sciendo

Journal of Smart Internet of Things (JSIoT)
VOL. 1 (2023), No.01 | 14-09 | 2023
DOI: 10.2478/jsiot-2023-0002

Article

Application of Artificial Intelligence and Machine Learning in Software Defined Networks

Shakir Salman Ahmad[1], Mohammed I. Habelamateen[2]

[1] Department of Electronic and Electrical Engineering, College of Engineering, Design and Physical Sciences, Brunel University London, Uxbridge, Middlesex, UB8 3PH, United Kingdom
[2] Wireless and Radio Science Centre (WARAS) Faculty of Electrical and Electronic Engineering, Universiti Tun Hussein Onn Malaysia, Malaysia

*Corresponding author: Shakir Salman Ahmad (email: shakirsalman.ahmed@brunel.ac.uk)

Received xx March 2021; Accepted x July 2021; Published xx July 202

Abstract: Academics and businesses are very interested in using artificial intelligence (AI) and machine learning (ML) to solve the most challenging problems in a variety of fields. This white paper provides a brief overview of key applications of Artificial Intelligence and Machine Learning in SDN- and NFV-based networks. According to their application history, we categorize the most important developments in this field into different groups and identify the relevant AI methods used. It also covers key challenges and the domain's future course. We highlight the critical role AI/ML can play in opening the door to self-configuring, self-adapting as well as self-managing networks, but research is inadequate due to the difficulties found in this domain.

Keywords: 5G, Machine learning, Deep learning, SDN, Network Planning, Management, and Security.

Copyright © 2023 Journal of Smart Internet of Things (JSIoT) published by Future Science for Digital Publishing and Sciendo . This is an open access article license CC BY (https://creativecommons.org/licenses/by/4.0/)

1. Introduction

Software Defined Networking (SDN) and Network Functions Virtualization (NFV) are modern networking techniques created with the goal of separating network services from the hardware that supports them. Such techniques are created to satisfy needs for dynamic quality of service (QoS), such as: B. Variety of lag, throughput, as well as bandwidth on a sole physical network. This is a technique for achieving an extremely flexible and responsive facility-oriented network implementation where an individual part is optimized to provide a specific usability with explicit QoS requirements. It is achieved by network slicing [1]. This creates a vast number of software units throughout the network that should be properly managed to guarantee QoS. It also poses network management problems, as it is technically impossible for a human hand to manage a large amount of interconnected network parts.

Additionally, the integrated nature of SDN/NFV networks raises significant security issues due to solitary points of error. If the fundamental controller is forfeited, attackers would be able to intercept or alter all communications. Therefore, SDN/NFV networks require utmost care to safeguard the readiness, discretion, reliability, and privacy of all network points, involving central controllers. Other possible challenges in virtualized networks include network preparation, resource consumption load balancing, and fault recognition and organization. AI and ML are enabling networks to confidently self-adapt and Self-protect and self-manage by embedding intelligence into your network. In particular, Artificial Intelligence and Machine Learning enables network to gain from experience, become more resilient towards vulnerabilities and losses, and enhance presentation by decoupling network management as well as operations from human intervention. As a result, ML and AI have been broadly concentrated on in the writing to determine the above issues in generally useful correspondence organizations. For a thorough overview of possible solutions, see the work presented in [2]-[5]. However, relevant to SDN and NFV, there are several publications focusing at the application of AI/ML in SDN and NFV in context of resolving above problems. This article provides an all-inclusive overview of existing works in this area. It is a brief overview, as the amount of work in the SDN/NFV and AI/ML areas is limited. Additionally, this white paper describes the challenges that AI/ML may face in this area. As far as anyone is concerned, this is the primary concentrate on the utilization of man-made intelligence/ML regarding the matter of SDN and NFV. The essential commitments of this paper are:

- Gives a comprehensive review of the AI/ML works to address probable challenges facing numerous features of SDN and NFV;
- Categorize various ways AI/ML can be applied to SDN and NFV architectures; Special emphasis is placed on network layout, network organization, network security, and network development.
- For each use case, we acknowledged the machine learning techniques used in the works; Table I provides a summary of the given taxonomies.
- Give a discussion of possible challenges and future guidelines in this growing field;

2. Application of Artificial Intelligence in SDN & NFV Based Networks

Work is divided into 5 major categories. i) Network architecture, ii) Network preparation / load balancing as well as resource utilization, iii) Error/failure recognition and management, iv) Network management and operation, v) Network planning and breach detection. Every existing work is divided into sections above and described under each category. Table 1 provides a summary of the literature. Each category is discussed separately below.

