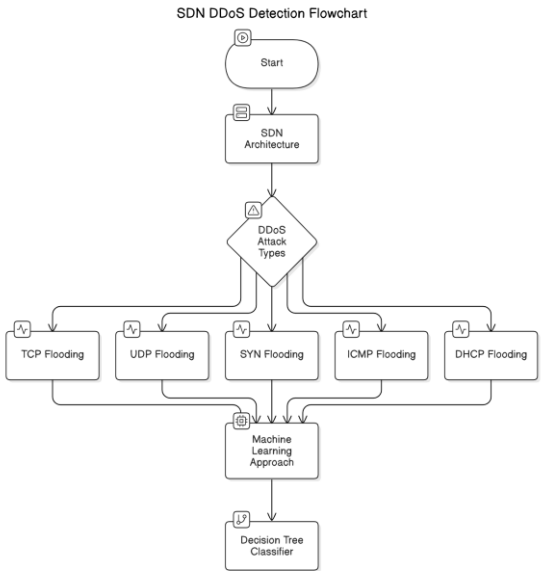

Fig.2. Workflow Diagram

RESULT

The implementation outcomes showed that the Decision Tree Classifier produced superior accuracy and reliability compared to other models for detecting DDoS attacks that occur in an SDN environment. The Decision Tree produced superior accuracy results than Gaussian Naive Bayes and Support Vector Machine while maintaining a better precision-recall equilibrium after the selected features received training and testing. The false negative rate highlighted in the confusion matrix remains critically low because it helps avoid missing attacks. The evaluation outcomes establish the effectiveness of Decision Tree for DDoS detection in real-time applications and support its potential introduction into SDN security platforms.

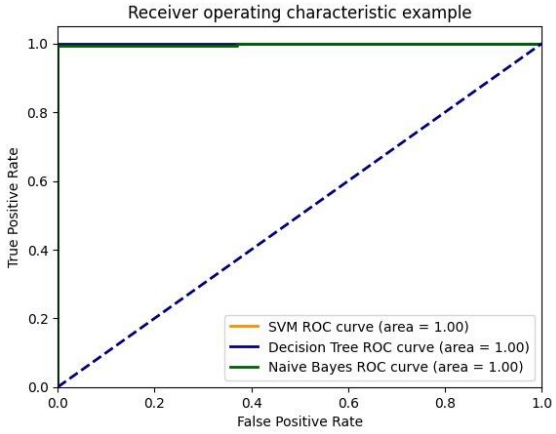

Fig. 3. Graph shows the ROC curve

```
# Compute ROC curve and area under the curve
sfpr, stpr, sthresholds = roc_curve(y_test, sprobas_[:, 1])
sroc_auc = auc(sfpr, stpr)
print("SVM Area under the ROC curve : %f" % sroc_auc)
# Compute ROC curve and area under the curve
dfpr, dtpr, dthresholds = roc_curve(y_test, dprobas_[:, 1])
droc_auc = auc(dfpr, dtpr)
print("Decision Tree Area under the ROC curve : %f" % droc_auc)
# Compute ROC curve and area under the curve
gfpr, gtpr, gthresholds = roc_curve(y_test, gprobas_[:, 1])
groc_auc = auc(gfpr, gtpr)
print("Gaussian Naive Bayes under the ROC curve : %f" % groc_auc)

SVM Area under the ROC curve : 0.997310
Decision Tree Area under the ROC curve : 1.000000
Gaussian Naive Bayes under the ROC curve : 0.997310
```

Fig. 4. Comparing Accuracy based on ROC Curve

```
    if y_test[i] == 0.0:
        if classifier_predictions[i] == 1.0:
            FD = FD + 1
        else:
            TN = TN + 1
#print("DD", DD , "DN", DN)
DR = DD / (DD + DN)
print("Detection rate ", DR)

#print("FD", FD , "TN", TN)
FAR = FD / (FD + TN)
print("False Alarm rate ", FAR)

Calculating Detection Ratio & False
Detection rate  1.0
False Alarm rate  0.6451612903225806
```

Fig. 5. Calculation of False Alarm Rate

CONCLUSION AND FUTURE ENHANCEMENTS

The project achieved successful deployment of a machine learning protocol which detects Distributed Denial of Service (DDoS) attacks in Software Defined Networking (SDN) environments by using Decision Tree Classifier. SDN achieves its flexibility through its control-data split and

centralized control yet creates weaknesses that cyber attackers can misuse. Our system detected and categorized different DDoS attack types such as TCP and UDP and SYN and ICMP flooding and DHCP flooding based on supervised learning models trained on network traffic records.

Through Forward Feature Selection the model gained efficiency due to its ability to select significant dataset features which simultaneously improved speed and prediction accuracy. The Decision Tree Classifier proved to be the most accurate model after testing with Gaussian Naive Bayes and Support Vector Machine because it offered superior interpretability and fewer incorrect negatives during detection. Real-time attack detection in dynamic SDN environments can be reliably performed using this model.

The developed system provides an essential foundation to enable progression toward creating superior security solutions for SDN environments. Future development will add ensemble systems to enhance the accuracy rates while enabling detection of changing cyber attack methods. An intelligent and autonomous SDN security framework can be developed by deploying real-time systems with automatic protection protocols.

