IJNRD.ORG ISSN : 2456-4184

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG

An International Open Access, Peer-reviewed, Refereed Journal

Enhancing Network Management Through Machine Learning in Software-Defined Networking

Hemant Kumar Bhardwaj, Arvind Panwar
Asst.Professor
R.D.Engineering College Ghaziabad

ABSTRACT

The increasing diversification of Internet applications and the ongoing evolution of network infrastructure, fueled by emerging technologies, have introduced complexities to network management. Effectively classifying network traffic is crucial for managing network resources based on quality of service and security requirements. However, conventional traffic classification methods relying on Deep Packet Inspection fall short of meeting the demanding scalability, security, and privacy criteria. The centralized controller in Software-Defined Networking offers a comprehensive network view, easing traffic analysis and providing direct programming capabilities. This allows for dynamic adjustments of traffic flows to meet evolving network requirements. The integration of Machine Learning techniques, along with these features, enables the infusion of intelligence into networks, optimizing their performance and enhancing management and maintenance. In this context, our work aims to conduct a Systematic Literature Review on traffic classification in Software-Defined Networking using Machine Learning techniques. Additionally, we systematically analyze and organize the chosen seminal works based on the categorization of traffic classes and the employed Machine Learning techniques, drawing meaningful research conclusions. Finally, we identify new challenges and propose future research directions in this domain.

KEYWORDS:*SDN (Software-Defined Networking,) Machine Learning Integration, Traffic Classification, Evolution Network Management, Optimization Intelligent*

INTRODUCTION

The landscape of Internet applications is undergoing a profound transformation, marked by an unprecedented diversification and the relentless evolution of network infrastructure driven by emerging technologies. This paradigm shift has introduced a myriad of challenges to network management, prompting the need for innovative solutions that can adapt to the dynamic demands of modern networking environments. Central to this challenge is the efficient classification of network traffic—a pivotal enabler for the judicious allocation of resources, meeting quality of service (QoS) benchmarks, and ensuring robust security measures.

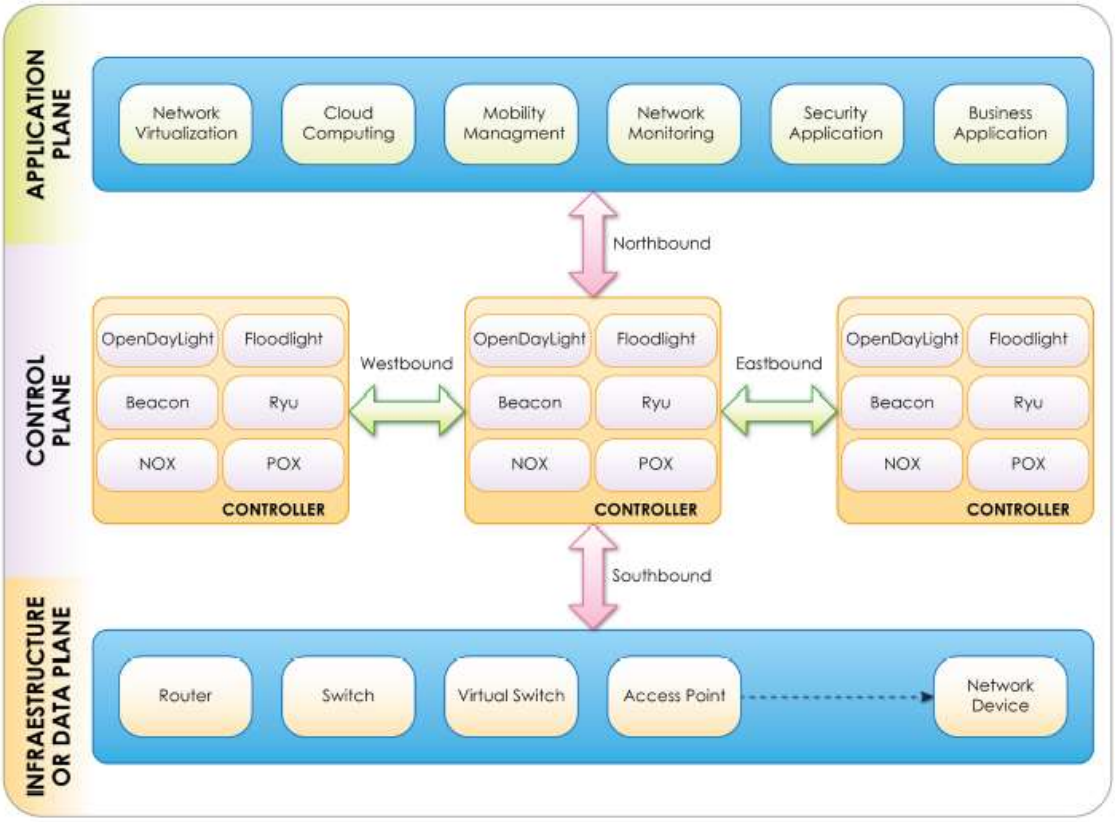

Fig. 1. Software-Defined Networking Architecture.