2.1. Network Planning:

In [6], The creators suggest Future Intelligent Network (FINE), one of the contending artificial intelligences based correspondence network systems and exhibit it utilizing the case of a cooperative SDN/NFV organization. The structure is divided into three unmistakable layers: I) a knowledge layer, ii) a specialist layer, and iii) a business layer that interacts through different interfaces. Intelligent aircraft are the brains of AI-based networks. Furthermore, we show that FINE framework can be utilized in real-world communication networks and facilities. In Fig 1.1 we have discussed about the network architecture of AI and ML in software-defined networks which is given below. There it has been shown about the interconnections between Network Applications and directory nodes and Network application layer and Management plane.

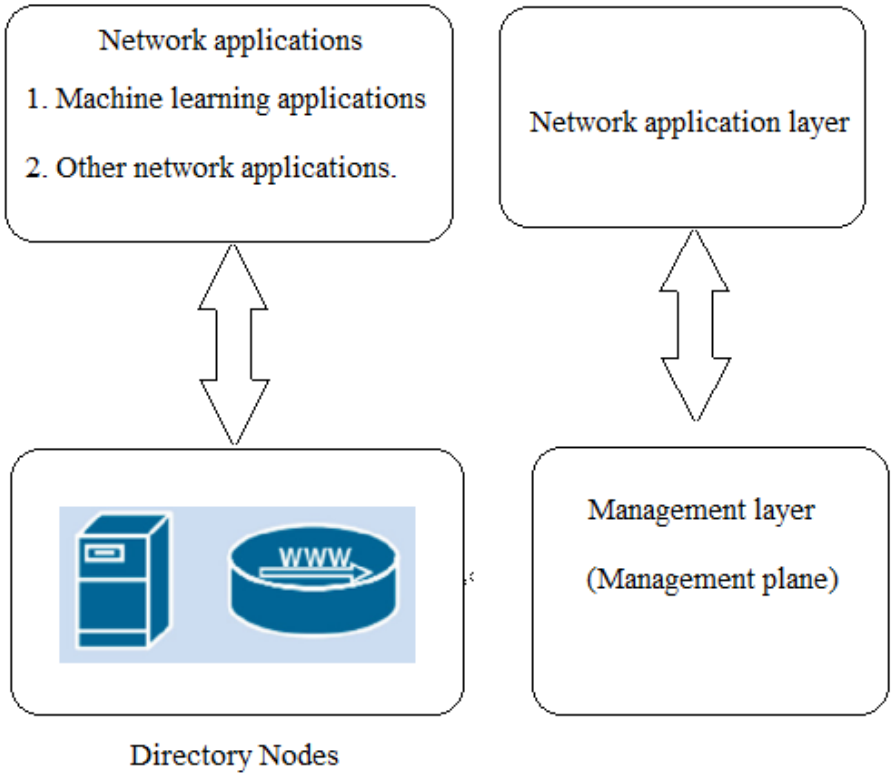


Figure 1: Network Architecture of AI and ML in software-defined networks.

2.2. Resource Utilization and Network Planning:

Great wisdom and others. [7] proposes the opportunities of using AI technology in the networks by demonstrating some use cases. The essential use cases were expected to address cell network functional issues like I) ideal organization asset arranging - traffic arranging, ii) network asset redistribution, and iii) network upkeep - network peculiarity acknowledgment. In [8] and [9], the creators recommend utilizing AI for helping the organization administrators in arranging the thick heterogeneous organizations. Specifically, he as of now utilizes information created from the 4G organizations, for instance radio estimations, in creating relationship factual models for the QoS-based network arranging. The creators incorporate various students to develop an aggregate technique utilized for relapse to estimate QoS in network arranging. The author focuses on her 5G networks in general for high-density heterogeneous settings, which we will discuss. SDN/NFV paving the way for his 5G networks in the future. There are basically three layers in which load balancing is done which is mentioned below in the Fig 1.2.

