

AN EVOLUTIONARY APPROACH USING ML IN SDN ARCHITECTURE

Abstract

The number of devices linked to the network is increasing dramatically in the current day. The complexity of network administration is rising as more IoT devices tend to use the internet to access the world. In order to compete with the current network technologies, traditional networking will not be sufficient. To handle and analyse the data, it is vital to use big networks and data centers. Self-Driven Networks (SDN) and Software Defined Networks (SDN) play an important part in this, aiding in the problem-solving process and enhancing network performance through the use of ML approaches. The main aim of this paper is to create a unique architecture that seamlessly integrates latency, bandwidth forecasting, and QoE estimation into the applications. The overall classification of the traffic is done based on the data from the SDN controller, this classification is used in predicting the traffic in each network route and helps in finding the optimum routes.

Keywords: Self-Driven Networks, Software Defined Networks, ML, IoT

Authors

Keerthika V

Department of Computer Science & Engineering
Alliance University
Bengaluru, Karnataka, India
keerthika.v@alliance.edu.in

Harinee Shanmuganathan

Department of Computer Science & Engineering
Alliance University
Bengaluru, Karnataka, India
harinees.s@alliance.edu.in

Geetha A

Department of Computer Science & Engineering
Alliance University
Bengaluru, Karnataka, India
Geetha.a@alliance.edu.in

Deepak Munirathinam

Department of Computer Science & Engineering
Alliance University
Bengaluru, Karnataka, India
deepak.raj@alliance.edu.in

I. INTRODUCTION

In order to address several issues in communication systems, Software Defined Networking (SDN) has become the most effective programmable network architecture. As a result of SDN, the network control plane is logically centralised and separated from the data forwarding plane [3]. SDN provides software-based control in the network system. Special capabilities of SDN, give us new chances to apply ML techniques and provide intelligence inside the networks. The next era of network design benefits from a fresh area of study in SDN. It has become increasingly necessary to manage communication networks in a different and more effective manner as a result of the quick development in IoT devices and new services like unmanned aerial vehicles, e-health, smart cities and e-commerce, etc. These application demands sophisticated network policies and challenging networking tasks [1]. SDN has mostly solved the problems that traditional communication networks now faces, including their static nature and administration complexity. The versatility in managing the network function may now be successfully accomplished with SDN.

Machine learning has paved it way in SDN because of its great advancement and inevitable benefits it provides in terms of security, analysis and predictions.

II. TRADITIONAL NETWORKING VS SDN

The infrastructure is the fundamental factor that sets SDN apart from conventional networking. Unlike traditional networking, which is hardware-oriented, SDN is software oriented. SDN has a software-oriented control plane, which gives it significantly greater flexibility than traditional networking. From a single user interface, administrators may take responsibility for the network, modify network configuration, supply resources, and enhance capacity of the network without having the need for more hardware. SDN offers greater security in many respects due to its enhanced visibility and capacity to designate safe pathways. But because SDN relies on a centralised controller, which is a single point of failure, protecting the controller is crucial to keeping the network secure.

III. SDN

Applications and users are dispersed more widely than ever, and the internet has essentially replaced wireless networks and IoT in businesses. The delivery of dependable connectivity, application performance, and security through networks and services that they do not directly own presents a challenge for network and IT teams as businesses continue to adopt the internet, cloud computing, IoT and SaaS.

In situations where anything goes wrong, network teams frequently have the duty of establishing the network's innocence. Network problems can appear as a result of application problems. The blame-game after a service interruption might go on forever. The ensuing cycles of isolating the problem's root cause can result in protracted service outages, which ultimately harm the company's revenue and reputation.

Beyond the conventional network, we have expanded visibility into the internet, IoT, cloud, and SaaS apps for useful insights. SDN is an architecture that makes networks more adaptable and flexible by abstracting the variations, easily recognisable levels of a network.

Modern applications' high- bandwidth, dynamic nature makes SDN, an emerging design, the ideal fit. SDN is flexible, dynamic, inexpensive, and controlled. The network control may be directly programmed in this approach since the forwarding operations and network control are separated. The goal of SDN is to enhance network control by enabling companies and service providers to quickly respond to changing customer demands.

IV. SDN ARCHITECTURE

The three tiers that frequently make up an SDN architectural representation are the application layer, the control layer, and the infrastructure layer. These levels communicate through northbound and southbound interfaces for application programming.

