Journal of Telecommunication, Electronic and Computer Engineering
ISSN: 2180 – 1843 e-ISSN: 2289-8131 Vol. 16 No. 2
jtec.utem.edu.my
DOI: https://doi.org/10.54554/jtec.2024.16.02.002

Machine Learning-based Enhanced Deep Packet Inspection for IP Packet Priority Classification with Differentiated Services Code Point for Advance Network Management

Fazeel Ahmed Khan, Adamu Abubakar Ibrahim
Faculty of Information and Communication Technology, International Islamic University Malaysia, Kuala Lumpur, Malaysia.
fazeelahmedkhan15@gmail.com

Article Info

Article history:
Received Feb 4th, 2024
Revised Apr 2nd, 2024
Accepted May 20th, 2024
Published June 30th, 2024

Index Terms:
Deep Packet Inspection (DPI)
Differentiated Services Code - Point (DSCP)
Quality of Service (QoS)
Network Traffic Classification
Intelligent Packet Classification

Abstract

In modern networking, the efficient prioritization and classification of network traffic is paramount to ensure optimal network performance and optimization. This study presents an approach to enhance intelligent packet forwarding priority classification on Differentiated Services Code Point (DSCP), leveraging classifiers from machine learning algorithms for Deep Packet Inspection (DPI). The DSCP resides inside the Differentiated Services (DS) field of the Internet Protocol (IP) packet header in an OSI or TCP/IP model, which prioritizes different types of packets for forwarding to the router based on the attached payload. Similarly, DPI plays a crucial role in network management, enabling the identification of applications, services, and potential threats within the network traffic. In this study, various machine learning models, namely Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Decision Tree, Random Forest, Logistic Regression and ensemble models such as, XGBoost, AdaBoost were used to harness the capabilities of network packet classification based on DSCP. Detailed experimentation was conducted to evaluate their performance. The results show that AdaBoost demonstrated superior performance with an accuracy of around 89.91%, showcasing its ability to adapt the evolving network configurations and conditions while maintaining high classification accuracy on the IP packets. The random forest model also performed well, achieving an accuracy of 89.41%, making it a strong candidate for the DSCP classification in network transmission. This study has the potential to significantly improve how networks manage traffic, prioritize packets, and secure complex and dynamic network environments.

I. INTRODUCTION

Deep packet inspection (DPI) is a network security mechanism which examines the header and content of an IP packet as they travel across a network. It is used in modern network management to inspect packet headers and contents in detail, enabling the monitoring transmission within a network, identification and mitigation of malicious traffic, enforcement of security policies and gaining insight into network activities. DPI allows network administrators to monitor the network traffic flow and take necessary measures to prevent unusual activities inside the network, such as triggering alerts, blocking packets, re-routing traffic, and managing logs [1]. It is a fundamental technology for establishing baseline application behavior such as, analyzing network usage, preventing malicious code, detecting eavesdropping, enforcing censorship, and troubleshooting network performance issues. It functions as a packet inspection and filtering mechanism within the Open System Interconnected (OSI) application layer, acting as a part of the network firewall. The DPI evaluates packets header and payloads based on specific rules set by network administrators [2]. Furthermore, in the context of DPI, the concept of Quality of Service (QoS) is essential in managing traffic priority among various network protocols, ensuring a certain level of performance across different types of traffic. Similar to how highways prioritizes emergency vehicles for speedy response, QoS prioritizes critical traffic over less urgent traffic, providing a smooth and responsive experience for users. This is particularly important for real-time applications like VoIP, RTMP, HLS, DASH, as it helps to reduce congestion and latency. Additionally, a key element of QoS is the Differentiated Service Code Point (DSCP), which manages IP packet priority. DSCP is a 6-bit field (ranging from 0 – 63) within the IP header, specifically inside the Differentiated Services (DiffServ) of IPv6. It acts as a *traffic marker*, classifying packets based on the desired QoS treatment.

In addition, encryption is widely recognized as a crucial measure to ensure security and privacy in the network transmission. According to [3] there is an increasing trend in the use of encryption, with around 85% of global network traffic being encrypted. There are several encryption tools such as Transport Layer Security (TLS), Secure Socket Layer (SSL), Secure Shell Protocol (SSH), Internet Protocol Security (IPsec), and Pretty Good Privacy (PGP), having a leverage for both ymmetric and asymmetric methods of encryption using Advance Encryption Standard (AES) and RSA algorithms. The encryption provides a deep-level protection for application delivery and network management [4]. Similarly, it safeguards critical applications that handle sensitive information, which are susceptible to interception through packet sniffing. This security measure ensures that data remains confidential and protected from incoming cyber-attacks. Additionally, encryption offers a highly secure communication channel for individuals and companies, keeping data obscure and safe [5]. However, encryption also poses various challenges related to the visibility of information during network monitoring. These challenges can create bottleneck in identifying cyberattacks and implementing network traffic management policies, such as routing, application caching, content optimization and many others [6].

