International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 13 Issue: 1
Article Received: *25 November 2024* ***Revised:*** *12 December 2024* ***Accepted:*** *02 January 2025*

A new Dynamic Routing Approach for Software Defined Network

Saroj Singh
Dept. Computer Science and Engineering
Manav Rachna International Institute of Research and Studies (MRIIRS), Sector – 43, Delhi–Surajkund Road
Faridabad – 121004, Haryana, India
sarojraj47@gmail.com

Kamlesh Sharma
Dept. Computer Science and Engineering
Manav Rachna International Institute of Research and Studies (MRIIRS), Sector – 43, Delhi–Surajkund Road
Faridabad – 121004, Haryana, India
associatedean_ks.academics@mriu.edu.in

Abstract—Introduces a new dynamic routing approach tailored for Software Defined Network (SDN) that takes advantages of the programmability and centralized control inherent SDN architectures. Traditional routing protocols often struggles often to adapt to dynamic network conditions, leading to suboptimal performance and resource utilization. In contrast the objective of the paper is to proposed approach uses real time network information collected by the SDN controller to dynamic adjust routing decisions and dynamic routing algorithms for software define networks in wide area network (SDN-WAN), provide a new approach; By employing a combination of machine learning algorithm and network speed back mechanism. Using the approach optimizes routing paths based on factors such as link utilization and quality of service requirements. The shortest feasible path (SOFP) is an adaptation of the shortest feasible path algorithm that uses a statistical technique from the OpenFlow interface. The goal of the SFOP algorithm is to efficiently use SDN-WAN resources by determining the best route from source to destination. Overall, the dynamic routing approach provides a promising solution to efficiently manage network traffic in SDN. Paving the way for more adaptative and responsive networking infrastructure.

Keywords- OpenFlow, QoS, Random Forest Algorithm, SDN-WAN, SFOP

I. INTRODUCTION *(HEADING 1)*

An approach to network administration known as "Software Defined Networking" allows for dynamic, programmatically managed network configuration [1]. To implement SDN firstly need to define and use algorithms to control the flow of data through the network. SDN is such a network that can solve all kinds of activities through software. It is divided into three types of layers. In the SDN structure it can interfaced with three types of layers. These layers include application layer, data layer and control layer [2]. Control layer application and data layer are separated by body. Now there will pick up provided data from the cloud and apply it to the random forest model [3].

A. Overview of Software Defined Networking Controller

An application in figure 1's SDN architecture called the software Defined Networking controller (SDN) controls the flow controller to improve network management and application performance [4]. Switch packets are sent by the SDN controller platform, which is usually executed on a server and employs protocols.

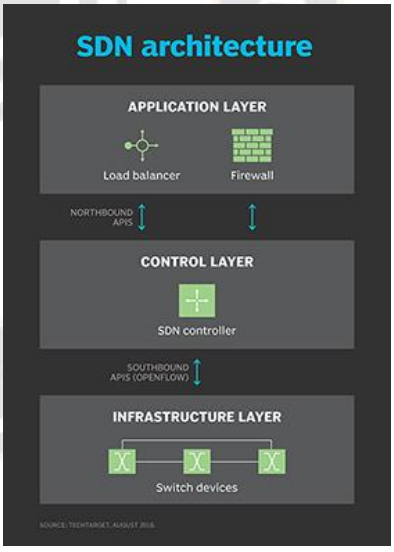

Figure 1: SDN architecture

SDN controllers [5] reduce the amount of manual configuration required for individual network devices by directing traffic in accordance with forwarding policies put in place by a network operator. The ability to support SFOP facilities automated network management [6] and facilities the administration and integration of corporate applications. Essentially, the SDN controller functions as a network's operating system (OS).

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 13 Issue: 1
Article Received: *25 November 2024* ***Revised:*** *12 December 2024* ***Accepted:*** *02 January 2025*

Northbound interfaces are used by the controller to communicate with devices like load balancers and firewalls. The ONF (Open Networking Foundation) [7] established a working group in 2013 with a primary focus on the development of northbound APIs. The industry has never agreed upon a standard set, though, because application needs differ so greatly controller supplier providing the following SDN controllers: VMware, NEC, Nvidia, Pica8, Hewlett Packard Enterprise, Juniper Networks and Cisco.

The Open source SDN controller facilitates communication within SDN, incorporating the following options: NOX/POX, Open Daylight, Open Network Operating System and Tungsten Fabric.