So, basically first one is Application Layers. Second one in Control Plane Layer followed by the third one layer i.e.,Data-Plane layer. Furthur details has been mentioned in the below diagram.

2.3. Fault/Failure Detection and Management

A semi-supervised learning approach is used by the author of [10] to show her AI-driven fault detection in her NFV application. To build a training data set and assess the system, I put up a testbed. His squared standard Euclidean distance is also used to assess how well the given method performs. At Mobile World Congress 2016, the first proof-of-concept for an automated network operating system backed by AI and based on AI error prediction, along with a networked SDN/NFV orchestrator and operational support system, was presented in [11]. Barcelona-based presentation.

Sichem and others [12] Provide availability and dependability for virtualized 5G end-to-end service chains with the LUMEN global fault management system (based on open-source products). Since LUMEN is a four-layer architecture, the following he is partitioned into four layers. i) source layer - gathers data every all entities, ii) sink layer - combines accumulated data into one form, iii) extraction layer - sink layer to extract data, and iv) decision level - Bayesian network. and machine learning techniques to make educated guesses/predictions.

In [13], The authors suggest embedding intelligence into the network using machine learning techniques to create an NFV/SDN-based self-healing and self-organizing network. The device is a component of his SELFNET H2020 project in Europe, which deploys numerous sensors throughout the network to supervise and report possible failures. The arrangement uses sensors and actuators to make intelligent decisions to detect and solve problems. Specifically, the network management framework is self-healing, self-protecting as well as self-optimizing.