In earlier days, network operators and administrators deployed DPI engines and related network traffic management tools to monitor the network traffic processes [7]. However, with the increasing use of advanced encryption, traditional DPI tools struggle to meet the latest network traffic needs and requirements. This has resulted in the necessity for more advanced DPI methods capable of processing encrypted traffic using machine learning (ML) algorithms [8]. Similarly, machine learning (ML) is built on the concept of *features*, which are parameters within a dataset. By using ML algorithms, a machine can learn from a given set of data to produce intelligent outputs [9]. The primary purpose of using ML technology is to develop the capacity to analyze, predict and gain insights for the effective classification of network packets [10]. Moreover, integrating ML with DPI can significantly enhance network packet classification and traffic management domain, helping to overcome issues related to network traffic congestion, latency, and security.

In this proposed study, a hybrid model that includes both the ML and DPI is integrated. Specifically, the DPI is applied to the IP header field known as Differentiated Services Code Point (DSCP) within the header section of Differentiated Services (DiffServ). The proposed work addresses the four Per-Hop Behavior (PHB) levels of the DSCP packet forwarding, which are the Expediated Forwarding (EF), Assured Forwarding (AF), and Default Forwarding (DF). These are classified based on ML techniques to optimize how routers and switches handle IP packet priority.

II. TRAFFIC CLASSIFICATION, DIFFERENTIATED SERVICES AND QUALITY OF SERVICE

The Quality of Service (QoS) is a network traffic management mechanism designed to ensure optimal performance for critical applications, particularly those with limited network resource capacity [11]. It enables the network operators and administrators to optimize overall network traffic by prioritizing specific high-performance, resource-intensive applications [12]. QoS is applied to IP networks that carry traffic for computationally intensive applications such as online gaming, streaming media, video conferencing, internet television, Voice over IP (VoIP) [13].

Differentiated Services (DiffServ) is an extension of QoS in modern IP networks, which assigns priorities to each IP packet based on the network resource requirements [14]. It uses the DSCP from the DiffServ within the IP packet header and utilizes a class-based mechanism. This classification marks packets based on their origin, such as host devices or network management tools and assigns them to specific tools [15]. DiffServ operates on the principles of per-hob behavior (PHB), sorting each packet into a limited number of QoS marked classes [16]. Routers are then configured to forward traffic according to the rules set for the PHBs, ensuring higher priority packets are transmitted efficiently. This reduces packet loss, jitter, and bandwidth issues by prioritizing critical packets [17].

The DSCP resides within DiffServ at the network layer of the OSI model, which encapsulates the data into the form of packets [18]. The DSCP was earlier replaced with Type of Service (ToS) header field from the IPv4 packet header and replace with Traffic Class in the latest IPv6 packet header [19]. Once the network traffic is marked with DSCP, it is considered for classification and priority conditioning by network devices, such as routers and switches. Incoming packets are inspected with different parameters such as source address, destination address, and protocol type, which are assigned with specific traffic classes to individual packets [20]. However, a traffic classifier within the receiving router can consider, ignore, or override these markings. Network administrators can also apply policies, like rate limiting, traffic compliance, and bandwidth management [21].

Similarly, the per-hop behavior (PHB) in a packet is determined by the DiffServ inside the IP header [22]. The DiffServ field consists of a 6-bit of DSCP value, allowing for up to 64 different classes, each represented by a DSCP value, which is identical in number [23]. However, in real-world environments, PHB typically falls into the following categories: the default forwarding (DF), expediated forwarding (EF), and assured forwarding (AF) [24]. DF implies that the router will make its best effort to forward the packet. However, there is a significant risk of packet dropping or higher loss of packet in DF [25]. Expediated forwarding (EF) is dedicated to minimizing packet dropping risk and ensuring low latency in traffic forwarding by the routers [26]. Assured forwarding (AF) provides a guarantee that the packet will be forwarded with high priority, reducing the risk of packet dropping and ensuring low latency [27]. AF is further divided into three classes of AF behavior group category: low, medium, and high [28]. The detailed orientation of PHB categories is shown in Figure 1.