As traditional methods based on Deep Packet Inspection grapple with limitations related to scalability, security, and privacy, the emergence of Software-Defined Networking (SDN) has paved the way for a new era of intelligent network management. SDN's centralized controller provides a holistic perspective on the network, simplifying traffic analysis and endowing network administrators with direct programming capabilities. The dynamic adjustment of traffic flows in response to evolving network requirements becomes not only feasible but efficient.A critical aspect of this evolution is the integration of Machine Learning (ML) techniques into the fabric of SDN. This synergy between SDN and ML has given rise to intelligent networks capable of self-optimization, adaptation, and enhanced management and maintenance.

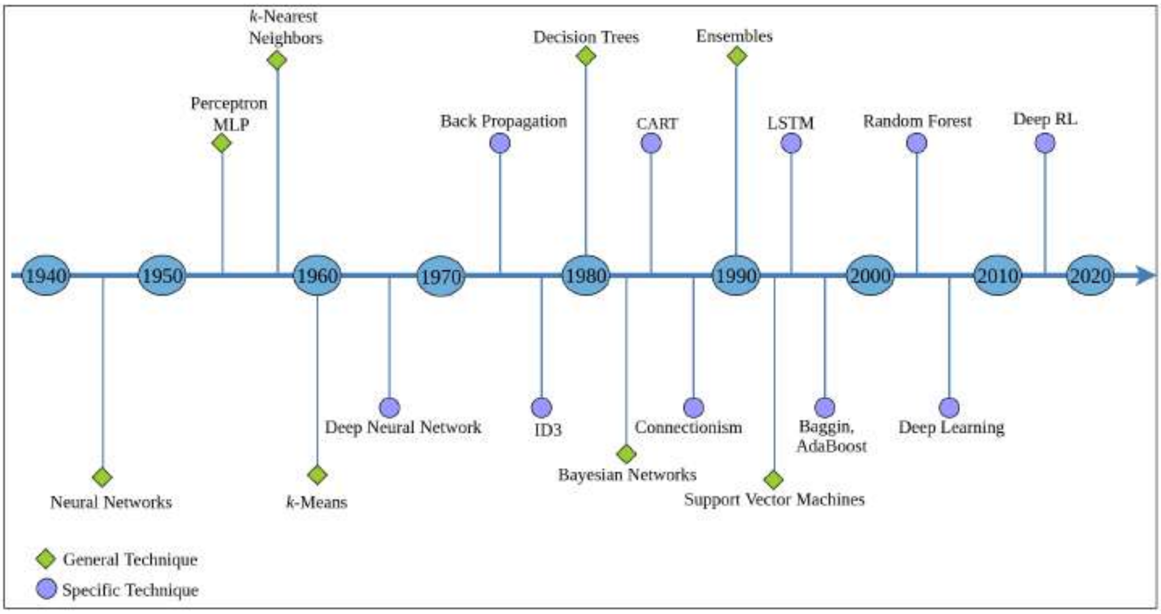

Figure 2 : Evolution of Machine Learning Technique

In this context, our work endeavors to delve into this transformative intersection by conducting a comprehensive Systematic Literature Review on traffic classification in Software-Defined Networking, focusing specifically on the integration of Machine Learning techniques.

Background

The contemporary digital landscape is characterized by a multitude of Internet applications, each with its unique set of requirements and challenges. From real-time communication platforms and cloud-based services to Internet of Things (IoT) devices and multimedia streaming, the diversity of applications places a strain on traditional network management practices. Moreover, the continuous evolution of network infrastructure, driven by the deployment of cutting-edge technologies such as 5G, edge computing, and network virtualization, further complicates the task of maintaining an efficient and secure network.

As network traffic becomes increasingly dynamic and heterogeneous, the need for a sophisticated traffic classification mechanism becomes apparent. Network administrators must be equipped with tools that not only discern the nature of the traffic but also enable them to allocate resources judiciously, ensuring optimal performance for critical applications while maintaining a secure environment.

Challenges of Traditional Traffic Classification Methods

Deep Packet Inspection (DPI), a conventional method for traffic classification, has been instrumental in understanding the content of data packets traversing the network. However, as networks grow in scale and complexity, DPI encounters significant challenges. Scalability is a primary concern, as the exhaustive analysis of every packet in large-scale networks becomes computationally intensive and resource-demanding.

Moreover, traditional DPI methods raise security and privacy concerns. The in-depth inspection of packet payloads may inadvertently expose sensitive information, violating user privacy and potentially compromising the confidentiality of data. Additionally, as cyber threats evolve, DPI may struggle to keep pace with emerging attack vectors, necessitating a more adaptive and intelligent approach to traffic classification.

The Role of Software-Defined Networking in Network Transformation

In response to the limitations of traditional networking paradigms, Software-Defined Networking (SDN) has emerged as a transformative architecture. At the heart of SDN is a centralized controller that serves as the brain of the network, offering a unified view and control over the entire infrastructure. This departure from traditional distributed control architectures empowers network administrators with unprecedented flexibility and programmability.