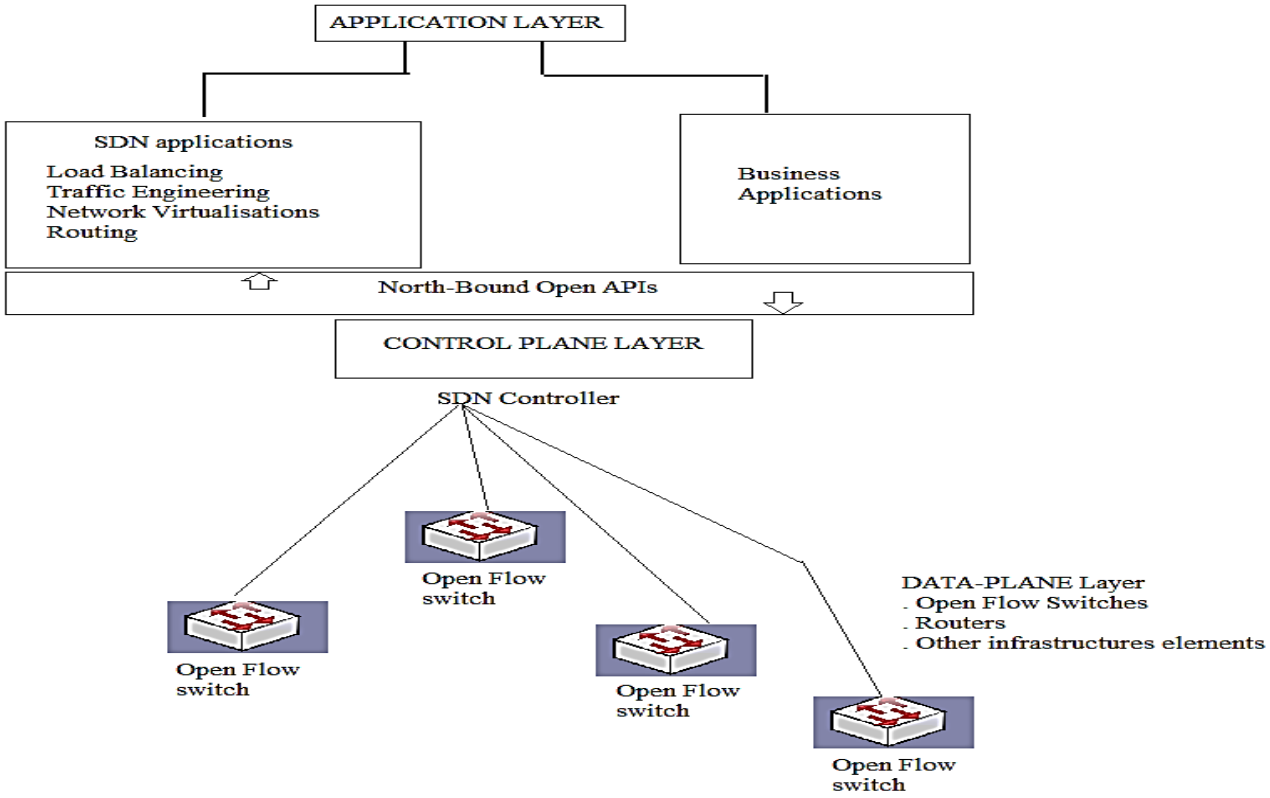


Figure 2**:** Load Balancing of Applications of AI and ML in software designed networks.

2.4. Network Managing and Processes

[14] suggests a brand-new paradigm for network operation and control. This paradigm, known as Knowledge-Defined Networking (KDN), is built on SDN, NA, and AI. The four functional levels of KDN are the data layer, the control layer, the knowledge layer (KP), and the management layer. KP converts the network analysis data gathered by the management plane into knowledge using machine learning and deep learning techniques, and then uses this information to make choices. In more detail, we may have a look at three distinct methods: supervised learning, unsupervised learning, and reinforcement learning are the first three. A cognitive administration engineering for controlling 5G organizations is recommended by Yimeng et al. [15]. They consider two of his AI based application cases.

ii) Versatile Quality Expectation (MQP): Precisely conjecture the continuous data transfer capacity prerequisites of every portable client. NFV System and Mental Structure Design are the two essential parts of mental engineering. Distributed monitoring agents included inside NFV parts are a must for cognitive architecture. It is made up of the following building blocks: Policy Manager, Cognitive Smart Engine (CSE), Data Store, and Data Collector. The central element, or CSE, is where all intelligence is found. The SLA enforcement use case is implemented using a specific kind of artificial neural network (ANN) called a recurrent neural network (RNN), while the MQP use case is implemented using a supervised learning method called the random forest algorithm. In the context of SDN/NFV, [16] provides an overview of autonomous communication and discusses the difficulties that network security, operations, and business support create as a result of the idea of autonomous and self-organizing networks. This white paper focuses especially on network function deployment, integration, and automated testing. The authors also explain how autonomous communication changes to real-time. Threats that use SDN/NFV security mechanisms to provide self-managing protection against them.

Another study is presented in [17] that explores the usage of machine learning in his SDN/NFV for network organization and management. The author mainly focuses on network autonomous operation, management and management in his 5G networks of the future. However, the author uses SDN/NFG as an initiater for his 5G network to integrate different applications with different QoS requirements, use machine learning to implement autonomous adaptability, and use experience during the decision-making process. It partially describes using the . The authors use supervised learning to estimate, predict, and classify numerous network management variables, unsupervised learning to recognize anomalous behavior and reduce network data dimensionality, and network management to control network parameters. It goes into detail about reinforcement learning when you need it. In [18], the authors propose including ANNs in autoregressive integrated moving average models (ARIMA) for traffic prediction and network modeling. The author leverages SDN, Network Analysis (NA), and ML to provide her various use cases and applications to illustrate new paradigms for future networks. The author focuses on NFV and models the performance of a single virtual network function (VNF) as a function of her inbound traffic. In particular, the author uses inbound traffic characteristics to estimate her CPU consumption of her VNF.

G. An ML method is suggested by a research in [19] for controlling concealed traffic in NFV-based networks. In a virtualized network, hidden traffic is any unseen data that never reaches the physical layer. The performance of several supervised learning algorithms for classifying IP traffic in NFV-based networks is compared by the authors. The Naive Bayes (NB) method was determined by the author to be the best IP traffic classification in NFV-based networks based on tested findings.