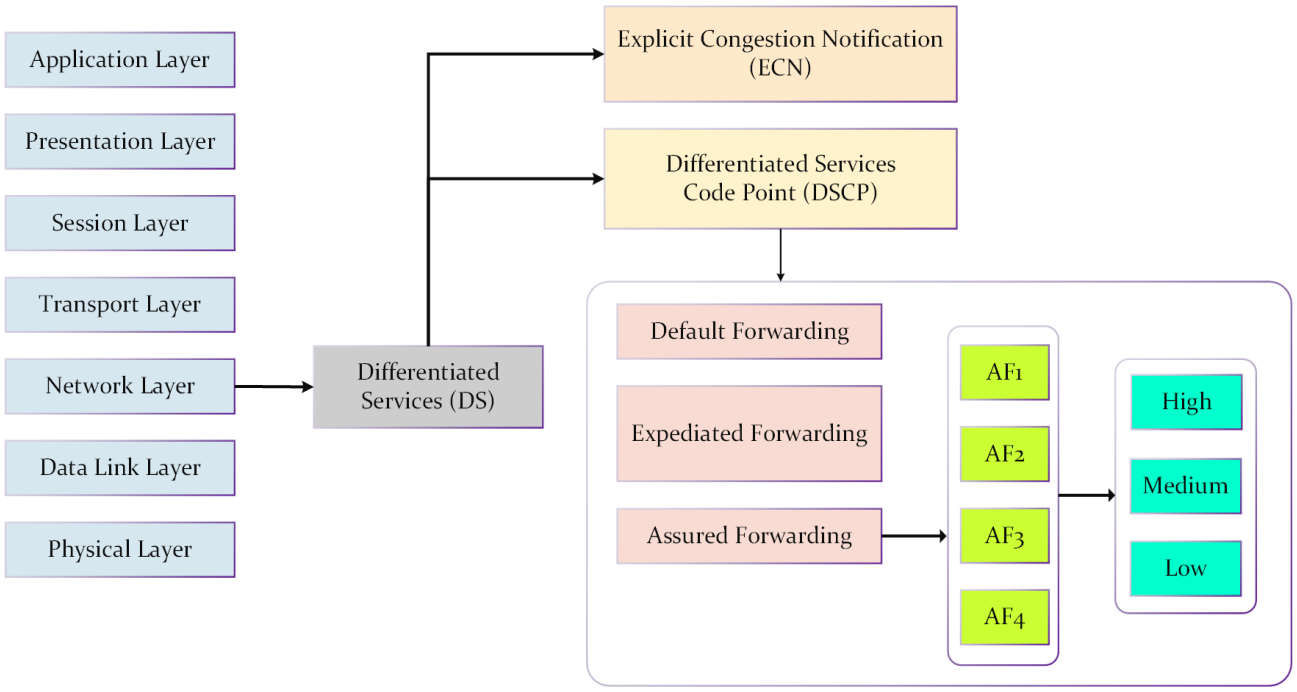

Figure 1. Per-Hop Behavior and Differentiated Service Code Point in OSI layer model

III. METHODOLOGY

The research design comprises of three stages, which includes dataset development, data-pre-processing and model development as shown in the Figure 2. Following the initial stages of dataset development, the research delves into a comprehensive exploration of the collected data. The dataset reflects real-time network interactions, which were meticulously gathered from a dynamic network environment using widely recognized network sniffing tool, notably Wireshark [29]. The captured data, initially in PCAP format and stored in binaries, was converted into a more accessible CSV format using built-in tools from Wireshark. This resulted in an extensive dataset comprising 1,16,315 rows of data. To enhance the richness and versatility of the dataset, an additional layer of refinement was applied through the utilization of various data-processing steps. The refined dataset encapsulates a myriad of essential IP-related fields, each contributing valuable insights into the intricacies of network activities. Table 1 provides an overview of the included IP fields, showcasing the depth and breadth of information available for analysis and modeling. This meticulous approach for dataset development and refinement lay a solid foundation for subsequent stages, ensuring the data used in the research is not only extensive, but also well-prepared for the challenges of model development and analysis.

The subsequent stage involves data preprocessing, which is a critical phase aimed at refining and enhancing the quality of gathered information. This involves various measures of implementation, such as handling of missing values and the extracting pertinent features respectively. Notably, the absence of missing values highlights the robustness of the dataset, signifying a meticulous data collection process and contributing to the overall reliability of the research. With missing values addressed, the focus shifted to feature extraction, a process pivotal in distilling the relevant information required for model development.

Table 1
IP Header Field in the dataset

IPv4	IPv6
Version	Version
IHL (Internet Header Length)	Traffic Class
Type of Service (ToS)	Flow Label
Total Length	Payload Length
Identification	Next Header
Flags	Hop Limit
Time to Live	Source Address
Protocol	Destination Address
Header Checksum	Payload
Source Address	
Destination Address	
Payload	

Two key features were extracted during this phase, namely the protocols and Differentiated Services Code Point classes (DSCP). The former provides insights into the communication protocols associated with the network packet, while the latter categorizes the packets based on their DSCP classes. These extracted features serve as the building blocks for the subsequent modeling and analysis, offering a concise yet comprehensive representation of the dataset. To provide a clear understanding of the refined dataset and its extracted features, Table 2 presents a detailed list of protocols alongside their respective counts. This enumeration offers a valuable insight into the prevalence of each protocol within the dataset, laying the groundwork for further analysis. Simultaneously, Table 3 provides an analogous breakdown for DSCP classes, showcasing the distribution and frequency of different DSCP classifications within the dataset.

In the model development phase, the research harnessed the power of six distinct machine learning algorithms, each carefully selected for its unique strengths and capability in the context of DSCP classification. The ensemble of algorithms comprised of Support Vector Machine (SVM), Logistic

Regression, Decision Tree, K-Nearest Neighbors (KNN), XGBoost and AdaBoost respectively.

