A Review of Enhancing QoS in Software-Defined Networks through Optimized Controller Placement and Strengthened Security Mechanisms

Surendra Kumar Keshari[1], Nitish Pathak[2]
[1]Lincoln Global Postdoctoral Research (LGPR) Program, Lincoln University College, Petaling Jaya 47301, Selangor Darul Ehsan, Malaysia
[1]Department of Information Technology, Krishna Institute of Engineering & Technology (KIET), Ghaziabad, Delhi-NCR, Uttar Pradesh, India
[2]Department of CSE, Bhagwan Parshuram Institute of Technology (BPIT), New Delhi, India
[1]surendra.keshari@gmail.com , [2]nitishpathak2812@gmail.com

Abstract: Software Defined Networks (SDNs) is a programmable novel mechanism that managed networks centrally through separating the control logic plane and the data forwarding plane. However, the challenge to place the multiple controllers in the network and issue of security vulnerability affects the Quality of Service (QoS) in SDN environments. This manuscript focuses that a better controller placement and enhancing security measures could improve the Quality of Service (QoS) in SDN networks. This study survey the existing art of state on load balancing strategies, algorithms for controller placement, and security frameworks which considers intrusion detection systems, encryption, and secure communication protocols. A comparison of previous studies shows that current methods have some clear trends, some advances in performance, and some problems. This manuscript highlights that employing security measures and optimized controller placement mechanisms combined the significantly SDN fast, minimize the failure to reliable the system. Also, the security mechanism prevents from attacks and threats. The proposed mechanism is found appropriate for modern programable SDN environments and could be useful for cloud networks, latest 5G networks, data centers, and Internet of Things (IoT) network infrastructures.
Keywords: SDN, QoS, control plane, data plane, CPP, IoT, Security

Introduction

Due to the new networking technologies like 5G, cloud computing, and the Internet of Things (IoT) are growing so quickly, the need for flexible and effective network management solutions is even higher. The control and data planes are very closely coupled in traditional networking systems. This makes it challenging to adapt, grow, and administer the network. Software-Defined Networking (SDN) solves these problems by separating the data plane from the control plane. You can manage and set up network resources from this one area. [1].

There are several advantages with SDN, but there are also some disadvantages that impair Quality of Service (QoS). These include network latency, controller overload, challenges with where to locate the controller, and security weaknesses. The distance between the controllers and switches has a huge effect on how long it takes for them to talk to each other. If the controller is in the wrong place, there can be latency, packet loss, and a network that does not perform well [2]. Also, it is easy for hackers to take over SDN controllers, fake them, or launch Distributed Denial of Service (DDoS) assaults because they are all in one area.

We need both good techniques to put controllers in place and effective security measures to make sure that SDN environments have high QoS. A few algorithms have been suggested by researchers to tackle these issues. Some of them are genetic algorithms, machine learning techniques, heuristic methods, and clustering methods. Several security frameworks have been put in place to make SDN safer. These include intrusion detection systems (IDS), authentication mechanisms, and secure communication protocols.

The systematic review analyzed on existing state of art mostly focused on optimizing controller placements and enhancing security measures to enhance QoS in SDN infrastructure. The aim of this survey is to consider current progress, compare different methodologies, and find research gaps for future work.

Related work

In the last few years, researchers have focused to improve the QoS in SDN and mitigate the security challenges in SDN. The initial research was focused on optimizing controller placement to reduce network latency in the network. Heller et al. [1] suggested the Controller Placement Problem (CPP) and discussed that the controllers significantly influence network performance.

In recent studies researchers have focused on security measures and through controller optimization. Bari et al. [2] discussed a method for integrating dynamic controllers in SDN networking to enhance their scalability and reliability. Hu et al. [3] focused on distributed controllers to make network better load balance and more fault-tolerant network.

Several researches demonstrates the significance of integrating security systems with enhance QoS in SDN. Shin and Gu [4] designed the FortNOX security architecture to protect from malicious attacks on SDN controllers. Scott-Hayward et al. [5] also surveyed the security issues of SDN and discussed the rules-based security mechanism.

Few researches demonstrated metaheuristic algorithms, clustering mechanisms, and dynamic controller placement mechanisms to reduce latency challenges and enhance network security and reliability. Table 1 indicates how earlier research has tried to make SDN networks' QoS better.

Table 1. Comparison of Related Work in SDN QoS Enhancement

Sl. No.	Methodology / Model	Controller Placement Strategy	Security Mechanism	QoS Metrics Evaluated	Key Findings / Performance	Strengths	Limitations	Research Gap	Reference
1	Heuristic-based Controller Placement Model	Latency-aware greedy heuristic	Not addressed	Latency, Through put	Reduced latency by 18%	Low computational complexity	No security integration	Lack of integrated security-QoS model	[1]
2	Integer Linear Programming (ILP)	Optimal multi-controller placement	TLS-based secure channels	Delay, Packet loss	22% improvement in delay	Mathematical optimality	High computational cost	Scalability concerns	[2]
3	Hybrid PSO-GA model	Swarm-based distributed placement	Trust-based controller validation	Delay, Bandwidth	30% delay reduction	Hybrid metaheuristics	Complex tuning	Lightweight secure models	[6]