Supreme value of 99.9%. A comparable study is shown in [20], [21] outlines the author's COgnition-Based NETworks (COBANETS) system idea, which leverages SDN technologies as the foundation for the creation and management of next-generation communication networks. In specifically, the authors suggest integrating system-level autonomous optimization and reconfiguration tactics utilising unsupervised deep learning algorithms in a network virtualization paradigm. Security for networks and finding breaches

A system for cognitive SLA requirement of organization administrations using VNFs and SDN regulators is planned and assessed by the creators of [22] utilizing ANN. The system finds and perceives conceivable help level goal (SLO) breaks and empowers specialist co-ops to go to the essential administration lengths. Utilize testbed implementations to evaluate the framework using streaming services running on virtualized software-based infrastructure (NFV and SDN). In order to assess whether the SLO has been broken, ANN solves the classification issue. They primarily concentrated on his two ANN types: recurrent neural networks and feedforward neural networks (FFNN) (RNN). The creators of [24] propose a proactive protection framework against Denial of

Service (DoS) and Distributed Denial of Service (DDoS) assaults in SDN. The construction depends on a game-hypothetical strategy utilizing hereditary calculations with Holt-Winters and fluffy rationale. The Holt-Winters for Computerized Mark (HWDS) arrangement they furnish blends game hypothesis choice models with the test of inconsistency discovery and recognizable proof. In an SDN-based network environment, anchor etc. [23] provided a model for selecting countermeasures as well as a game theory assault analysis (DDoS attack). This approach is based on the dynamic incentives and penalties for multiplayer participation in his game.

A user whose attacker's network bandwidth is temporarily reduced and then goes back to normal once the player cooperates once more. In order to implement player incentives and penalties depending on their separate behaviours, their collaboration, and the attackers who are taking part in the DDoS attack, we apply the Nash-Folk theorem. [25] models attacker behaviour in the ML function space using a combination of game theory and machine learning (ML - NB classifier). Spam filtering is the intended target application for this work's defence against ongoing and upcoming threats.

3. Results and discussion

In the framework of SDN and NFV, the authors of [26] discuss the difficulties and possible advantages for cybersecurity in the IoT edge computing environment. The authors go into how ML and AI may be used to address these problems. The authors specifically advise employing virtual machines (VMs) as firewalls to fend off security intrusions. The authors also go into how ML and AI may be used to evaluate cyber activity to find possible dangers and weaknesses in edge computing settings for IoT that are built on SDN/NFV. The authors suggest using autonomous robots that can monitor an organization's surroundings and spot suspicious activity within the network using deep learning techniques.

The goal of the European project SHIELD [27] is to deploy NFV-enabled environments to defend networks against attacks and intrusions. To avoid and identify different security vulnerabilities, the initiative makes use of machine learning algorithms that security professionals have trained. The writers also look at cybersecurity solutions that are out now, concentrating on cloud virtualization services like AlienVault, ArcadiaData, and BlackStratus. DISCUSSION

The key obstacles and potential paths for implementing Artificial Intelligence/ML in SDN and NFV network settings are featured in this segment. We partition the significant difficulties into four fundamental classes: I computational intricacy and dormancy, ii) re-source necessity iii) admittance to assets - datasets and iv) capacity of important data.

3.1. Latency and Complexity

The majority of cloud-based ML operations include several computationally intensive procedures and algorithms, which increases latency while carrying out the necessary activities. There should be a method to do some of the time-sensitive activities using more effective algorithms or perhaps by developing some of the modules near to the network's edge. Future research should concentrate on examining and quantifying the effects of complexity and latency on the performance of the system [28].

3.2. Resource Requirement (CPU/Memory):

The needed procedures must be able to be performed using cloud-allocated resources due to the computational complexity indicated in Section III-A. Large datasets must be stored or computed using complicated low-latency procedures that need quick CPU and memory resources. Even though a centralised data centre can distribute adequate resources, allocating the resources you require when you require them is always a smart idea. The data centre uses less electricity as a

result of this.

3.3. Access to Resources – Datasets:

The absence of freely accessible standard datasets is another significant obstacle to deploying AI in the telecom sector. The majority of these records are the property of cell providers, who are required by law not to reveal the information. He suggests two ways to generate the datasets required to compare various algorithms in order to solve this issue. Additionally, having these datasets openly accessible promotes creativity and gives other researchers a strong incentive to contribute the datasets. By doing this, the community may develop a collection of standardised data that can be used to assess various use cases, applications, and situations [29].