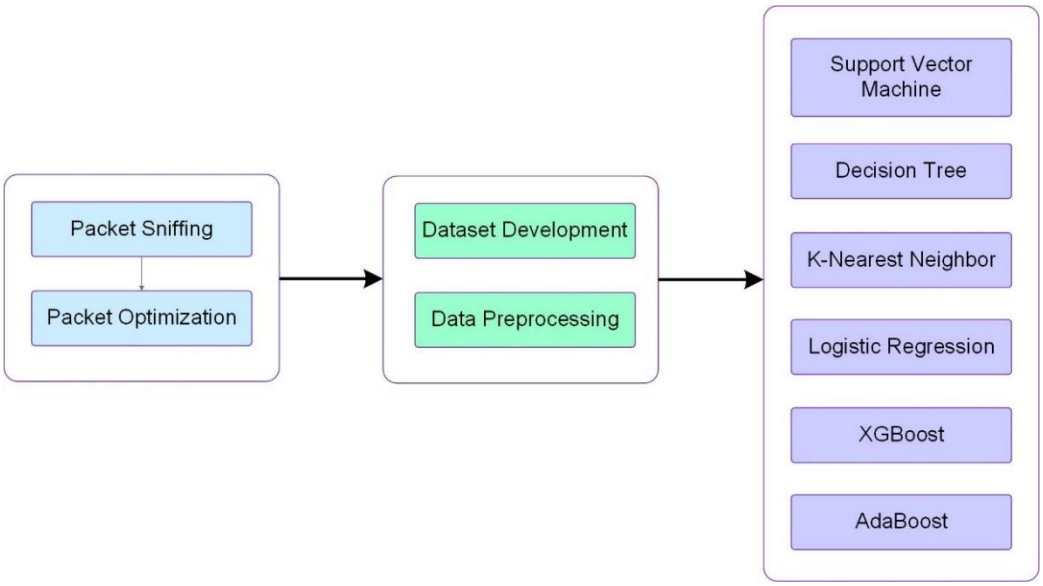

Figure 2. Packet Classification Methodology

This diverse selection enables a comprehensive exploration of various modeling approaches, ensuring a thorough evaluation of their effectiveness in classifying DSCP within the network packet and transmission flow.

The SVM is a powerful algorithm known for its capability to handle both linear and non-linear classification tasks [30]. In the context of DSCP classification, SVM was employed to create a decision boundary that effectively separates different DSCP classes. Its ability to handle high-dimensional data and uncover complex relationships made it invaluable for discerning patterns within the dataset. Further, logistic regression, commonly used for binary classification tasks, was adapted to handle multiple classes (multinomial approach) for DSCP classification. The logistic regression algorithm models the probability that a packet belongs to a particular DSCP class based on its features. It uses the logistic function to transform the output into a probability distribution across different classes [31]. Its simplicity, interpretability, and efficiency make it a valuable addition to the suite of machine learning algorithms, providing insights into the likelihood of a packet belonging to a specific DSCP class based on individual features.

K-Nearest Neighbors (KNN) is a versatile algorithm which classifies data points based on the majority class among their K-Nearest Neighbors [32]. In DSCP classification, KNN was applied to identify similarities between network packets, assigning a DSCP class based on the classes of neighboring packets. This approach leveraged spatial relationships within the dataset. Extreme Gradient Boosting (XGB) is an ensemble learning model employed to build a strong predictive model by combining multiple weak models [33]. In DSCP classification, XGB excelled in handling complex relationships within the data, providing a robust and accurate model by boosting the performance of individual weak learners. The random forest creates an ensemble of decision trees and aggregates their predictions to improve the overall accuracy and generalization [34]. In the context of DSCP classification, it excelled at handling complex interactions among features and mitigate the issue of overfitting. It operates by constructing multiple decision trees during training and outputs the model of the classes predicted by the individual trees. Each decision tree is constructed using a random subset of the dataset and a random subset of features, introducing diversity among the constituent trees. Lastly, the AdaBoost focuses on the combination of predictions of multiple weak learners to form a strong classifier [35]. In the DSCP classification, it iteratively adjusted the weights of misclassified instances, emphasizing challenging cases and enhancing the overall model's performance. Its adaptability and ability to handle diverse datasets made it valuable inclusion in the model ensemble.

Table 2
List of Protocols and their counts in the dataset

Protocols	Count
QUIC	84187
TCP	17947
TLSv1.3	8954
DNS	1272
UDP	1030
SRTP	875
TLSv1.2	768
ICMPv6	286
SRTCP	213
MDNS	192
SSDP	164
ARP	140
IGMPv3	61
DTLSv1.2	50
ICMP	43
STUN	38
LLMNR	30
HTTP	24
OCSP	12
DHCP	9
DHCPv6	8
TLSv1	4
SSLv2	4
IGMPv2	4

Table 3
List of DSCP classes and their counts in the dataset

DSCP Classes	Priority	Count
CS0	Low	93371
CS4	Medium	12713
CS2	Medium	7031
AF31	High	1620
AF41	High	1327
CS3	Medium	103
CS6	Medium	10

IV. EXPERIMENTAL ANALYSIS AND RESULT

The experimental analysis and results phase involves evaluating the accuracy and classification performance based on positive and negative values. In the context of DSCP classification, the performance of various classification algorithms such as, SVM, Decision Tree, Random Forest, Logistic Regression, KNN, XGBoost and AdaBoost was evaluated based on their confusion matrices. The confusion matrix provides a detailed insight into the model's classification performance by breaking down predictions into true positives (TP), false positives (FP), true negatives (TN) and false negatives (FN). Table 4 summarizes the model analysis based on accuracy, precision and recall percentages respectively.