REFERENCES

[1] S. Dasari and R. Kaluri, "An Effective Classification of DDoS Attacks in a Distributed Network by Adopting Hierarchical Machine Learning and Hyperparameters Optimization Techniques," *IEEE Access*, vol. 12, pp. 10834–10845, Jan. 2024, doi: 10.1109/ACCESS.2024.3352281.

[2] J. Halladay, D. Cullen, N. Briner, J. Warren, K. Fye, and R. Basnet, "Detection and Characterization of DDoS Attacks Using Time-Based Features," *IEEE Access*, vol. 10, pp. 49794–49807, May 2022, doi: 10.1109/ACCESS.2022.3173319.

[3] K. M. K. Raghunath, V. V. Kumar, M. Venkatesan, K. K. Singh, T. R. Mahesh, and A. Singh, "XGBoost Regression Classifier (XRC) Model for Cyber Attack Detection and Classification Using Inception V4," *Journal of Web Engineering*, vol. 21, no. 4, pp. 1295–1322, Jun. 2022, doi: 10.13052/jwe1540-9589.21413.

[4] A. Alsirhani, S. Sampalli, and P. Bodorik, "DDoS Detection System: Using a Set of Classification Algorithms Controlled by Fuzzy Logic System in Apache Spark," *IEEE Transactions on Network and Service Management*, vol. 16, no. 3, pp. 936–949, Sep. 2019, doi: 10.1109/TNSM.2019.2929425.

[5] C. Xu, H. Lin, Y. Wu, X. Guo, and W. Lin, "An SDNFV-Based DDoS Defense Technology for Smart Cities," *IEEE Access*, vol. 7, pp. 137856–137874, Sep. 2019, doi: 10.1109/ACCESS.2019.2943146.

[6] S. Naiem, A. E. Khedr, A. M. Idrees, and M. I. Marie, "Enhancing the Efficiency of Gaussian Naïve Bayes Machine Learning Classifier in the Detection of DDOS in Cloud Computing," *IEEE Access*, vol. 11, pp. 124597–124608, Oct. 2023, doi: 10.1109/ACCESS.2023.3328951.

[7] G. W. De Oliveira, M. Nogueira, A. L. dos Santos, and D. M. Batista, "Intelligent VNF Placement to Mitigate DDoS Attacks on Industrial IoT," *IEEE Transactions on Network and Service Management*, vol. 20, no. 2, pp. 1319–1331, Jun. 2023, doi: 10.1109/TNSM.2023.3274364.

[8] A. A. Alashhab, M. S. Zahid, B. Isyaku, A. A. Elnour, W. Nagmeldin, and A. Abdelmaboud, "Enhancing DDoS Attack Detection and Mitigation in SDN Using an Ensemble Online Machine Learning Model," *IEEE Access*, vol. 12, pp. 51630–51649, Apr. 2024, doi: 10.1109/ACCESS.2024.3384398.

[9] A. Hussain, E. M. Tordera, X. Masip-Bruin, and H. C. Leligou, "Rule-Based With Machine Learning IDS for DDoS Attack Detection in Cyber-Physical Production Systems (CPPS)," *IEEE Access*, vol. 12, pp. 114894–114911, Aug. 2024, doi: 10.1109/ACCESS.2024.3445261.

[10] 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, Dec. 2019, doi: 10.1109/ACCESS.2019.2963077.

[11] N. M. Yungaicela-Naula, C. Vargas-Rosales, and J. A. Perez-Diaz, "SDN-Based Architecture for Transport and Application Layer DDoS Attack Detection by Using Machine and Deep Learning," *IEEE Access*, vol. 9, pp. 108495–108512, Jul. 2021, doi: 10.1109/ACCESS.2021.3101650.

[12] C.S. Shieh, F.-A. Ho, M.-F. Horng, T.-T. Nguyen, and P. Chakrabarti, "Open-Set Recognition in Unknown DDoS Attacks Detection With Reciprocal Points Learning," *IEEE Access*, vol. 12, pp. 56461–56476, Apr. 2024, doi: 10.1109/ACCESS.2024.3388149.

[13] D. Saveetha, G. Maragatham, V. Ponnusamy, and N. Zdravković, "An Integrated Federated Machine Learning and Blockchain Framework With Optimal Miner Selection for Reliable DDOS Attack Detection," *IEEE Access*, vol. 12, pp. 127903–127915, Jun. 2024, doi: 10.1109/ACCESS.2024.3413076.

[14] R. F. Hayat, S. Aurangzeb, M. Aleem, G. Srivastava, and J. C.-W. Lin, "ML-DDoS: A Blockchain-Based Multilevel DDoS Mitigation Mechanism for IoT Environments," *IEEE Transactions on Engineering Management*, vol. 71, pp. 12605–12618, May 2022, doi: 10.1109/TEM.2022.3170519.

[15] W. I. Khedr, A. E. Gouda, and E. R. Mohamed, "FMDADM: A Multi-Layer DDoS Attack Detection and Mitigation Framework Using Machine Learning for Stateful SDN-Based IoT Networks," *IEEE Access*, vol. 11, pp. 28934–28954, Mar. 2023, doi: 10.1109/ACCESS.2023.3260256.