3.4. Storage of Valuable Information:

A thorough review of AI/ML applications in SDN and NFV is provided in this white paper. In particular, we separated the material based on several application routes that were discovered in the literature. We also highlighted the relevant AI/ML methods applied in each featured work. We then spoke about potential difficulties in performing AI/ML-based research on various NFV and SDN topics. We emphasise that research in this developing subject is constrained by the scarcity of available datasets and the restricted availability of network resources. In the future, we intend to run several ML algorithms for various network sizes and traffic loads in order to quantify the computational resource utilisation of network nodes [30]. We specifically want to determine how network size affects the link between computational complexity and network traffic load. H. The number of participating network nodes.

4. CONCLUSIONS

A thorough review of AI/ML applications in SDN and NFV is provided in this white paper. In particular, we separated the material based on several application routes that were discovered in the literature. We also highlighted the relevant AI/ML methods applied in each featured work. We then spoke about potential difficulties in performing AI/ML-based research on various NFV and SDN topics. We emphasize that research in this developing subject is constrained by the scarcity of available datasets and the restricted availability of network resources. In the future, we intend to run several ML algorithms for various network sizes and traffic loads in order to quantify the computational resource utilisation of network nodes. In particular, our goal is to establish the association between network traffic load and computational complexity as a function of network size.

Funding Statement*:* The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. A. Gebremariam, M. Usman, P. Du, A. Nakao, and F. Granelli, “Towards E2E Slicing in 5G: A Spectrum Slicing Testbed and Its Extension to the Packet Core,” in 2017 IEEE Globecom Workshops (GC Wkshps), Dec 2017, pp. 1–6.

[2] T. T. Nguyen and G. Armitage, “A survey of techniques for internet traffic classification using machine learning,” IEEE Communications Surveys & Tutorials, vol. 10, no. 4, pp. 56–76, 2008.

[3] A. L. Buczak and E. Guven, “A survey of data mining and machine learning methods for cyber security intrusion detection,” IEEE Commu- nications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016.

[4] R. Sommer and V. Paxson, “Outside the closed world: On using machine learning for network intrusion detection,” in Security and Privacy (SP), 2010 IEEE Symposium on. IEEE, 2010, pp. 305–316.

[5] A. Imran, A. Zoha, and A. Abu-Dayya, “Challenges in 5g: how to empower son with big data for enabling 5g,” IEEE network, vol. 28, no. 6, pp. 27–33, 2014.

[6] X. Guibao, M. Yubo, L. Jialiang, “INCLUSION OF ARTIFICIAL INTELLIGENCE IN COMMUNICATION NETWORKS AND SER- VICES,” ITU Journal: ICT Discoveries, Special Issue, no. 1, pp. 1–6, Oct. 13 2017.

[7] T. Otani, H. Toube, T. Kimura, and M. Furutani, “APPLICATION OF AI TO MOBILE NETWORK OPERATION,” ITU Journal: ICT Discoveries, Special Issue, no. 1, pp. 1–7, Oct. 13 2017.

[8] J. Moysen, L. Giupponi, and J. Mangues-Bafalluy, “On the potential of ensemble regression techniques for future mobile network planning,” in Computers and Communication (ISCC), 2016 IEEE Symposium on. IEEE, 2016, pp. 477–483.

[9] M. Jessica and G. Lorenza and M.-B. Josep, “A machine learning enabled network planning tool,” in Personal, Indoor, and Mobile Ra- dio Communications (PIMRC), 2016 IEEE 27th Annual International Symposium on. IEEE, 2016, pp. 1–7.

[10] Julian A., Mathias S., Lia A. and Hans D. S., “An AI-driven Mal- function Detection Concept for NFV Instances in 5G,” CoRR, vol. abs/1804.05796, pp. 1–5, 2018.

[11] KDDI Research and Development Laboratories, Inc. (2016, Feb. 22) World’s first successful AI-assisted automated network operation system PoC towards 5G. [Online]. Available: http://www.kddi-research.jp/english/newsrelease/2016/022201.html

[12] S. Cherrared, S. Imadali, E. Fabre, and G. Go¨ssler, “LUMEN: A global fault management framework for network virtualization environments,” in 2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN). IEEE, 2018.

[13] M. G. Pe´rez, G. M. Pe´rez, P. G. Giardina, G. Bernini, P. Neves, J. M. Alcaraz-Calero, Q. Wang, and K. Koutsopoulos, “Self-Organizing Capabilities in 5G Networks: NFV & SDN Coordination in a Complex Use Case,” 2018.