- 1. Data Plane:** Switches, routers, wireless access points, and other network equipment are located on the data plane, which is the lowest layer. Lowest layer is also known as user plane, forwarding plane or carrier plane [1]. These devices just execute a set of forwarding operations for changing network data packets and flows and provide an abstract top-level communication inter- face, being devoid of any SDN control logic (such as routing algorithms). Network equipment's in data plane interacts with the control plane via southbound interfaces, through which the control plane can manage the processing and forwarding capabilities of the data plane.
- 2. Control plane:** The Control Plane, which makes choices on traffic signaling, and manages policies and routing, is the brain of the network [1]. The controller monitors and samples real-time data from the network nodes and packets to gain a comprehensive understanding of the network. The controller is in charge of deciding on the network's routing and has the ability to dynamically program the network. The controller is in charge of providing a programmatic interface to the network, which is used to add new functionality and carry out different administration duties. It also encapsulates the networking logic.

The control plane and the application plane are connected through Northbound Interfaces (NBIs). Applications can express management, and promote automation, network behaviors, innovation, and requirements of SDN networks by utilising NBIs to avail the abstract network views offered by the control plane.

- 3. Application Plane:** Business apps make up the application plane, the top layer of the SDN architecture. In addition to performing company administration and optimization, these programs can offer new services. They can access the necessary network status data via controllers' NBIs. The apps can put the control logic to change network behaviors into action based on the information they have received and the business needs.

V. RELATED WORK

In [1] explained the characteristics of SDN, provides a perspective logically connected centralized controller of SDN and also described about data gathered using network telemetry of Syslog data. Suggested ML algorithms can be used to process the structured data, and exploit it to control the network.

In [3] described the solution for dealing the complex issues in the field of SDN using advanced networking techniques and computing tools. Analysed Area Under the curve(AUC) for different ML techniques to counter DoS attacks faced in SDN. Performed detailed Analysis of performance metrics like Accuracy, sensitivity, specificity, precision, FI score. According to their results SVM performs better than other algorithms with 97.5% accuracy.

In [4] simulated the SDN in Mininet; container-based emulation. In this demonstrated distributed Mininet emulation, which simplifies experiments, requires minimal setup and configuration which suited for ad-hoc networks.

In [5] used ML algorithms for traffic classification in SDN to inform decisions regarding their quality of service (QoS) based on PSO Complexity analysis and the Stability analysis of FFNN-PSO. The proposed approach hybrid Feed Forward Neural Networks (FFNN)-PSO has achieved high percentage of accuracy in wireless traffic classification.

In [7] presented classification which solves the issues for improving network performance of Software Defined Net- working , analyses of machine learning algorithms and illustrated how to use machine learning techniques in computer networks.

In [8] discussed process network testing , flow rule installation mechanisms, network security and network management issues ,SDN programming languages, and SDN controller platforms.

In [9] presented the Real-Time Multipath Transmission Protocol (RMTP) for the regulation of multiple paths in DCN. it choose the best path in a DCN ,stated that RMPT improves the transmission of big data with parameters throughput, packet loss and throughput.

In [10] presented data-sets with ML techniques applied to SDN compared for traffic classification. The work shows supervised Learning of ML helps to obtain high accuracy classification [10]. In [11] proposed a novel approach Knowledge defined SDN framework which is compatible to SDN architectures, proposed a novel approach auto-scaling NFV using machine learning dataset to compare with VNF-CPU performance data

VI. MEACHINE LEARNING TECHNIQUES

Machine Learning (ML) technique assists in creating net- work behaviour that can learn from past data and offer a forecast for the upcoming packets based on the training data, SVM, naive bayes, decision tree, and logic regression. In order to forecast packet flow and optimise parameters, ML is a useful technology that may be applied to SDN.

- 1. Support Vector Machine (SVM):** SVM is preferred over other Machine Learning techniques used to find suitable hyperplane which Can differentiate the data points and it can be widely used for both classification as well as regression tasks. SVM is considered as the ML classifier which used to separate the classes to find optimal hyperplane.
- 2. Rainforest Algorithm:** It is an algorithm of constructing a decision tree (how to do splitting) when the dataset is so large that it does not fit the memory. In the

rainforest, the complete dataset is not required for making a splitting decision. Rainforest can be used when the dataset is large, and memory is less, you can use rainforest to build several different decision trees. The number of Internet of Things (IoT) devices connected with SDN have increased hugely in the past decade with the rapid developments of technology it results that dataset also increased, it is also observed that SDN dataset can handled effectively by Rainforest.

VII. PROPOSED FRAMEWORK

The main goal of our framework is to predict the traffic condition and route the data packets accordingly. The traffic prediction is based on the bandwidth and latency requirement of the routing path. The proposed framework consists of IoT devices, switch/ network elements from the SDN data plane, control plane, and application plane. The traffic classification and the routing module are located in the centralized controller. This architecture can be seen in Figure 1

In order to ensure that the best available path is chosen during routing operations, the solution makes use of bandwidth and latency prediction on networks. Extraction of the routing prediction mechanism's invariances is the design objective. The framework chooses the appropriate path by fusing user requirements with the upcoming link latency and bandwidth availability. The SDN controller obtains and transmits the essential knowledge about the network topology in order to choose the optimum path. In order to consistently choose a path among all the devices, the routing model integrates the output of the prediction with the network topology information and modifies the flow rules accordingly.