The classification performance of these algorithms in the context of DSCP was thoroughly analyzed using metrics, such as accuracy, precision, and recall with a detail analysis of their confusion matrices. To begin with the SVM model, it achieved accuracy, precision, and recall of 88.59%. The confusion matrix highlighted that 88.59% of instances belonging to the DSCP class were correctly classified (TP), indicating a well-balanced performance in terms of both precision and recall. Only 11.41% of instances were misclassified (FP and FN), demonstrating the model's ability to make accurate predictions. Furthermore, the decision tree model exhibited accuracy, precision, and recall of 89.25%. The confusion matrix revealed that 89.25% of DSCP instances were accurately identified, showcasing a consistent and well-balanced classification performance. The model demonstrated its reliability across different aspects of classification, maintaining steady precision and recall values. Moreover, the random forest model demonstrated accuracy, precision, and recall of 89.41%. The confusion matrix showed that a significant majority of instances were correctly classified, emphasizing the effectiveness of the ensemble approach in reducing misclassifications. This highlighted the robustness of the random forest model in DSCP classification. Additionally, the logistic regression model achieved accuracy, precision, and recall of 88.89%. The confusion matrix showed a well-balanced classification performance, with nearly 89.89% of DSCP instances correctly identified. The model demonstrated consistency in both precision and recall, affirming its reliability in predicting DSCP classes accurately. The confusion matrices visualization is shown in Figure 3 and 4 respectively. The KNN model demonstrated competitive performance with an accuracy, precision, and recall of 89.23%. The confusion matrix emphasized the model's effectiveness in identifying a large number of DSCP instances, contributing to its overall accuracy. The well-aligned precision and recall values indicated a balanced trade-off between false positives and false negatives. Similarly, the XGBoost model exhibited accuracy, precision, and recall of 89.69%, emphasizing its robust performance in DSCP classification.

Table 4
Summary of Model's Classification Performance and Analysis

Model	Accuracy (%)	Precision (%)	Recall (%)
SVM	88.59	88.59	88.59
Decision Tree	89.25	89.25	89.25
Random Forest	89.41	89.41	89.41
Logistic Regression	88.89	88.89	88.89
KNN	89.23	89.23	89.23
XGBoost	89.69	89.69	89.69
AdaBoost	89.91	89.91	89.91