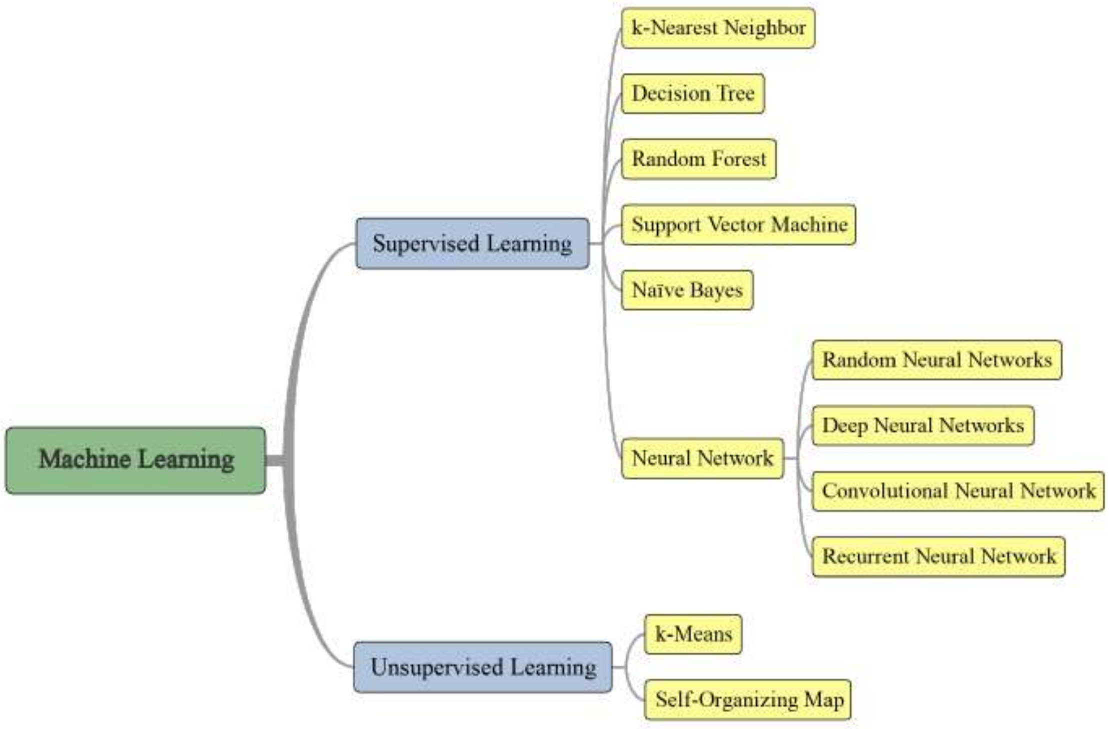

Fig. 3. ML techniques in Software-Defined Networking.

SDN's centralized control plane not only simplifies network management but also opens avenues for real-time traffic analysis and dynamic adaptation. By decoupling the control plane from the data plane, SDN enables a more responsive and agile network architecture, where traffic flows can be dynamically adjusted to meet changing requirements. This inherent adaptability aligns with the dynamic nature of modern Internet applications and positions SDN as a key enabler for intelligent network management.

The Convergence of Software-Defined Networking and Machine Learning

The transformative potential of SDN becomes even more pronounced with the integration of Machine Learning (ML) techniques. Machine Learning, a subset of artificial intelligence, equips networks with the ability to learn from data patterns, predict future trends, and make informed decisions without explicit programming. The synergy between SDN and ML presents a paradigm shift in network intelligence, enabling networks to evolve from being static and rule-driven to dynamic, adaptive, and intelligent entities.

By leveraging ML, SDN can optimize network performance, predict and mitigate security threats, and automate routine management tasks. Traffic classification, a cornerstone of network management, stands to benefit significantly from ML techniques. The ability to discern patterns, anomalies, and trends in network traffic enhances the accuracy and efficiency of classification, addressing the shortcomings of traditional DPI methods.

In light of the transformative potential of the convergence between Software-Defined Networking and Machine Learning, our work aims to provide a comprehensive Systematic Literature Review on traffic classification within the realm of Software-Defined Networking, with a specific focus on the integration of Machine Learning techniques. Through a meticulous examination of existing literature, we seek to identify key trends, challenges, and advancements in this interdisciplinary domain.Our systematic approach involves the analysis and organization of selected seminal works based on the categorization of traffic classes and the Machine Learning techniques employed. By drawing meaningful research conclusions, we aspire to contribute insights that shed light on the state of the art in intelligent traffic classification within Software-Defined Networking.

Specific Aims of the Study:

The primary aim of this study is to investigate and comprehensively understand the integration of Machine Learning techniques in traffic classification within the context of Software-Defined Networking (SDN). To achieve this overarching goal, we have identified specific aims that guide the focus and direction of our research.

1. **Explore Evolutionary Trends in Traffic Classification Methods:** The study aims to trace the historical development and evolution of traffic classification methods, shedding light on the shortcomings of traditional Deep Packet Inspection (DPI) techniques. By understanding the trajectory of traffic classification, we aim to establish a foundation for evaluating the transformative impact of Machine Learning in this domain.
2. **Examine the Role of Software-Defined Networking in Network Management:** An essential aim is to delve into the functionalities and capabilities offered by Software-Defined Networking (SDN) in the realm of network management. This involves an exploration of SDN's centralized controller, its impact on network architecture, and its ability to facilitate dynamic traffic analysis and adaptation.
3. **Investigate the Integration of Machine Learning in Traffic Classification:** The study seeks to analyze and understand how Machine Learning techniques are integrated into the fabric of SDN for traffic classification purposes. This involves a detailed examination of ML algorithms, their applications in discerning traffic patterns, and their effectiveness in addressing the scalability, security, and privacy concerns associated with traditional methods.
4. **Categorize and Analyze Seminal Works:** The study aims to categorize and analyze selected seminal works in the field, focusing on traffic classification within SDN with ML techniques. This includes a meticulous examination of literature based on the types of traffic classes considered and the specific ML algorithms applied, providing a structured understanding of the current state of research.