In the proposed framework the switch inspects the incoming packets for the matching rules. The SDN controller will receive the message and a packet trace via a dedicated channel if there is no flow rule enabled. From the packet trace of the flow, the controller estimates the flow statistical features. The flow of the proposed framework can be seen in Fig. 2. The topology graphs extracted from the SDN controller help in analyzing the data flow in the network. Then the proposed framework makes use of this topology graph to find the shortest path with A star or by mid-point-based A star algorithm.

The advantage of the A-Star algorithm is simple and relatively fast when compared to the Dijkstra algorithm.

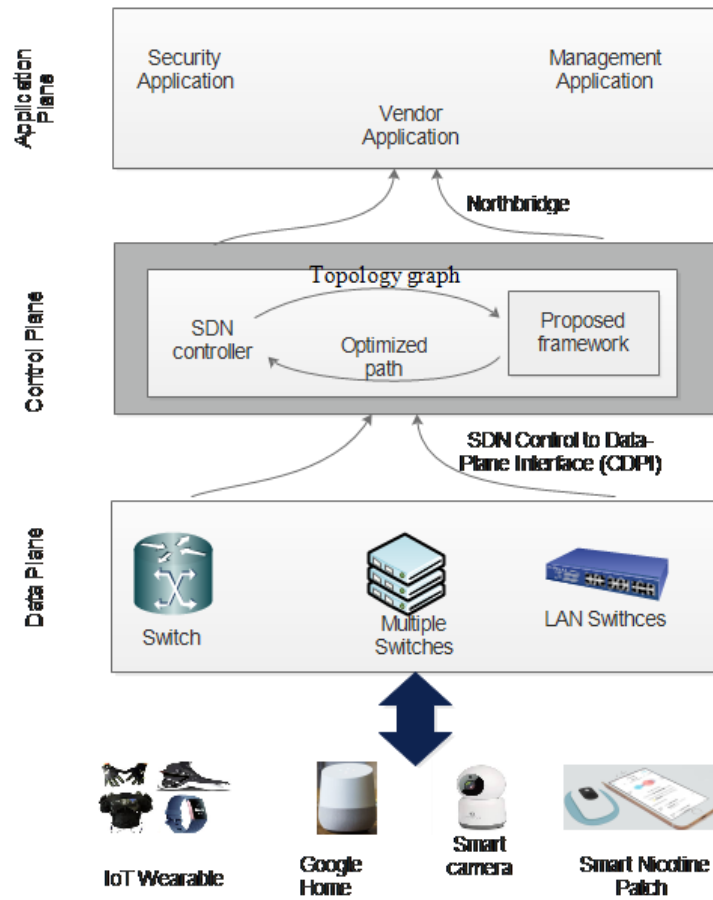


Figure 1: Architecture of SDN with the Framework Fitted in SDN Controller

A star applies heuristic function in equation (1) to accelerate the speed of finding the shortest path to the target.

$$F = G + H \tag{1}$$

where,

F- evaluation function.

G- the cost to the finishing.

H- distance between the current point and target location.

This classical heuristic function would quickly guide the search toward the target location.

1. **Initial Phase:** The data about the network topology and the traffic in each network path is obtained from the SDN controller. This data helps in analysing the present and future data flow in the network.
2. **Contiguity Check Phase:** In this phase, the source and the destination nodes are checked if they are within the network range and if nodes are active, else the packets are dropped.
3. **Path Determination:** In this phase, the distance of the straight-line path (SLP) between the source and the destination is calculated. The A- star algorithm is applied to the network.

to find the shortest path (A-SP) and the second shortest path (A-SSP) between the source and the destination