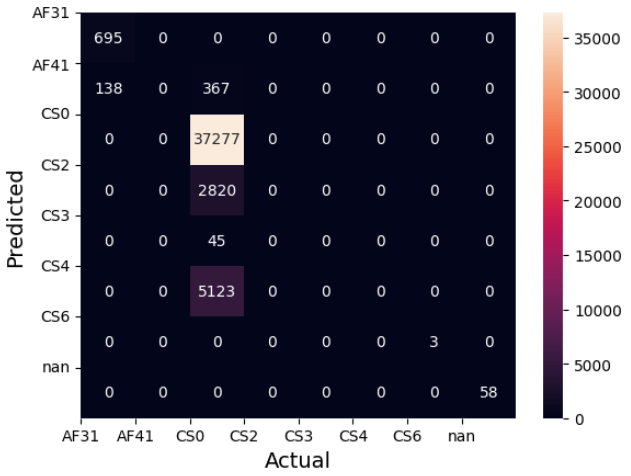

Figure 3 (a). Visuals of SVM Confusion Matrix

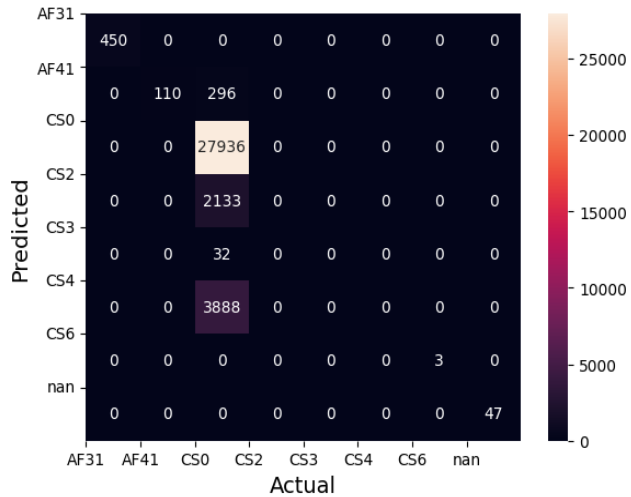

Figure 3 (b). Visuals of Decision Tree Confusion Matrix

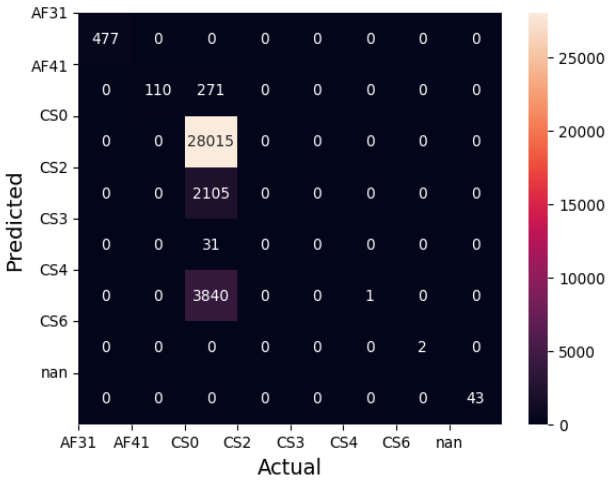

Figure 4 (a). Visuals of Random Forest Confusion Matrix

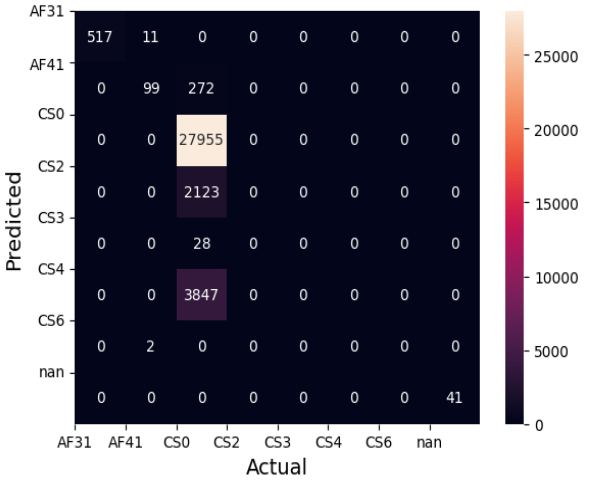

Figure 4 (b). Visuals of Logistic Regression Confusion Matrix

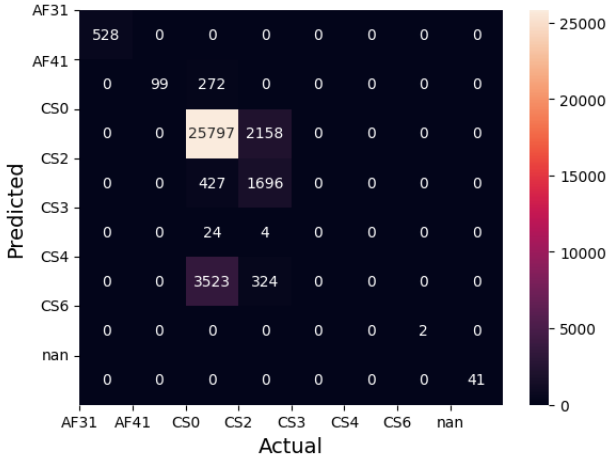

Figure 5 (a). Visuals of KNN Confusion Matrix

The confusion matrix highlighted a high proportion of true positive predictions, showcasing its effectiveness in DSCP classification. The model maintained a balance between precision and recall, maintaining its reliability. Lastly, the AdaBoost model has achieved an accuracy, precision, and recall of 89.91%. The confusion matrix demonstrated the model's excellence in correctly identifying DSCP instances, with a high proportion of true positives.

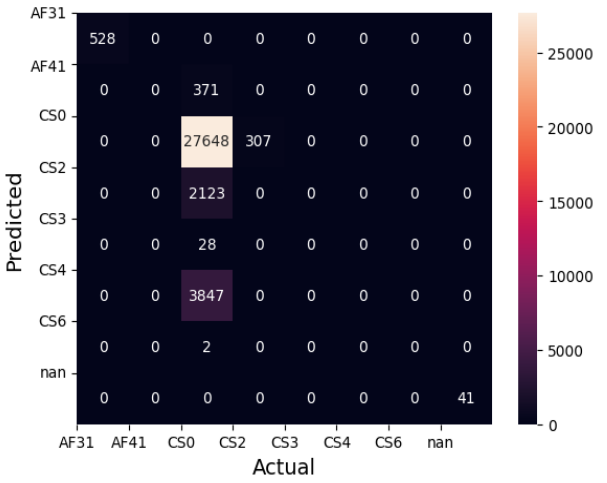

Figure 5 (b). Visuals of XGBoost Confusion Matrix

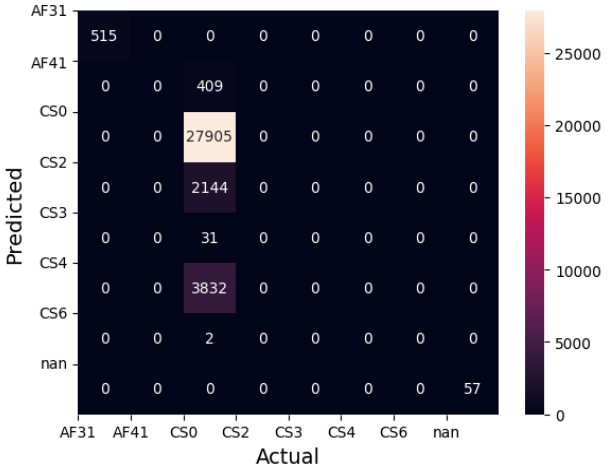

Figure 6. Visualization of AdaBoost Confusion Matrix

The AdaBoost's ensemble learning approach contributed to its superior performance in DSCP classification, emphasizing its potential as a powerful classifier in this context. The confusion matrices visualization is shown in Figure 5 and 6 respectively. In summary, each algorithm exhibited strong performance in DSCP classification, with accuracy, precision, and recall metrics providing a comprehensive evaluation of their capabilities. The detailed examination of confusion matrices further enriched the understanding of the strengths and generalization capabilities of each algorithm in the specific context of DSCP classification.