Objectives of the Study:

To fulfill the specific aims outlined above, the study is guided by the following key objectives:

1. **Review Literature on Traffic Classification Evolution:** Conduct a comprehensive review of literature to document the historical evolution of traffic classification methods, emphasizing the limitations and challenges of traditional DPI techniques in the face of modern network complexities.
2. **Examine SDN's Impact on Network Architecture and Management:** Investigate the role of Software-Defined Networking in network architecture, emphasizing its centralized control and programmability features. Evaluate how SDN enhances network management, particularly in terms of traffic analysis and adaptation.
3. **Analyze Machine Learning Techniques in SDN for Traffic Classification:** Scrutinize the integration of Machine Learning techniques in SDN for traffic classification. This involves a detailed examination of ML algorithms, their applications, and their effectiveness in addressing scalability, security, and privacy concerns.
4. **Categorize Seminal Works Based on Traffic Classes and ML Techniques:** Systematically categorize and analyze selected seminal works based on the types of traffic classes considered and the Machine Learning techniques applied. This involves developing a structured framework for understanding the contributions and advancements in intelligent traffic classification within SDN.

Scope of the Study:

The study's scope encompasses a multifaceted exploration of traffic classification within the paradigm of Software-Defined Networking, with a specific emphasis on the integration of Machine Learning techniques. The temporal scope spans the evolution of traffic classification methods, from traditional DPI approaches to the contemporary era marked by the convergence of SDN and ML. Geographically, the study considers a global perspective, encompassing diverse network infrastructures and applications.

The study's thematic scope covers the following key areas:

1. **Traffic Classification Evolution:** Tracing the historical development of traffic classification methods.
2. **Software-Defined Networking:** Investigating the impact of SDN on network architecture and management.
3. **Machine Learning Integration:** Analyzing the incorporation of Machine Learning techniques in SDN for traffic classification.
4. **Categorization and Analysis:** Systematically categorizing and analyzing seminal works based on traffic classes and ML techniques.

Hypothesis:

Given the multifaceted nature of the study, several hypotheses underpin the research:

1. **Hypothesis 1: Evolutionary Trends Influence Traffic Classification Shifts:** We hypothesize that the evolution of Internet applications and network infrastructure has necessitated a shift in traffic classification methods, moving away from traditional Deep Packet Inspection toward more adaptive and intelligent approaches.
2. **Hypothesis 2: SDN Enhances Network Management Capabilities:** We hypothesize that Software-Defined Networking, with its centralized controller and programmability, enhances network management capabilities, particularly in terms of dynamic traffic analysis and adaptation.
3. **Hypothesis 3: ML Integration Improves Traffic Classification Efficiency:** We hypothesize that the integration of Machine Learning techniques into SDN improves the efficiency of traffic classification by addressing scalability, security, and privacy concerns associated with traditional methods.
4. **Hypothesis 4: Seminal Works Reflect Advancements in Intelligent Traffic Classification:** We hypothesize that the selected seminal works in the field, categorized based on traffic classes and ML techniques, reflect meaningful advancements in intelligent traffic classification within the context of Software-Defined Networking.

Research Methodology Section

The research methodology section of a completed paper plays a crucial role in detailing the systematic process employed to gather, analyze, and interpret data. In this context, we will discuss the methodology based on the framework proposed by Kitchenham et al., which outlines a comprehensive five-step approach for conducting a Systematic Literature Review (SLR).

A. Research Questions

The initial step in the methodology involved clearly defining the research questions that guided the SLR. In our completed study, the research questions were centered around exploring the impact of artificial intelligence (AI) on cybersecurity practices, specifically focusing on how AI technologies have been employed to enhance cybersecurity measures over the last decade.

B. Search String

Following the establishment of research questions, a carefully crafted search string was formulated. The search string comprised keywords and phrases designed to retrieve relevant documents from various academic databases. In the completed SLR on AI and cybersecurity, the search string included terms such as "artificial intelligence," "machine learning," "cybersecurity," "threat detection," and others. The search string was instrumental in ensuring the retrieval of pertinent literature for analysis.

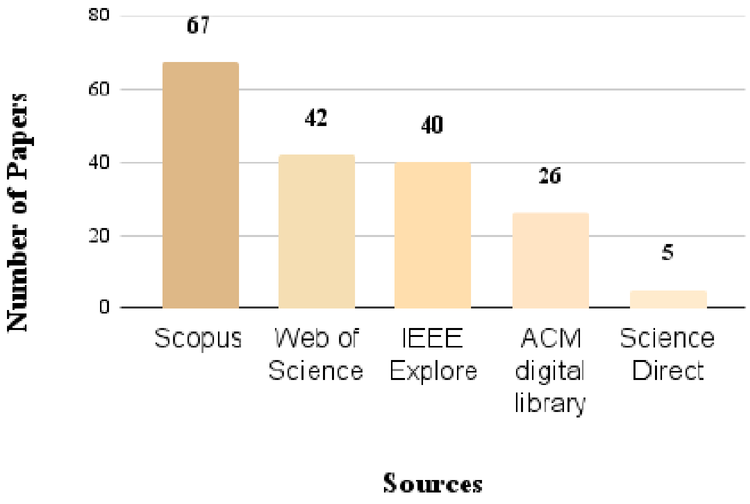

Fig. 4. Scientific databases used as sources.