[14] A. Mestres, A. Rodriguez-Natal, J. Carner, P. Barlet-Ros, E. Alarco´n, M. Sole´, V. Munte´s-Mulero, D. Meyer, S. Barkai, M. J. Hibbett et al., “Knowledge-defined networking,” ACM SIGCOMM Computer Communication Review, vol. 47, no. 3, pp. 2–10, 2017.

[15] I. G. B. Yahia, J. Bendriss, A. Samba, and P. Dooze, “CogNitive 5G networks: Comprehensive operator use cases with machine learning for management operations,” in Innovations in Clouds, Internet and Networks (ICIN), 2017 20th Conference on. IEEE, 2017, pp. 252– 259.

[16] Z. Zhao, E. Schiller, E. Kalogeiton, T. Braun, B. Stiller, M. T. Garip, J. Joy, M. Gerla, N. Akhtar, and I. Matta, “Autonomic Communications in Software-Driven Networks,” IEEE Journal on Selected Areas in Communications, vol. 35, no. 11, pp. 2431–2445, 2017.

[17] J. Moysen and L. Giupponi, “From 4G to 5G: Self-organized Network Management meets Machine Learn- ing,” Computer Communications, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366418300380

[18] A. Mestres Sugran˜es, “Knowledge-defined networking: a machine learn- ing based approach for network and traffic modeling,” 2017.

[19] J. Vergara-Reyes, M. C. Martinez-Ordonez, A. Ordonez, and O. M. C. Rendon, “IP traffic classification in NFV: A benchmarking of supervised Machine Learning algorithms,” in Communications and Computing (COLCOM), 2017 IEEE Colombian Conference on. IEEE, 2017, pp. 1–6.

[20] L. He, C. Xu, and Y. Luo, “VTC: Machine learning based traffic classification as a virtual network function,” in Proceedings of the 2016 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization. ACM, 2016, pp. 53–56.

[21] M. Zorzi, A. Zanella, A. Testolin, M. D. F. De Grazia, and M. Zorzi, “Cognition-based networks: A new perspective on network optimization using learning and distributed intelligence,” IEEE Access, vol. 3, pp. 1512–1530, 2015.

[22] J. Bendriss, I. G. B. Yahia, P. Chemouil, and D. Zeghlache, “AI for SLA management in programmable networks,” in DRCN 2017-Design of Reliable Communication Networks; 13th International Conference; Proceedings of. VDE, 2017, pp. 1–8.

[23] A. Chowdhary, S. Pisharody, A. Alshamrani, and D. Huang, “Dynamic game based security framework in sdn-enabled cloud networking envi- ronments,” in Proceedings of the ACM International Workshop on Secu- rity in Software

Defined Networks & Network Function Virtualization. ACM, 2017, pp. 53–58.
[24] M. V. De Assis, A. H. Hamamoto, T. Abrao, and M. L. Proenc¸a, "A game theoretical based system using holt-winters and genetic algorithm with fuzzy logic for DoS/DDoS mitigation on SDN networks," IEEE Access, vol. 5, pp. 9485–9496, 2017.
[25] R. Colbaugh and K. Glass, "Predictability oriented defense against adaptive adversaries." In Proceedings of IEEE International Conference on Systems, Man, and Cybernetics (SMC), Seoul, Korea, pp. 2721–2727, Oct. 14-17 2012.
[26] J. Pan and Z. Yang, "Cybersecurity Challenges and Opportunities in the New Edge Computing+ IoT World," in Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization. ACM, 2018, pp. 29–32.
[27] G. Gardikis, K. Tzoulas, K. Tripolitis, A. Bartzas, S. Costicoglou,
A. Lioy, B. Gaston, C. Fernandez, C. Davila, A. Litke et al., "SHIELD: A novel NFV-based cybersecurity framework," in Network Softwariza- tion (NetSoft), 2017 IEEE Conference on. IEEE, 2017, pp. 1–6.

[28] (2018, Aug. 26). [Online]. Available: https://www.nsnam.org/
[29] (2018, Aug. 26). [Online]. Available: http://www.openairinterface.org/
[30] (2018, Aug. 26). [Online]. Available: http://mininet.org/