Software Defined Networks

Ifra Ejaz	Abdullah Awan	Ali Hassan Zaidi
21L-7508	21L-7713	21L-5274
l217508@lhr.nu.edu.pk	l217713@lhr.nu.edu.pk	l215274@lhr.nu.edu.pk

Literature Review

The inherent flaws and limitations in traditional network architectures have developed a need to shift towards a more centralized form of networking, called the "software defined networking". In traditional networking, the control plane is embedded within each network device, making it difficult to adjust network behavior dynamically or implement global policies efficiently. The purpose of this literature review is to summarize all the research that has been done on SDN and to address the issues that are missed out in the researches.

A. Overcoming Legacy Limitations and Embracing Programmability

According to Jamal et.al (2014), SDN overcame the limitations of legacy networks by simplifying network management through centralized control and programmability. This paper [1] underscores the research community's efforts in developing SDN solutions to create more agile, flexible, and efficient networks, marking a significant shift in networking paradigms to meet modern digital requirements. This study highlights that SDN is not only a means to simplify network architecture by centralizing control but also as a foundation for network virtualization, thereby heralding a new era of programmable and agile networks.

B. Strategic SDN Controller Selection and Network Management

The article [2] particularly focuses on the critical aspects of SDN controller selection, interoperability, security, and the overarching goal of implementing effective network management strategies. The choice of an appropriate SDN controller to achieve optimal network performance and reliability is very crucial. It impacts the network's flexibility, scalability, and the ability to implement advanced features such as load balancing, network virtualization, and dynamic access control. Mishra & AlShehri (2017) suggest using the Analytic Hierarchy Process (AHP) for selecting the best controller, a methodology that allows for a systematic comparison of controllers based on multiple criteria, ensuring a decision that best aligns with the network's specific needs and goals. The introduction of OpenFlow as a concrete realization of SDN's principles is particularly noteworthy. OpenFlow facilitates the experimental deployment of new protocols and the reengineering of network traffic without disrupting production applications, showcasing the practical benefits of SDN's architecture. The article [3] also explores the organizational objectives, presenting a detailed analysis of SDN's challenges and opportunities in shaping the Future Internet. This encompasses discussions on network visibility and management, routing and service convergence, and the evolution towards hybrid SDN control architectures.

C. Software-Defined Networking: Enhancing Security, Revolutionizing Applications, and Shaping the Future of Network Management

Strong protection for the SDN controller, a crucial component that might be the target of cyberattacks, is one of the important security measures highlighted. SDN's ability to strengthen network security from the ground up is further demonstrated by the creation of a comprehensive policy framework and the building of trust within the network. According to recent studies, this direct integration of security controls into SDN design and operation represents a break from traditional security approaches and creates more manageable and secure network environments.

In parallel, SDN's applications in a variety of industries highlight how drastically it has changed network configuration and management. By enabling dynamic resource allocation and offering intelligent control over network operations, SDN completely transforms the conventional network paradigm. Its uses are numerous and range from providing network intelligence and monitoring to improved defense services, as well as from guaranteeing adherence to NPM standards to assisting with high-performance applications.

D. *Multiple Controllers in SDN: Enhancing Network Management through Scalability and Reliability*

Despite the fact that a single controller provides centralized control, its vulnerability as a single point of failure poses serious limitations, particularly with regard to scalability and reliability. In order to overcome these drawbacks, the paper proposes using multiple controllers in SDN networks. This strategy seeks to improve the network's scalability, dependability, and overall performance in order to overcome the drawbacks of a single controller system. The article [5] outlines different design principles, architectures, placement strategies, and scheduling techniques relevant to multiple controller implementations in SDN through a comprehensive review of the literature. A comparative examination of the various controller platforms and projects currently in use reveals a varied range of options, each with special qualities and attributes. This article has discussed different architectures for multiple controllers and significance of each.

E. *Enhancing IoT Security through Machine Learning and SDN Integration: Challenges and Opportunities*

A new era of connectivity and data interchange has been brought about by the Internet of Things' (IoT) exponential expansion, which has created previously unheard-of potential for innovation in a variety of industries. But the spread of IoT devices also brings serious security risks, calling for cutting-edge solutions to protect networked ecosystems. Drawing from the anticipated contents of the cited article, this literature review summarizes talks on the convergence of machine learning (ML), IoT security, and the function of Software-Defined Networking (SDN) in improving IoT security postures.

The article [6] also emphasizes the various risks that IoT faces, such as malware and data breaches, highlighting the need for sophisticated security frameworks and best practices designed to address IoT's particular difficulties. The usefulness of ML and SDN in protecting IoT deployments across different industries is illustrated through real-world case studies, indicating future research directions centered on issues related to scalability, interoperability, and compliance.

Potential Gaps in the Research:

Despite the extensive research and development in SDN, several areas remain underexplored or present ongoing challenges that necessitate further investigation. Notably, the adoption of SDN in practical scenarios and the comprehension of hybrid networks are impeded by the inadequate investigation of SDN's integration and interoperability with legacy systems [1]. Furthermore, even while SDN's potential for network management is acknowledged, nothing is known about how it may improve energy efficiency and offer complete, end-to-end security solutions at the control, data, and application layers [2]. The importance of having several controllers in SDN presents additional problems, such as the requirement for intricate inter-controller communication protocols and the need to handle fresh security vulnerabilities arising from their implementation [5]. Furthermore, a critical gap exists in the scalability of SDN and Machine Learning (ML) solutions, notably in IoT security. To close this gap, research is needed to determine efficient scaling techniques that can handle the exponential expansion of IoT devices without sacrificing security or performance [6].

References:

[1] https://www.sciencedirect.com/science/article/abs/pii/S1389128614002588

[2] https://sciresol.s3.us-east-2.amazonaws.com/IJST/Articles/2017/Issue-29/Article23.pdf

[3] https://www.researchgate.net/publication/267339360_Software-Defined_Networking_Challenges_and_research_opportunities_for_Future_Internet

[4] https://www.researchgate.net/publication/350081639_Software_Defined_Networking_A_review_on_Architecture_Security_and_Applications

[5] https://doi.org/10.1016/j.jnca.2017.11.015