B. Traditionally- SDN-Wide Area Network Controller

Data centre networks make use of SDN controllers. WAN, however, become a desirable use case as SDN technology advanced, with prompted the creation of software defined WAN(SD-WAN) [8] technology. So, the main functions of the controller including: Managing the flow of data in a managed network. Providing an API for applications and other components such as orchestration platforms which is interact with the network. Providing visibility into the network, allowing monitoring of network performance [9] and detection of problems.

C. Check device registration status

There are getting device registration status from the following figure 2 such as after typing the URL POST https://global.azure-devices-provisioning.net/{idScope}/registrations/{registrationId}?api-version=2021-06-01.

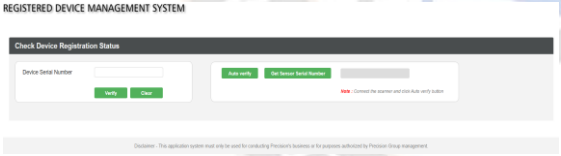

Fig 2: Device registration status

D. Flow Table Entries Check

It consists of a set of actions to take and a set of packet fields to match, such as IP addresses and ethernet addresses to the matching for example send-out-port or modify-field or drop. So, each entry in the flow table [10] consists of three parts first matching rule second action and third counters. The fundamental concept of current programming APIs is to statically compile SDN programs and then generating a unique scheme for each network switch's flow table.

E. Flow Surveillance

It is a technique that measures data flow via a network between two devices or apps. The goal of the flow monitoring approach is to provide IT teams with information about the traffic that flows through their network and the day-to-day performance of their network. Analysis of flow data includes: including bandwidth [11] hogs. Individual sources often use disproportionately high amount of bandwidth. Spot load peaks quickly. Many companies experience fluctuations in access to various websites or applications used internally and avoid backup overload.

F. Policy enforcement check

The process of controlling network and application [12] connectivity, access, and use in accordance with one or more policies that specify the circumstances in which access is allowed is known as policy enforcement

G. Logs Analytics

In order to obtain operational insights, log analytics includes examining, analysing and visualizing machine data produces by IT systems and technology infrastructure.

H. Dynamic Adaptation

The dynamic Adaption is shown as the metallurgical potential that accounts for the variability of the concrete application. Variability and the response to it are modelled as various conformance relationships in between the application model these are the target, the environment and the underlying system.

I. Quality of Service (QoS)

With restricted network capability, it is the deployment of technologies or methods that helps to regulate network traffic and guarantee the operation of vital applications [13]. Through the prioritizing of particular high-performance apps, QoS enables enterprises to modify their overall network traffic.

J. Security Testing.

It is a process that aims to detect vulnerabilities in the security mechanisms of an information system and thereby help it protect data and maintain intended functionality.

II. LITERATURE REVIEW

The current status of research on dynamic routing techniques in software Defined Networks (SDNs) id reviewed in the literature. It focuses on a unique dynamic routing called "Routing algorithm optimization for software defined network WAN", which was recently proposed in the IEEE conference. SDNs and their importance on contemporary networking technologies. The difficulties with conventional routing protocols and the requirement for dynamic routing in SDNs are then covered. Afterward, the review delves into various existing dynamic routing approaches in SDNs, highlighting their strengths and limitations. Finally, it critically evaluates the proposed new dynamic routing approach, discussing its potential contributions, innovative features, and areas for further improvement. Overall, In the literature review aims to provide insights into the advancements and challenges in dynamic routing for SDNs, offering valuable guidance for future research in the domain.

Dynamic routing in software defined networks lacks flexibility and adaptability, resulting in inefficient resource utilization.

A. Role of dynamic routing in SDNs:

Benefits of dynamic routing over traditional approaches such as classification of dynamic routing approaches. Existing Dynamic Routing Approaches in SDNs. Overview of prominent dynamic routing protocols (e.g., OSPF, BGP)

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 13 Issue: 1
***Article Received:** 25 November 2024 **Revised:** 12 December 2024 **Accepted:** 02 January 2025*

B. Evaluation of their suitability for SDNs

By structuring the literature review in the manner, readers can gain a holistic understanding of the landscape of dynamic routing in SDNs, the challenges faced by traditional routing protocols, and the potential of the proposed new approach to address these challenges. Additionally, the critical evaluation and discussion sections provide valuable insights for researchers and practitioners looking to contribute to the advancement of dynamic routing in SDNs.