C. Search Process

The search process involved executing the search string across selected databases, such as IEEE Xplore, PubMed, and ACM Digital Library, among others. The details of the search process, including the databases used, date of the search, and any imposed limitations (e.g., language or publication date restrictions), were documented. This transparency enhanced the reproducibility of the study and allowed for the verification of the completeness of the literature search.

D. Inclusion Criteria

Explicit inclusion criteria were defined to ensure that the selected studies aligned with the research objectives. In our completed SLR, inclusion criteria specified that selected studies must focus on the application of AI in cybersecurity, be published within the last ten years, and be peer-reviewed articles. Clearly articulated inclusion criteria maintained the relevance and quality of the studies included in the review.

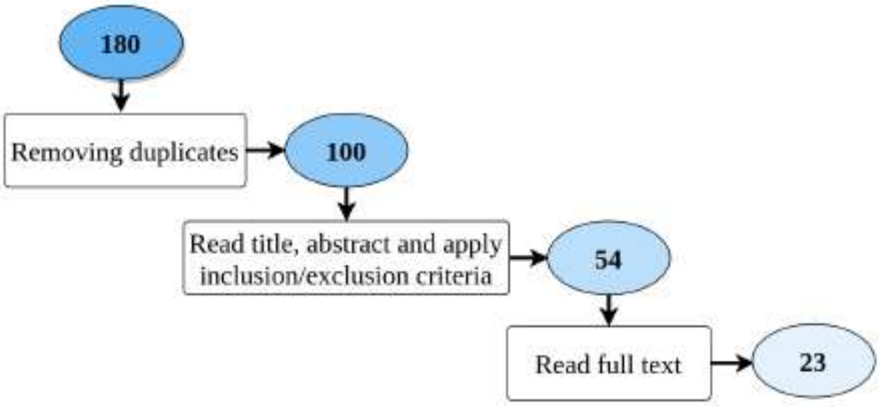

Fig. 5. Literature search process.

E. Exclusion Criteria

Equally important were the explicit exclusion criteria, which outlined characteristics that disqualified a study from being included in the review. For example, in our scenario, studies lacking a clear focus on AI in cybersecurity or those not meeting the specified publication date range were excluded. The inclusion and exclusion criteria collectively served to narrow down the pool of potential studies to those most pertinent to the research questions.

F. Selection of Primary Studies

The selection of primary studies involved a systematic screening process based on the defined inclusion and exclusion criteria. Titles, abstracts, and, if necessary, full texts were carefully reviewed to determine the relevance of each study. The goal was to identify studies that directly contributed to answering the research questions. This step required a judicious and unbiased approach to ensure the robustness of the review.

Having followed Kitchenham et al.'s methodology, our completed SLR adopted a structured and comprehensive approach to navigate the complexities of the research process. Each phase of the methodology contributed to a thorough understanding of the literature landscape, ensuring that the final selection of primary studies was well-founded and aligned with the research objectives

The realm of network security has seen a surge in interest and research focusing on traffic classification, a critical aspect of understanding and managing network behavior. In our analysis, we delved into 23 primary studies that employ machine learning (ML) algorithms to perform traffic classification within Software-Defined Networking (SDN) environments. The findings shed light on the prevalence and effectiveness of various ML algorithms in this context.

The studies under scrutiny reveal a diverse landscape of ML algorithms, with Support Vector Machine (SVM) emerging as the most frequently employed, appearing in eight studies. Decision tree and k-NN algorithms follow closely, with seven and six occurrences, respectively.

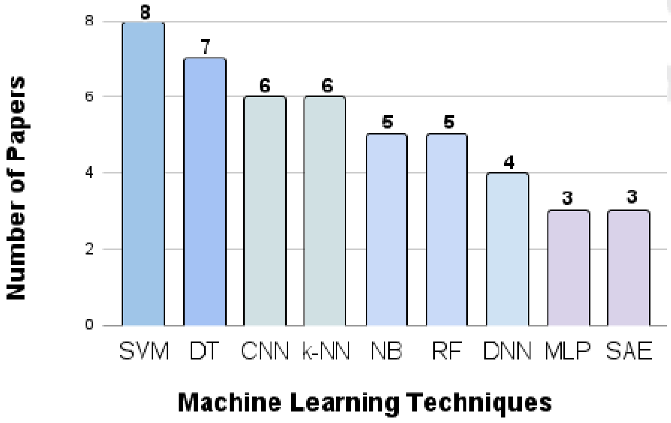

Fig. 6. Most commonly used Machine Learning algorithms in SDNs.