V. CONCLUSION

In conclusion, this study delved into the realm of Deep Packet Inspection (DPI) within network management, focusing on the classification of Differentiated Services Code Point (DSCP) to enhance Quality of Service (QoS). The introduction provides a comprehensive overview of DPI's role in network security, emphasizing its significance in monitoring and mitigating malicious traffic, enforcing security policies, and gaining insights into network activities. The motivation for incorporating machine learning (ML) algorithms alongside DPI addressed the limitations of traditional DPI tools in handling network traffic. The proposed hybrid model integrating ML and DPI and specifically applied to DSCP in IP headers, offered a novel

approach to addressing challenges associated with traffic classification, congestion, latency, and security in modern network environments. The methodology section outlined a detailed research design, encompassing stages such as dataset development, data pre-processing, and model development. The inclusion of six distinct ML algorithms, including SVM, Logistic Regression, Decision Tree, KNN, XGBoost, and AdaBoost, demonstrated a comprehensive exploration of modeling approaches. Moreover, the experimental analysis and results provided a detailed evaluation of the performance of each algorithm in DSCP classification, showcasing higher accuracy, precision, and recall values. The confusion matrices offered a granular understanding of the model's capabilities, emphasizing their effectiveness in correctly classifying DSCP instances. The visualization of confusion matrices further enriched the analysis, providing a detailed insight into true positives, false positives, true negatives, and false negatives. The SVM model demonstrated robustness with an accuracy of 88.59% and a well-balanced precision-recall trade-off, accurately classifying 88.59% of DSCP instances. Similarly, the decision tree and random forest models achieved accuracies of 89.25% and 89.41% respectively, resulting in reliable performance and effective reduction of misclassifications. Furthermore, the logistic regression model achieved an accuracy of 88.89% with a well-balanced classification performance. This comprehensive analysis contributes to the advancement of DPI applications in network management, particularly in the context of QoS enhancement through DSCP classification. The integration of ML algorithms with DPI for DSCP classification presents a promising avenue for improving network traffic management, security, and performance. In addition to the current findings, there are several areas where future research that could enhance the understanding and application of classification algorithms in the context of DSCP can be conducted. A potential area for further exploration is the refinement of the classifier performance through the optimization of hyperparameters and feature selection techniques. Fine-tuning the parameters of the models, such as kernel functions in SVM or tree depth in decision trees, could potentially improve classification accuracy and address any limitations identified in this study. The research findings underscore the potential of the proposed hybrid model in addressing contemporary challenges in network environments, paving the way for more robust and adaptive approaches to DPI and QoS optimization.

ACKNOWLEDGMENT

This research is supported by UMP-IIUM Sustainable Research Collaboration Grant 2022 (IUMP-SRCG), Research Project IUMP-SRCG22-014-0014.

REFERENCES

[1] R. T. El-Maghraby, N. M. A. Elazim and A. M. Bahaa-Eldin, "A survey on deep packet inspection," in Proc. of 2017 12th International Conference on Computer Engineering and Systems (ICCES), 2017.

[2] J. Sherry, C. Lan, R. A. Popa and S. Ratnasamy, "BlindBox: deep packet inspection over encrypted traffic," in Proc. of 2015 ACM Conference on Special Interest Group on Data Communication, 2015.

[3] N. Shah, "The Challenges of Inspecting Encrypted Network Traffic", Accessed: Oct. 5, 2023, [Online]. Available: https://www.fortinet.com/blog/industry-trends/keeping-up-with-performance-demands-of-encrypted-web-traffic

[4] C. Xu, S. Chen, J. Su, S. M. Yiu and L. C. K. Hui, "A survey on regular expression matching for deep packet inspection: applications, algorithms, and hardware platforms," IEEE Communications Surveys & Tutorials, vol. 18, no. 4, pp. 2991-3029, 2016.

[5] G. D. L. T. Parra, P. Rad and K.-K. R. Choo, "Implementation of deep packet inspection in smart grids and industrial Internet of Things: Challenges and opportunities," Journal of Network and Computer Applications, vol. 135, no. 1, pp. 32-46, 2019.

[6] M. Al-hisnawi and M. Ahmadi, "Deep packet inspection using quotient filter," IEEE Communications Letters , vol. 20, no. 11, pp. 2217-2220, 2016.

[7] W. Song, M. Beshley, K. Przystupa, H. Beshley, O. Kochan, A. Pryslupskyi, D. Pieniak and J. Su, "A software deep packet inspection system for network traffic analysis and anomaly detection," Sensors, vol. 20, no. 6, pp. 1637, 2020.

[8] J. Hypolite, J. Sonchack, S. Hershkop, N. Dautenhahn, A. DeHon and J. M. Smith, "DeepMatch: practical deep packet inspection in the data plane using network processors," in Proc. of the 16th International Conference on emerging Networking EXperiments and Technologies, 2020.

[9] J. Fan, C. Guan, K. Ren, Y. Cui and C. Qiao, "SPABox: safeguarding privacy during deep packet inspection at a middlebox," IEEE/ACM Transactions on Networking, vol. 25, no. 6, pp. 3753-3766, 2017.

[10] R. Sun, L. Shi, C. Yin and J. Wang, "An improved method in deep packet inspection based on regular expression," The Journal of Supercomputing, vol. 75, pp. 3317-3333, 2019.

[11] M. Karakus and A. Durresi, "Quality of service (QoS) in software defined networking (SDN): a survey," Journal of Network and Computer Applications, vol. 80, pp. 200-218, 2017.

[12] M. Faheem, G. Tuna and V. C. Gungor, "QERP: quality-of-service (QoS) aware evolutionary routing protocol for underwater wireless sensor networks," IEEE Systems Journal, vol. 12, no. 3, pp. 2066-2073, 2018.