III. NETWORK TOPOLOGY USED FOR SDN

The meaning of "Topology" is "structure" or "arrangement" of the network. Network topology term is used in different contexts, such as in computer networks, electrical circuits, or even geometric shapes. In the context of computer networks, topology describe the physical or logical structure of the network through topology. It explains how devices on the network are connected and how information flows. Here are some common network topologies:

a) Bus Topology: Bus topology means all devices share a single communication line. Every device is connected to the endpoints of the bus.

b) Star Topology: Star topology means every device is connected to a central hub or switch. Devices are directly connected to the hub/switch, and the hub/switch manages it.

c) Ring Topology: Every device is directly connected to its neighbours, and the last device to the first device. There is a circular path in which data flows in one direction.

d) Mesh Topology: Every device is directly connected to other devices. It is robust because if one link fails, other alternate routes are available.

e) Hybrid Topology: There are some combinations like star-bus, star-ring, etc. Organizations use a mix of different topologies based on their specific requirements. To set the topology for the specific requirements to consider these factors.

f) Scale of the Network: Before selecting any topology, it is important to see how many devices are there and accordingly how much complexity is required.

g) Reliability Requirement: Whenever the topology is to be set, it is important to know whether additional network is required or not.

h) Cost: While checking the topology it will clear how much budget is available for the network.

i) Ease of Management: As per setup the network there will have to decide which topology will be easier to manage.

j) Performance: It also becomes to know how much speed and efficiency is required to operate the network.

Topology choose the appropriate topology as per the requirements by considering these factors.

IV. DYNAMIC ROUTING IN SDNS

Dynamic routing refers to the process by which network topology changes cause routers to dynamically exchange routing information and modify their routing tables or other factors. Some key aspects of dynamic routing including: routing protocols, routing metrics, routing information exchange route convergence, administrative distance.

Dynamic routing offers several advantages such as: automatic adaption, scalability, load balancing, ease of management, etc. dynamic also introducing complexity and overhead, particularly in terms of protocol configuration network convergence and resource consumption.

A. Importance of dynamic routing in SDNs

The Dynamic routing plays a crucial role in Software Defined Networks (SDNs) due to several key reasons:

1) Flexibility and adaptability: SDNs provide for centralized network control and programmability by severing the control plane from the data plane. Dynamic routing protocols allow for flexible and adaptive routing decisions based on real-time network conditions and policies. Dynamic routing flexibility is essential in modern networking environments where traffic patterns, application requirements, and network demands can vary dynamically.

2) Efficient Resource Utilization: Dynamic routing in SDNs facilitates efficient utilization of network resources by dynamically adjusting routing paths based on factors such as link congestion, load balancing, and Quality of Service (QoS) requirements. By dynamically optimizing the routing paths, SDNs can improve network performance, reduce latency, and enhance overall resource utilization, leading to a more efficient network operation.

3) Scalability: Traditional routing protocols, such as OSPF and BGP, face scalability challenges in large and complex networks. In contrast, dynamic routing in SDNs offers scalability advantages by enabling centralized control and management of the network through a logically centralized controller. Scalability centralized control facilitates simplified network management and scalability, allowing SDNs to efficiently handle large-scale networks with thousands of devices and diverse traffic patterns.

4) Policy Enforcement and Traffic Engineering: Dynamic routing in SDNs enables fine-grained policy enforcement and traffic engineering capabilities. Network administrators can define routing policies and traffic engineering objectives centrally and enforce them dynamically across the network. PETE centralized control allows for more granular control over traffic flows, better alignment with business objectives, and the ability to adapt routing decisions based on changing requirements or security threats.

5) Support for Network Virtualization: SDNs often support network virtualization, enabling the creation of multiple virtual networks (e.g., Virtual Private Networks - VPNs) over a shared physical infrastructure. Dynamic routing protocols play a critical role in supporting network virtualization by dynamically routing traffic between virtual networks, ensuring isolation, and efficient utilization of network resources while maintaining network security and performance.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 13 Issue: 1
***Article Received:** 25 November 2024 **Revised:** 12 December 2024 **Accepted:** 02 January 2025*

6) Resilience and Fault Tolerance: Dynamic routing in SDNs enhances network resilience and fault tolerance by enabling rapid detection and recovery from network failures or link congestion. With centralized control and real-time visibility into network conditions, SDNs can dynamically reroute traffic to alternate paths, bypassing failed or congested links, and minimizing the impact of network disruptions on application performance and user experience.

V. METHODOLOGY

Shortest Feasible path OpenFlow Design (SFOP)refer to a networking concept or methodology aimed at optimizing the routing of data packets within OpenFlow-based Software-Defined Networking (SDN) architectures. In SDN, OpenFlow is a protocol that permits network device programmability and centralized control by separating the control plane from the data plane. The term "Shortest Feasible Path" likely pertains to the efficient routing of traffic within the network.