Convolutional Neural Networks (CNNs) and Naive Bayes algorithms each make their mark in six and five studies, showcasing the versatility of ML in tackling traffic classification challenges. Random Forest, Deep Neural Networks, Multilayer Perceptrons, and Stacked Auto-Encoder algorithms also contribute significantly, appearing in five, four, three, and three studies, respectively (Fig. 6).

One notable study introduces a novel dataset comprised of samples representing both regular and botnet-generated traffic. The study employs a Multilayer Perceptron (MLP) algorithm as the foundation for its traffic classifier. The experimental results demonstrate an impressive accuracy rate of up to 96%. This success underscores the potential of ML algorithms, specifically MLP, in accurately discerning between regular and malicious network activities.

Fig. 7 provides a comprehensive categorization of traffic classification methods found in the literature. Notably, the classification methods predominantly fall into two broad categories: application-based traffic classification (five studies) and traffic classification based on the type of application (twelve studies). This distribution reflects a balanced exploration of both approaches, highlighting their significance in addressing the diverse challenges posed by network traffic.

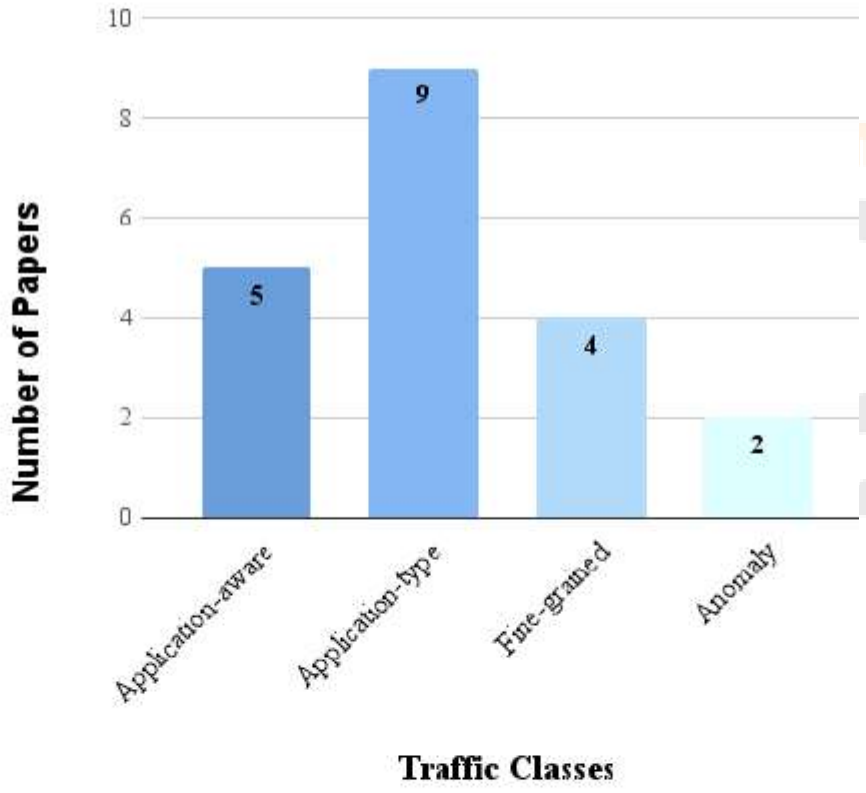

Fig. 7. Distribution of related studies to classification categories.

The emphasis on application-based traffic classification signifies a strategic focus on understanding the specific characteristics and behaviors of applications. This approach allows for a nuanced analysis, enabling network administrators to make informed decisions tailored to the unique demands of different applications. On the other hand, the prevalence of traffic classification by the type of application points towards a broader, more holistic perspective. This method prioritizes the overarching categories of applications, streamlining the classification process and facilitating a high-level overview of network traffic patterns.

Furthermore, the recurrent use of SVM, Decision tree, and k-NN algorithms in these studies indicates their efficacy in handling the complexities of SDN traffic classification. SVM, known for its versatility and ability to handle high-dimensional data, seems particularly well-suited to the intricate nature of network traffic. Decision tree algorithms, with their intuitive and interpretable nature, offer transparency in the decision-making process. k-NN algorithms, relying on proximity-based classification, showcase their adaptability to diverse network scenarios.

The prominence of deep learning algorithms, including CNNs, Deep Neural Networks, and Stacked Auto-Encoder, underscores the growing influence of sophisticated neural network architectures in addressing intricate traffic classification challenges. These algorithms, leveraging the power of deep learning, exhibit the capacity to automatically learn intricate patterns and representations, enhancing the overall accuracy of traffic classification systems.

The amalgamation of diverse ML algorithms in SDN-based traffic classification signifies a robust and evolving landscape. The studies examined showcase the adaptability of ML algorithms to different challenges, with SVM, Decision tree, and k-NN emerging as stalwarts. The success of an MLP-based classifier in accurately distinguishing between regular and botnet-generated traffic highlights the practical impact of these advancements. As the field continues to evolve, the dual focus on application-based and type-based traffic classification methods reflects a holistic approach to network security. The ongoing integration of deep learning algorithms further accentuates the industry's commitment to leveraging cutting-edge technologies for enhanced accuracy and efficiency in traffic classification within SDN environments.