[13] T. Mazhar, M. A. Malik, S. A. H. Mohsan, Y. Li, I. Haq, S. Ghorashi, F. K. Karim and S. M. Mostafa, "Quality of service (QoS) performance analysis in a traffic engineering model for next-generation wireless sensor networks," Symmetry, vol. 15, no. 2, pp. 513, 2023.

[14] A. A. Nacer, K. Bessai, S. Youcef and C. Godart, "A multi-criteria based approach for web service selection using quality of service (QoS)," in Proc. of 2015 IEEE International Conference on Services Computing, 2015.

[15] M. Nkongolo, J. P. v. Deventer and S. M. Kasongob, "Using deep packet inspection data to examine subscribers on the network," Procedia Computer Science , vol. 215, pp. 182-191, 2022.

[16] K. M. Malikovich, G. S. Rajaboevich, T. S. Sobirovna and E. Temurmalik, "Differentiated services code point (DSCP) traffic filtering method to prevent attacks," in Proc. of 2021 International Conference on Information Science and Communications Technologies (ICISCT), 2021.

[17] R. Barik, M. Welzl, A. Elmokashfi, T. Dreibholz, S. Islam and S. Gjessing, "On the utility of unregulated IP diffserv code point (DSCP) usage by end systems," Performance Evaluation, vol. 135, pp. 102036, 2019.

[18] A. Custura, R. Secchi and G. Fairhurst, "Exploring DSCP modification pathologies in the Internet," Computer Communications, vol. 127, pp. 86-94, 2018.

[19] N. Roddav, K. Streit, G. D. Rodosek and A. Pras, "On the usage of DSCP and ECN codepoints in internet backbone traffic traces for IPv4 and IPv6," in Proc. 2019 International Symposium on Networks, Computers and Communications (ISNCC), 2019.

[20] R. Barik, M. Welzl, A. M. Elmokashfi, T. Dreibholz and S. Gjessing, "Can webRTC QoS work? A DSCP measurement study," in Proc. of 2018 30th International Teletraffic Congress (ITC 30), 2018.

[21] A. Custura, A. Venne and G. Fairhurst, "Exploring DSCP modification pathologies in mobile edge networks," in Proc. of 2017 Network Traffic Measurement and Analysis Conference (TMA), 2017.

[22] A. k. Jabbar, B. Karimi, T. M. Jamel and A. Abood, "QoS mapping method based on DSCP/IP in LTE and EDCA AC/MAC in WiFi network," in Proc. of 2019 12th International Conference on Developments in eSystems Engineering (DeSE), 2019.

[23] L. F. Hussein, A.-H. A. Hashim, M. H. Habaebi and W. H. Hassan, "A QoS awareness scheme sustaining seamless handover for network mobility," Indian Journal of Science and Technology, vol. 9, 2016.

[24] O. N. Nyasore, P. Zavarsky, B. Swar, R. Naiyeju and S. Dabra, "Deep packet inspection in industrial automation control system to mitigate attacks exploiting modbus/TCP vulnerabilities," in Proc. of 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and

Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), 2020.

[25] C. Yu, J. Lan, J. Xie and Y. Hu, "QoS-aware traffic classification architecture using machine learning and deep packet inspection in SDNs," Procedia Computer Science, vol. 131, pp. 1209-1216, 2018.

[26] H. Ren, H. Li, D. Liu, G. Xu, N. Cheng and X. Shen, "Privacy-preserving efficient verifiable deep packet inspection for cloud-assisted middlebox," IEEE Transactions on Cloud Computing, vol. 10, no. 2, pp. 1052-1064, 2022.

[27] P. Khandait, N. Hubballi and B. Mazumdar, "Efficient keyword matching for deep packet inspection based network traffic classification," in Proc. of 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), 2020.

[28] G. Li, M. Dong, K. Ota, J. Wu, J. Li and T. Ye, "Deep packet inspection based application-aware traffic control for software defined networks," in Proc. of 2016 IEEE Global Communications Conference (GLOBECOM), 2016.

[29] Wireshark Foundation, "Wireshark," Accessed: April 2024 [Online]. Available: https://www.wireshark.org/

[30] S. Ghosh, A. Dasgupta and A. Swetapadma, "A study on support vector machine based linear and non-linear pattern classification," in Proc. of 2019 International Conference on Intelligent Sustainable Systems (ICISS), 2019.

[31] Q. Cheng, P. Varshney and M. Arora, "Logistic regression for feature selection and soft classification of remote sensing data," IEEE Geoscience and Remote Sensing Letters, vol. 3, no. 4, pp. 491-494, 2006 .

[32] G. Guo, H. Wang, D. Bell, Y. Bi and K. Greer, "KNN model-based approach in classification," in Proc. of OTM Confederated International Conferences "On the Move to Meaningful Internet Systems", 2003.

[33] X. Ren, H. Guo, S. Li, S. Wang and J. Li, "A novel image classification method with CNN-XGBoost model," in Proc. of Digital Forensics and Watermarking, 2017.

[34] J. L. Speiser, M. E. Miller, J. Tooze and E. Ip, "A comparison of random forest variable selection methods for classification prediction modeling," Expert Systems with Applications, vol. 134, pp. 93-101, 2019.

[35] P. Dou, Y. Chen and H. Yue, “Remote-sensing imagery classification using multiple classification algorithm-based AdaBoost,” International Journal of Remote Sensing, vol. 39, no. 3, pp. 619-639, 2018.