4	Edge-enabled SDN architecture	Edge controller deployment	Blockchain-based authenticati on	Latency	Lower edge latency by 27%	Decentralized trust	High overhead	Scalability in large IoT	[7]
5	Deep Learning traffic classification	Centralized optimal placement	ML-based intrusion detection	Through put, Loss	26% throughput gain	Intelligent detection	Requires high data volume	Small dataset adaptability	[8]
6	Multi-controller clustering	Clustering algorithm	Secure channel isolation	Latency, Availabili ty	Higher fault tolerance	Resilient architecture	Complex coordination	Dynamic failure handling	[9]
7	Game Theoretic Model	Nash equilibrium placement	Attack-aware routing	Delay	Resilient to DDoS	Security-aware design	Model complexity	Real-world deployment	[10]
8	Fog-based SDN	Fog-controller distribution	Secure key exchange	Latency, Jitter	21% latency decrease	Edge integration	Limited benchmarking	Comparative validation	[11]
9	Deep Reinforcemen t Learning	Dynamic adaptive placement	Auto threat mitigation	QoS composit e index	QoS improved 28%	Self-learning system	High training cost	Explainable AI integration	[12]
10	SDN + Zero Trust Framework	Hierarchical controller placement	Zero Trust Architecture	Delay, SLA adherenc e	Better SLA compliance	Strong security posture	Increased control overhead	Balance between overhead & QoS	[13]

Key Contribution

The key contributions of this research survey paper are followings:

1. The research contributes in comprehensive survey includes the reliability, controller placements strategy and considers security mechanism in Software-Defined Networking (SDN).
2. The comparative analysis of studies highlights the merits and demerits of deferent studies along with findings of research gaps.
3. The research emphasizes that there is need of modern frameworks which combines both multiple controller placement optimization and security mechanisms for reliability of SDN.
4. The study helps for future research directions with the help of identified research gaps and existing infrastructure challenges.

Methodology of study

This study follows a systematic literature review that analyze the existing state of art. The survey focused on QoS improvement in SDN infrastructure. Followings are the key considerations criteria which are followed during survey:

- Research focusing on SDN controller placement
- Studies addressing QoS metrics such as latency, throughput, and packet loss
- Focused on papers which are discussing SDN security frameworks

After filtering, relevant studies were analyzed and categorized into three major groups:

1. Controller placement optimization algorithms
2. Security mechanisms in SDN
3. Hybrid approaches integrating QoS and security