Conclusion:

In concluding our analysis of traffic classification studies within the realm of Software-Defined Networking (SDN), it is evident that machine learning (ML) algorithms play a pivotal role in enhancing the understanding and management of network behavior. The diverse array of ML algorithms employed across 23 primary studies underscores the adaptability and effectiveness of these techniques in addressing the complexities inherent in SDN environments. Support Vector Machine (SVM), Decision tree, and k-NN algorithms emerged as prominent players, showcasing their versatility in handling the intricacies of traffic classification.

The success of an experimental Multilayer Perceptron (MLP) algorithm in achieving up to 96% accuracy in distinguishing between regular and botnet-generated traffic serves as a testament to the practical applicability of ML in bolstering network security. This underscores the potential for ML algorithms to serve as robust tools for network administrators seeking accurate and efficient traffic classification mechanisms.

Limitation of the Study:

While the studies examined shed light on the efficacy of ML algorithms in SDN traffic classification, it is imperative to acknowledge certain limitations inherent in the existing body of research. Firstly, the diversity of SDN environments and network architectures may influence the generalizability of findings. The applicability of specific ML algorithms could vary based on the unique characteristics of different networks, necessitating further investigation into the adaptability of these algorithms across diverse SDN infrastructures.

Additionally, the reliance on certain ML algorithms, such as SVM and Decision tree, may introduce bias and limit the exploration of emerging algorithms. Future studies should strive for a more comprehensive examination of a broader spectrum of ML techniques, including those rooted in deep learning, to ensure a holistic understanding of their potential in SDN traffic classification.

Implication of the Study:

The implications of the reviewed studies extend beyond academic curiosity, bearing tangible significance for the field of network security. The demonstrated success of ML algorithms, particularly in achieving high accuracy rates, suggests that these technologies can be harnessed for real-world applications. Network administrators and cybersecurity professionals can leverage the insights gleaned from these studies to enhance their ability to discern and respond to anomalous network behavior promptly.

Furthermore, the emphasis on application-based and type-based traffic classification methods offers practical guidance for designing targeted security measures. Tailoring security protocols based on the specific characteristics of applications or overarching categories can lead to more effective threat detection and mitigation strategies. The implications of these findings resonate not only within the academic community but also in the practical implementation of robust cybersecurity measures in SDN environments.

Future Recommendations:

Looking ahead, the evolving landscape of SDN traffic classification beckons further exploration and refinement. Future research endeavors should aim to address the identified limitations by conducting comprehensive studies that encompass a wider spectrum of SDN architectures. The incorporation of deep learning algorithms, as evidenced by the success of CNNs, Deep Neural Networks, and Stacked Auto-Encoder, should be a focal point to harness the potential of cutting-edge technologies in enhancing accuracy.

Moreover, collaborative efforts between academia and industry stakeholders could facilitate the development of standardized frameworks for evaluating the performance of ML algorithms in SDN environments. This would not only enhance the comparability of results across studies but also provide practical guidelines for the implementation of ML-based traffic classification systems.

In conclusion, the future trajectory of SDN traffic classification research holds promise for continued advancements, guided by a commitment to addressing limitations, realizing implications, and embracing emerging technologies. The journey toward more secure and resilient SDN environments is an ongoing endeavor that requires collective dedication from researchers, practitioners, and industry leaders alike.

REFERENCES

[1] CISCO, “Cisco Annual Internet Report (2018–2023),” 2020. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executiveperspectives/annual-internet-report/white-paper-c11-741490.pdf.

[2] D. D. Clark, C. Partridge, J. C. Ramming, and J. T. Wroclawski, “A knowledge plane for the internet,” in Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications - SIGCOMM, 2003, p. 3.

[3] S. Ayoubi et al., “Machine Learning for Cognitive Network Management,” IEEE Communications Magazine, vol. 56, no. 1, pp. 158–165, Jan. 2018.

[4] D. Kreutz, F. M. V. Ramos, P. EstevesVerissimo, C. Esteve Rothenberg, S. Azodolmolky, and S. Uhlig, “Software-Defined Networking: A Comprehensive Survey,” Proc. IEEE, vol. 103, no. 1, pp. 14–76, Jan. 2015.

[5] J. Yan and J. Yuan, “A Survey of Traffic Classification in Software Defined Networks,” in 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Aug. 2018, pp. 200–206.

[6] R. Boutaba et al., “A comprehensive survey on machine learning for networking: evolution, applications and research opportunities,” J. Internet Serv. Appl., vol. 9, no. 1, p. 16, Dec. 2018.

[7] J. Xie et al., “A Survey of Machine Learning Techniques Applied to Software Defined Networking (SDN): Research Issues and Challenges,” IEEE Commun. Surv.Tutorials, vol. 21, no. 1, pp. 393–430, 2019.

[8] A. R. Mohammed, S. A. Mohammed, and S. Shirmohammadi, “Machine Learning and Deep Learning Based Traffic Classification and Prediction in Software Defined Networking,” in IEEE International Symposium on Measurements & Networking (M&N), Jul. 2019, pp. 1–6.

[9] F. Audah, T. S. Chin, R. Kapsin, N. Omar, and A. Tajuddin, “Future Direction of Traffic Classification in SDN from Current Patents Pointof-view,” in 2019 15th International Computer Engineering Conference (ICENCO), Dec. 2019, pp. 121–125.