A design based on SFOP principles would likely involve:

1) *Traffic Engineering:* Analysing the network topology and traffic patterns to determine the shortest feasible paths for data packets.
2) *Path Computation:* Calculating the shortest paths using algorithms such as Dijkstra's or variations of it.
3) *OpenFlow Configuration:* Programming the network devices (such as switches and routers) using OpenFlow to enforce the computed paths.
4) *Dynamic Adaptation:* Implementing mechanisms for dynamic adaptation to network changes, such as link failures or traffic fluctuations.
5) *Performance Optimization:* Fine-tuning the design to achieve optimal network performance, considering factors like latency, throughput, and reliability.

Overall, SFOP design in the context of OpenFlow based SDN aims to create efficient and adaptive network architecture that help to dynamically optimize the routing of traffic based on current conditions and requirements.

VI. A NEW PROPOSED SFOP ALGORITHM

The Shortest Feasible OpenFlow Path (SFOP) algorithm is a technique used in Software defined networking (SDN) to find the shortest path between two nodes in a network while considering the feasibility of OpenFlow rules on the path. OpenFlow [14] is a communications protocol that enables control of the paths through network devices such as switches by an external controller. Some of the basic outline of to implement the SFOP algorithm:

Step 1: Define the network topology

Step 2: Node and link weights

Step 3: Specify Source and destination

Step 4: Calculate Shortest path

Step 5: Check Feasibility of OpenFlow Rules

Step 6: Create OpenFlow Rules

Step 7: Implement Flow Entries

Step 8: Monitor and Update

Step 9: Route the traffic as per monitoring

VII. DYNAMICALLY CONFIGURE AND CONTROL NETWORK DEVICES

Software-Defined Networking (SDN) is a network architecture in which the control and data planes of the network are separate. In the way, network control and management software operate from a centralized location, which helps to dynamically configure and control network devices. Whenever SDN chosen some important factors should be in the mind such as:

1) *Requirements and Use Cases:* Help in understanding the requirements and use cases of the network. Different SDN solutions are designed for different use cases.
2) *Scalability:* It is also important to keep in mind the future growth of the organization. Choose an SDN solution that can scale easily.
3) *Vendor Compatibility:* If already have network devices from a specific vendor, then will choose an SDN solution that is compatible with that vendor's devices.
4) *Open Standards:* SDN solutions that are based on open standards can be used to avoid vendor lock-in. OpenFlow is a common SDN standard.
5) *Security:* Network security is a critical aspect. Ensure that SDN solution enhances the network security and minimizes vulnerabilities.
6) *Ease of Management:* The purpose of SDN is to simplify network management. Choose an SDN solution that helps to manage the team easily.
7) *Cost: Cost is also an important factor:* Apart from the initial investment, operational costs should also be considered when implementing SDN.
8) *Community Support:* Considering open-source SDN solutions is also an option. SDN can get support from the community for support and updates.
9) *Training and Skillset:* It is also important to train the team on the concepts and implementation of SDN. Ensure and have the required skillset.

Some popular SDN solutions are Open Daylight, ONOS (Open Network Operating System), Cisco ACI (Application Centric Infrastructure), and VMware NSX. While choosing any of these, it is important to keep in mind the given factors.

A. Preliminary SDN dataset

1) *The term "SDN dataset":* is a bit vague, because SDN (Software-Defined Networking) is a network architecture and does not have directly associated datasets. But, if there are talking about datasets for SDN technology implementation, security, performance, or optimization, then datasets are available in some specific areas.
2) *SDN Benchmarks and Performance:* the SDN Benchmarking and performance includes datasets that can be used to evaluate the performance of SDN architecture. These

datasets typically cover metrics of network traffic, latency, and throughput.

3) *Network Traffic Dataset:* Such datasets include samples of real-world network traffic, which are suitable for testing algorithms and protocols used in SDN environments.

4) *Security Datasets:* SDN includes datasets for security, samples of network attacks, vulnerabilities, and data for intrusion detection. These datasets are used to test security algorithms and mechanisms.

5) *SDN Controller Logs:* SDN controllers generate logs in which network events and activities are recorded. By analysing these logs, SDN performance and security can be evaluated.

6) *Topology Datasets:* topology datasets describe the physical or logical structure of the network. These include network devices, links, and their attributes.