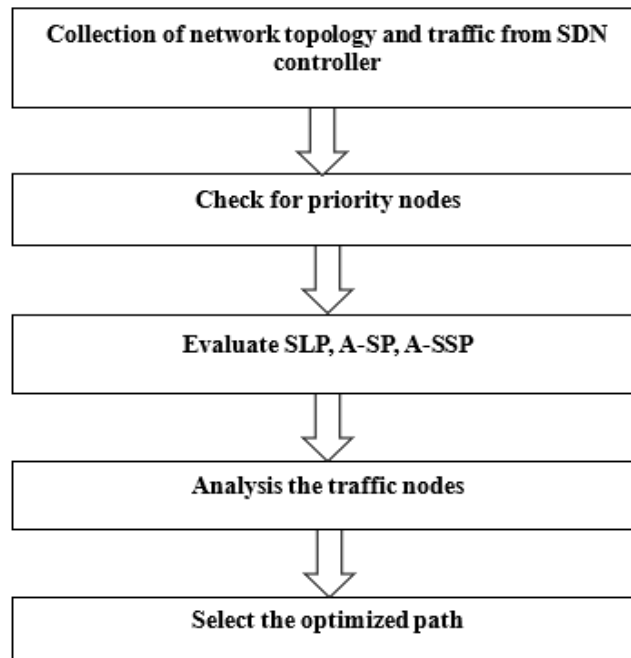


Figure 2: Architecture of SDN with the Framework Fitted in SDN Controller

- 1. Traffic Classification:** In this phase, the network traffic is classified into different labels based on rain forest classification. The classified data are stored under different labels in the database. The reason for selecting rain forest algorithm is because it can handle large set of data with small memory space. In this classifier, only some aggregate information of the nodes is required rather than the whole dataset of the network.
- 2. Selection of Optimized Path:** In this phase, the nodes in the SLP, A-SP and A-SSP are checked for the labels provided by the traffic classifier. If there are more nodes with higher traffic labels in the A-SP then it predicts the traffic labels in A-SSP. The path which has less higher traffic label is selected as the optimal path. Thus the optimizer selects the best path among SLP, A-SP, A-SSP.

VIII. CONCLUSION

The IoT and SDN technologies are still in their early stages, and the norms of betterment and management are still being developed. Some issues in SDN-IoT have only been addressed by a few researchers. With the current networking patterns and IoT devices, the data exchange is going to bloom in higher rate. Then it will be a magnified change in the traffic pattern when compared to the traditional traffic. The proposed framework utilizes machine learning techniques, which make the network become more intelligent and, as a result, make better judgements. The use of A star algorithm makes the decision of finding the shortest path easier, simpler, faster and regular. The use of rain forest classifier helps in reducing the memory usage.

REFERENCES

- [1] Adnane Mzibri, "Knowledge Defined Networking: State of the Art and research challenges," EasyChair Proceedings and Collections, July 2022.
- [2] A. F. Molisch, "Wireless Communications", vol. 34. Chichester, U.K.:Wiley, 2012.
- [3] Ahmad, E. Harjula, M. Ylianttila and I. Ahmad, "Evaluation of Machine Learning Techniques for Security in SDN", 2020 IEEE Globecom Workshops GC Wkshps, 2020, pp. 1-6,
- [4] Bob Lantz, Brian O'Connor. "A Mininet-based Virtual Testbed for Distributed SDN Development", SIGCOMM 2015, August 18-20, 2015, London, UK.
- [5] Buddhadeb Pradhan, Mir Wajahat Hussain, Gautam Srivastava, Mrinal K. Debbarma, Rabindra K. Barik, Jerry Chun-Wei Lin, "A neuro- evolutionary approach for software-defined wireless network traffic classification", IET communication, December 2022.
- [6] epehr Ashtari, Ian Zhou, Mehran Abolhasan, Negin Shariati, Justin Lipman, Wei Ni, "Knowledge-defined networking: Applications, challenges and future work", Elsevier, Volume 14, 2022.
- [7] Guo, Z., "Machine Learning for Software-Defined Networking. In: Bringing Machine Learning to Software-Defined Networks". Springer Briefs in Computer Science. Springer, Singapore.
- [8] Mudassar Hussain, Nadir Shah, Rashid Amin, Sultan S. Alshamrani, Aziz Alotaibi and Syed Mohsan Raza, "Software-Defined Networking: Categories, Analysis, and Future Directions", Sensors 2022, 22, 5551.
- [9] M. J. Anjum, I. Raza and S. A. Hussain, "Real-Time Multipath Transmission Protocol (RMTP): A Software Defined Networks (SDN) based Routing Protocol for Data Centric Networks," 2019 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), 2019, pp. 1-6.
- [10] P. Amaral, J. Dinis, P. Pinto, L. Bernardo, J. Tavares and H. S. Mamede, "Machine Learning in Software Defined Networks: Data collection and traffic classification," 2016 IEEE 24th International Conference on Network Protocols (ICNP), 2016, pp. 1-5.
- [11] Rojia Nikbazm, Mahmood Ahmadi, "KSN: Modeling and simulation of knowledge using machine learning in NFV/SDN-based networks", Simulation Modelling Practice and theory, vol. 121, 2022.
- [12] Wang T, Guo Z, Chen H, Liu W, "Bwmanager: mitigating denial of service attacks in software-defined networks through bandwidth prediction", IEEE Trans Netw Service Manag, vol. 15(4), pp.1235–1248.