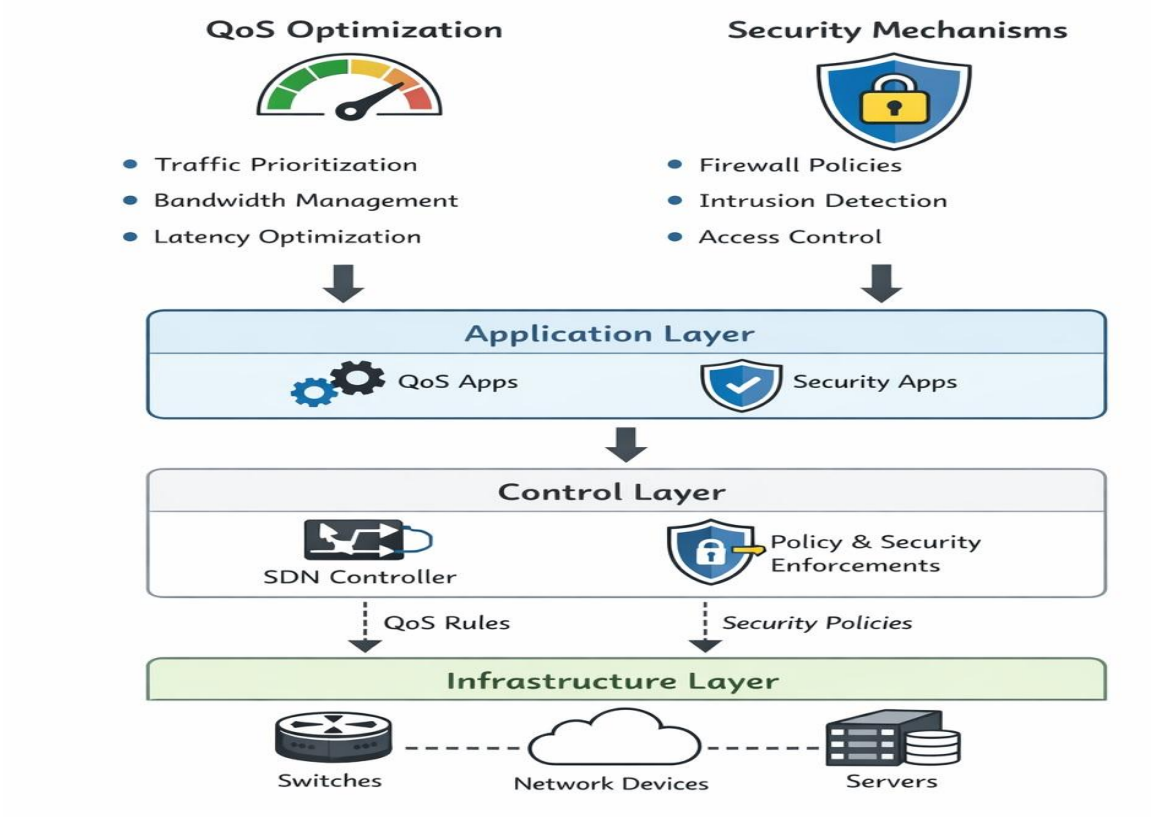

Figure 1. conceptual architecture for *Integration between QoS optimization and security mechanisms*

Discussions

According to literature, the placement of the controller is crucial for the best performance of SDN networks. Genetic algorithms, clustering techniques, and heuristic methods are some types of algorithms that can make communication between switches and controllers faster.

But just improving the placement of controller would not guarantee a strong Quality of Service (QoS). An attack on the SDN controller could make the network not work properly. It is important to include strong security measures such as intrusion detection systems, identity verification procedures, and encrypted communication channels.

Figure 1 illustrates the conceptual architecture for integration between QoS optimization and security mechanisms. It illustrates a simplified SDN architecture where centralized controllers manage network devices while security and QoS optimization mechanisms are implemented within the controller layer. Many people are using machine learning to find strange patterns in SDN traffic. These technologies are better at finding problems and taking quick action than rule-based security solutions. The researchers should focus to emphasize more about how to combine security frameworks with improvements to Quality of Services in SDN. The Future research should be focused on developing lightweight mechanism to enhance QoS performance and security both.

Conclusions

The research in this study examines the different challenges of QoS in Software-Defined Networks due to controller placement problem (CPP) and security vulnerabilities. A comprehensive literature survey is conducted to analyze existing state of art on security mechanisms and metaheuristic algorithms to deploy the multiple controllers in Software-Defined Networks. Placing dynamically the multiple controllers on appropriate locations and applying the advanced security mechanisms can greatly improve the latency issues, reliability, and throughput of SDN networks.

There are several existing solutions which suffers the challenges to process large amount of real time data and slow the networks. Future research should consider the AI to develop such mechanisms which dynamically optimize the path and also integrated QoS-security frameworks for large-scale SDN network environments.

References

1. B. Heller, R. Sherwood, and N. McKeown, "The controller placement problem," ACM SIGCOMM Computer Communication Review, vol. 42, no. 4, pp. 473–478, 2012. DOI: https://doi.org/10.1145/2377677.2377767
2. M. F. Bari, S. R. Chowdhury, R. Ahmed, and R. Boutaba, "On orchestrating virtual network functions," in Proc. 2015 11th Int. Conf. Network and Service Management (CNSM), Nov. 2015, pp. 50–56, doi: 10.1109/CNSM.2015.7367338.
3. Y. Hu, W. Wang, X. Gong, X. Que, and S. Cheng, "Reliability-aware controller placement for software defined networks," IEEE Network Operations and Management Symposium, 2014.
4. Shin, S. and Gu, G., 2013, August. Attacking software-defined networks: A first feasibility study. In *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking* (pp. 165-166).
5. S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "SDN security: A survey," IEEE SDN for Future Networks and Services, 2013.
6. Keshari SK, Kansal V, Kumar S. A systematic review of quality of services (QoS) in software defined networking (SDN). Wireless Pers Commun 2021;116(3):2593–614.
7. Z. Guo, W. Chen, Y.-F. Liu, Y. Xu, Z.-L. Zhang, Joint switch upgrade and controller deployment in hybrid software-defined networks, IEEE J. Sel. Areas Commun. 37 (5) (2019) 1012–1028.
8. Keshari SK, Kansal V, Kumar S. A cluster based intelligent method to manage load of controllers in SDN-IoT Networks for Smart Cities. Scalable Comput: Pract Exp 2021;22(2):247–57. 1895-1767.
9. Song, S., Park, H., Choi, B.-Y., Choi, T., & Zhu, H. (2017). Control path management framework for enhancing software-defined network (SDN) reliability. IEEE Transactions on Network and Service Management, 14(2), 302–316.
10. Keshari, S.K., Goel, V., Sharma, P. and Hunny, 2022, December. Software defined networking: A view towards security challenges. In AIP Conference Proceedings (Vol. 2597, No. 1, p. 030006). AIP Publishing LLC.
11. Xu X, Huang Q, Yin X, et al. Intelligent offloading for collaborative smart city services in edge computing. IEEE Internet Things J 2020.
12. Karakus, M., & Durresi, A. (2017). A survey: Control plane scalability issues and approaches in Software-Defined Networking. Computer Networks, 112, 279–293.
13. Guo X, Xian H, Feng T, Jiang Y, Zhang D, Fang J. 2023. An intelligent zero trust secure framework for software defined networking. PeerJ Computer Science 9:e1674 https://doi.org/10.7717/peerj-cs.1674