7) *Flow Table Datasets:* In SDN, flow tables define the behaviour of network devices. Flow tables are used to populate tables in datasets and their study is important for flow control algorithms of SDN.

Looking for SDN datasets focused on the specific use case or research area. When creating an SDN dataset, it's essential to include a statement of limitations to provide transparency about the dataset's characteristics and potential biases.

B. Data Collection Constraints:

There are some data Collection Constraints, Data Quality, Representativeness, Labelling Challenges, Bias and Generalization, Privacy and Ethical Considerations.

C. Scope and Use Cases:

Future Work: Identify areas for future research or improvements to the dataset. The research could include expanding the dataset size, incorporating additional features, or addressing specific limitations identified during analysis.

By including a statement of limitations, the analysis provides users of the dataset with valuable context and insights into its characteristics, enabling them to interpret the results and findings appropriately. Additionally, it helps foster transparency and trust in the research community.

VIII. Conclusion and Future Scope

The SFOP discussed through the paper define the capability of the implementation of automated network management facilitates the integration and administration of corporate applications. The SDN controller functions as a network's operating system in essence the operator communicates through a northbound interface such as a firewall or load balancer. Shortest Feasible Path OpenFlow design (SFOP) methodology`s aims to optimize the routing of data packets within OpenFlow-based Software-Defined Networking (SDN) architectures. After taking some of the basic outline of the algorithm (SFOP), define topology, node and link weights, specified source and destination, calculate shortest path, Check feasibility of OpenFlow rules, create Open Flow rules, implement Flow entries, monitor and update, route the traffic as per monitoring.

SFOP aims to address scalability challenges in SDN deployments by optimizing the forwarding and control plane interactions. SFOP offers significant potential for improving the scalability, efficiency, and reliability of future SDN deployments, making it a promising algorithm for use in next-generation networking architectures.

IX. References

[1] Casado M., Freedman M. J., Pettit J., Luo J., McKeown N., and Shenker S. (2007). Ethane: Taking control of the enterprise. In SIGCOMM '07.

[2] M. Casado, T. Koponen, D. Moon, and S. Shenker. (2008). Rethinking packet forwarding hardware. In Proc. Seventh ACM SIGCOMM HotNets Workshop.

[3] Cisco Application eXtension Platform Overview. http://www.cisco.com/en/US/prod/collateral/routers/ps9701/white_paper_c11_459082.html.

[4] Benamrane et al. (2017) An east-west interface for distributed SDN control plane: implementation and evaluation Compute. Electr. Eng.

[5] Kodzai, C. 2020. Impact of network security on SDN controller performance. Master Thesis. University of Cape Town. http://hdl.handle.net/11427/32514.

[6] Rossi, F.D., Rodrigues, G.D.C., Calheiros, R.N., Conterato, M.D.S. (2017). Dynamic network bandwidth resizing for Big Data applications, In: Proceedings of thirteenth IEEE International Conference on eScienc.

[7] "Software Defined Networking: The New Norm for Networks", ONF White Paper, April 13, (2012).

[8] Bloomberg, "SD-WAN: Entry Point For Software-Defined Everything." [Online]. Available: https://www.forbes.com/sites/jasonbloomberg/2017/03/20/s

[9] McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., et al.: (Mar 2008). OpenFlow: Enabling Innovation in Campus Networks, In: SIGCOMM Computer Communication Review, vol. 38, no. 2, pp. 69–74.

[10] Limoncelli, T. A. (2012). OpenFlow: a radical new idea in networking, In: ACM Queue, vol. 10, no. 6,

[11] Hu, F., Hao, Q., Bao, K. (2014) A survey on software defined network and OpenFlow: from concept to implementation. IEEE Commun. 16(4), 2181–2206.

[12] Hakiri, A., Gokhale, A., Berthou, P., Schmidt, D.C., Gayraud, T. (2014). Software defined networking: challenges and research opportunities for future internet. Comput. Netw. 75, 453–471.

[13] Farhady, H., Lee, H., Nakao, A. (2015) Software defined networking: a survey. Comput. Netw. 81, 79–95.

[14] Gong, Y., Huang, W., Wang, W., Lei, Y. (2015). A survey on software defined networking and its applications. Front. Comput. Sci. 9(6), 827–845.

[15] AI-Sadi Ameer Mosa, AI-SHerbaz Ali, Xue James, Turner Scott (2016). Routing algorithm otimiztion for software defined network WAN. IEEE Conference. Doi:10.1109/AIC-MITCSA.2016.7759945