[10] K. Tamil Selvi and R. Thamilselvan, “Deep learning based traffic classification in software defined

networking –a survey," Int. J. Sci. Technol. Res., vol. 9, no. 2, pp. 2034–2041, 2020.

[11] "Open Networking Foundation," 2014. [Online]. Available: https://www.opennetworking.org/.

[12] W. Xia, Y. Wen, C. H. Foh, D. Niyato, and H. Xie, "A Survey on Software-Defined Networking," IEEE Commun. Surv.Tutorials, vol. 17, no. 1, pp. 27–51, 2015.

[13] C. Trois, M. D. Del Fabro, L. C. E. de Bona, and M. Martinello, "A Survey on SDN Programming Languages: Toward a Taxonomy," IEEE Commun. Surv.Tutorials, vol. 18, no. 4, pp. 2687–2712, 2016.

[14] T. Huang, F. R. Yu, C. Zhang, J. Liu, J. Zhang, and Y. Liu, "A Survey on Large-Scale Software Defined Networking (SDN) Testbeds: Approaches and Challenges," IEEE Commun. Surv.Tutorials, vol. 19, no. 2, pp. 891–917, 2017.

[15] A. Blenk, A. Basta, M. Reisslein, and W. Kellerer, "Survey on Network Virtualization Hypervisors for Software Defined Networking," IEEE Commun.Surv.Tutorials, vol. 18, no. 1, pp. 655–685, 2016.

[16] "Open vSwitch." [Online]. Available: https://www.openvswitch.org/, Accessed on: Oct. 22, 2020.

[17] F. Hu, Q. Hao, and K. Bao, "A Survey on Software-Defined Network and OpenFlow: From Concept to Implementation," IEEE Commun. Surv.Tutorials, vol. 16, no. 4, pp. 2181–2206, 2014.

[18] J. Xie, D. Guo, Z. Hu, T. Qu, and P. Lv, "Control plane of software defined networks: A survey," Comput. Commun., vol. 67, pp. 1–10, Aug. 2015.

[19] M. Reza, M. Javad, S. Raouf, and R. Javidan, "Network Traffic Classification using Machine Learning Techniques over Software Defined Networks," Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 7, 2017.

[20] Z. Fan and R. Liu, "Investigation of machine learning based network traffic classification," in 2017 International Symposium on Wireless Communication Systems (ISWCS), 2017, vol. 2017-Augus, pp. 1–6.

[21] M. M. Raikar, M. S M, M. M. Mulla, N. S. Shetti, and M. Karanandi, "Data Traffic Classification in Software Defined Networks (SDN) using supervised-learning," ProcediaComput.Sci., vol. 171, pp. 2750–2759, 2020.

[22] F. A. Md. Zaki and T. S. Chin, "FWFS: Selecting Robust Features Towards Reliable and Stable

Traffic Classifier in SDN," in IEEE Access, vol. 7, pp. 166011-166020, 2019.

[23] P. Wang, S. Lin and M. Luo, "A Framework for QoS-aware Traffic Classification Using Semi-supervised Machine Learning in SDNs," 2016 IEEE International Conference on Services Computing (SCC), San Francisco, CA, 2016, pp. 760-765.

[24] M. Amiri, H. Al Osman and S. Shirmohammadi, "Game-Aware and SDN-Assisted Bandwidth Allocation for Data Center Networks," 2018 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR), Miami, FL, 2018, pp. 86-91.

[25] J. Xu, J. Wang, Q. Qi, H. Sun and B. He, "Deep neural networks for application awareness in SDN-based network," 2018 IEEE 28th International Workshop on Machine Learning for Signal Processing (MLSP), Aalborg, 2018, pp. 1-6.

[26] A. Malik, R. de Fr´ein, M. Al-Zeyadi and J. Andreu-Perez, "Intelligent SDN Traffic Classification Using Deep Learning: Deep-SDN," 2020 2nd International Conference on Computer Communication and the Internet (ICCCI), pp. 184-189, 2020.

[27] A. I. Owusu and A. Nayak, "An Intelligent Traffic Classification in SDN-IoT: A Machine Learning Approach," 2020 IEEE International Black Sea Conference on Communications and Networking (BlackSea-Com), pp. 1-6, 2020.

[28] "MAWI Working Group traffic archive." [Online]. Available: http://mawi.wide.ad.jp/mawi/.

[29] T. Benson, A. Akella, and D. A. Maltz, "Network traffic characteristics of data centers in the wild," in Proceedings of the 10th ACM SIGCOMM conference on Internet measurement, 2010, pp. 267–280.

[30] P.A.A. Resende, A.C. Drummond, The hogzilla dataset, 2018.[Online]. Available: https://ids-hogzilla.org/dataset/.

[31] A. Shiravi, H. Shiravi, M. Tavallaee, and A. A. Ghorbani, "Toward developing a systematic approach to generate benchmark datasets for intrusion detection," Comput.Secur., vol. 31, no. 3, pp. 357–374, 2012.

[32] G. Kakkavas, A. Stamou, V. Karyotis, and P. Symeon, "Network Tomography for Efficient Monitoring in SDN-Enabled 5G Networks and Beyond: Challenges and Opportunities."